Nonlinearity 5 (1992) 961–978. Printed in the UK

Galois theory of periodic orbits of rational maps

Franco Vivaldi and Spyros Hatjispyros

School of Mathematical Sciences, Queen Mary and Westfield College, University of London, Mile End Road, London E1 4NS, UK

Received 10 July 1991, in final form 5 February 1992
Accepted by P Cvitanovic

Abstract. The periodic points of a rational mapping are roots of a polynomial. If the coefficients of the mapping are algebraic numbers, then the periodic orbits are also algebraic numbers. A sequence of algebraic number fields is naturally associated with rational mappings, namely the fields containing all orbits of a given period. We study the corresponding Galois groups. We show that the latter have subgroups that permute the points of an orbit in the same way as the dynamics. The subgroup having all orbits as invariant sets identifies a field which contains the multipliers of the orbits. We construct their minimal polynomial, thereby computing the multiplier of a cycle without computing the cycle itself. We show that the periodic orbits of the quadratic family are soluble by radicals if their period is less or equal to 4, and we exhibit examples of unsoluble orbits of period 5. Dynamics over algebraic number fields is discrete, and all numerical experiments are reproducible.

AMS classification scheme numbers: 11R21, 11R32, 58F22

1. Introduction

The arithmetical environment for dynamics is the real number system, but most numbers are random and cannot be defined or manipulated (see [1], for an introduction). Numerical experiments can only make use of those numbers that are representable as a finite collection of integers.

Most computer experiments are performed using the floating-point representation of the real line. The resulting sets are subsets of the rationals which are not closed under any of the four arithmetical operations (see [2], vol 2) and, as such, hardly compatible with mathematical rigour. Because the floating-point representation is machine-dependent, and because the exponential instability of motion amplifies round-off errors, numerical experiments in dynamics have been plagued by the same lack of reproducibility that characterizes physical experiments.

A uniform discretization, whereby each dynamical variable is forced to assume values that are equally spaced on the real line, is more amenable to exact computations, since the phase space acquires the structure of a linear space over the integers ($\boldsymbol{Z}$-module). While more satisfactory, this type of discretization has been rarely used in dynamics, mainly because a nonlinear system does not usually leave these modules invariant, making the development of a discrete theory distinctively difficult [3–8].

Thus while in the past three decades dynamics has flourished thanks to a myriad of computer experiments, only a handful of exact numerical results have emerged.

0951-7715/92/040961+18$04.50

The theoretical basis for the use of computers is founded mostly on shadowing considerations, which forces statistics upon a deterministic problem (see [9, 10] and references therein).

But this price need not always be paid. There are dynamical systems for which discrete structures can be found which not only allow exact computation, but also the developement of a discrete dynamical theory. Here we refer to certain classes of algebraic mappings, whose phase points can be represented as *algebraic numbers*.

An algebraic number is the root of a polynomial with integral coefficients and it can be represented in a computer without approximations [11]. The set of all algebraic numbers is denumerable, and its elements can be regrouped to form infinitely many *fields*, which are 'intermediate' between $\boldsymbol{Q}$ and $\boldsymbol{R}$ or $\boldsymbol{C}$. Each field contains $\boldsymbol{Q}$ as a subfield, and is dense in $\boldsymbol{R}$ or $\boldsymbol{C}$. Consequently, numerical experiments involving only algebraic numbers can be performed exactly (in principle, at least), being limited solely by machine size and computation time.

Algebraic numbers appear naturally in certain linear dynamical systems [12–14]. Their discrete phase spaces are the $\boldsymbol{Z}$-modules alluded to above, but in this case these are not only invariant, but also possess a *ring* structure (a multiplication between phase points), which proves to be crucial for the development of an arithmetical theory.

Discrete structures for nonlinear systems are naturally associated with rational mappings of one or more complex variable. If the coefficients of the mappings are rational numbers, these dynamical systems possess an infinite set of discrete dynamical invariants, namely all algebraic number fields. Infinite towers of invariant fields will still be found when the coefficients are not rational, but are themselves algebraic numbers.

For instance, let d be a square-free integer. The set of numbers of the form $r+s\sqrt{d}$, with r and s rational form a *quadratic field*, denoted by $\boldsymbol{Q}(\sqrt{d})$. All its elements are roots of quadratic equations with integral coefficients. Consider a rational mapping f with coefficients in $\boldsymbol{Q}(\sqrt{d})$. It is clear that $f(\boldsymbol{Q}(\sqrt{d})) \subseteq \boldsymbol{Q}(\sqrt{d})$, that is f can be restricted to $\boldsymbol{Q}(\sqrt{d})$ which becomes a discrete 'phase space' for the mapping. Any number field containing $\boldsymbol{Q}(\sqrt{d})$ will serve the same purpose.

In this context the main problem is to select from all possible algebraic number fields those that are relevant to a particular dynamical phenomenon. A natural starting point is to consider the fields containing periodic orbits, in view of the prominent place of the latter in both theoretical and computational problems (for a recent development concerning computations with periodic orbits, see [15]).

The simplest case of rational mappings is that of a single complex variable. We let

$$f(x)=\frac{r(x)}{s(x)} \qquad f^n(x)=\frac{r_n(x)}{s_n(x)} \qquad n=1,2,\ldots \tag{1.1}$$

where f^n denotes the nth iterate of f (with $f=f^1$), and r_n and s_n are polynomials with coefficients in some algebraic number field K. We may assume that r_n and s_n have no common factor. The periodic points of period n of f are roots of the polynomial

$$P_n(x)=r_n(x)-xs_n(x). \tag{1.2}$$

Because the coefficents of P_n belong to K, the periodic points are numbers lying in algebraic extensions of K.

The purpose of this paper is to study the structure of the equation $P_n(x)=0$. For simplicity of exposition we shall only deal with the case in which f is a polynomial (i.e. $s_n(x) = 1$ in (1.2)). The extension of the theory to the case of rational functions will require only minor adjustments. By constructing the smallest field containing all periodic orbits of each minimal period n, we shall single out a family of algebraic number fields naturally associated with a dynamical system of the type (1.1). The central task will be the study of the Galois groups of these field extensions. We shall address the classical question of solubility by radicals, the very motivation of Galois's work [16]. (A discussion on radicals in computer algebra will be found in [11], section 2.6.)

In section 2 we introduce the polynomials H_n whose roots are the periodic points of *minimal* period n, and we study the rules governing their factorization. Their Galois groups G are studied in section 3. We show that G commutes with the dynamics, that is it preserves the orbit structure, and we determine some of its properties. In section 4 we turn to algebraic number fields, by applying the Galois correspondence. We show that the relation between the derivative of a map at a periodic orbit (the *multiplier* of an orbit) and the orbit itself is expressed algebraically by a *cyclic field extension*, which is the signature of dynamics within the Galois group. These multipliers are found to be roots of a polynomial, which we construct explicitly (this means that one can compute them without computing the orbit itself). We also show that the Galois group of the multiplier polynomial acts as a permutation of the orbits, and that its solubility coincides with that of G. In sections 5 and 6 we apply this theory to the quadratic family, first studying the factorization of H_n over the rationals, and then considering Galois groups. We show that all periodic orbits of period less than 5 are soluble by radicals, and we exhibit unsoluble orbits of period 5. Concluding remarks will be found in section 7.

For background reference on Galois theory, see [16]. For the reader's convenience, we have included in appendix 1 a glossary of the most commonly used terms.

Note added in proof. After this paper was completed, Odoni brought to our attention two recent preprints by Morton and Patel [17] and Morton [18], which deal with the same problem from a number-theoretical angle. The overlap between our work and theirs is considerable in substance, even though their viewpoint, motivations and style are quite different from ours.

2. Factorization

Let K be an algebraic number field (a finite extension of the rationals), and let f be a polynomial with coefficients in K, with degree $\partial f > 1$. (The simplest example is the quadratic mapping with rational coefficients: $f(x) = x^2 + c$, with $c \in \mathbb{Q} = K$.) The periodic points of period n of the map f are the roots of the polynomial P_n defined in (1.2). The degree of P_n is equal to $(\partial f)^n$, and if f is monic so is P_n. The polynomial P_n has multiple roots if

$$\frac{\mathrm{d}}{\mathrm{d}x}(f^n(x)) = 1$$

at some periodic point $x = \alpha$. This implies that such an α belongs to a marginally unstable n-cycle. Thus if f depends on a parameter, the occurrence of multiple roots is not generic, and will not be considered here.

Let H_n be the polynomial whose roots are the points of minimal period n. To construct it, we first note that

$$P_n = \prod_{d|n} H_d \tag{2.1}$$

where the product is taken over all positive divisors d of n. Then we express H as a function of P by means of the Möbius inversion formula for a product

$$H_n = \prod_{d|n} P_d^{\mu(n/d)} \tag{2.2}$$

where μ is the Möbius function ([19], ch 2). The degree of H_n is computed from (2.2) as

$$\partial H_n = \sum_{d|n} \partial P_d \mu\left(\frac{n}{d}\right) = \sum_{d|n} (\partial f)^d \mu\left(\frac{n}{d}\right). \tag{2.3}$$

By construction, ∂H_n is divisible by n, and it is also divisible by ∂f from (2.3) (for numerical examples, see table 1). Let $m = m(n)$ be the number of orbits of minimal period n. Clearly, $\partial H_n = mn$, whence, asymptotically, $m(n) \sim (\partial f)^n/n$.

The number of different ways a polynomial of degree d can factor is equal to the number of ways d can be expressed as a sum of positive integers (called the number $p(d)$ of *unrestricted partitions* of d [19], ch 14). In our case however, not all $p(mn)$ factorizations are possible, because the roots of H_n are permuted by a polynomial mapping. To see this we factor H_n over K into irreducibles

$$H_n = \prod_r h_r$$

and denote by Σ and Σ_r the respective splitting fields.

Let G be the Galois group of H_n. If $g \in G$, then, by definition, g preserves both addition and multiplication in Σ, and it leaves all coefficients of H_n fixed, because they belong to the ground field K. Thus, for any root α of H we have $g(f(\alpha)) = f(g(\alpha))$, that is *the Galois group commutes with the dynamics.*

Let h_r have roots $\alpha_r, \beta_r, \ldots$, and let $f(\alpha_r) = \alpha_s$, a root of h_s. Because h_r is irreducible, the Galois group permutes its roots *transitively* ([20], section 50). Then there exists an element g in G such that $g(\alpha_r) = \beta_r$, whence

$$h_s(f(\beta_r)) = h_s(f(g(\alpha_r)) = g(h_s(f(\alpha_r))) = g(h_s(\alpha_s)) = g(0) = 0$$

that is $f(\beta_r)$ is a root of h_s. Thus the roots of h_r are mapped into those of h_s, and by using f^{n-1} in place of f in the above argument we see that the converse is also true. Then the action of f on the roots of H_n induces a permutation of the irreducible factors of H_n. We express this by writing $f(h_r) = h_s$, which clearly implies $\Sigma_r = \Sigma_s$.

For illustration, consider the case $\partial f = 2$ and $n = 3$. From (2.3) we obtain $\partial H_3 = 6$. The possible factorizations of H_3 correspond to the following partitions of the number 6

$$\begin{array}{l} 6 \\ 3+3 \\ 2+2+2 \\ 3+1+1+1 \\ 1+1+1+1+1+1 \end{array} \tag{2.4}$$

Thus if H_3 is not irreducible it can either have two cubic factors, three quadratic ones, one cubic factor and three linear ones or six linear ones. These five permitted factorizations are to be compared with the $p(6) = 11$ available to a generic polynomial of degree 6.

We now consider the degree of the field extensions of the h_rs. Assume first that $f(h_r) = h_r$ (which includes the case in which H_n is irreducible, with $H_n = h_r$). Then $N_r = \partial h_r$ is a multiple of n. Let $m_r = \partial h_r/n$. The splitting field Σ_r is obtained from K by adjoining successively roots belonging to distinct orbits (m_r in all), as all points of a single orbit generate the same field extension. Specifically, if $\alpha_1, \ldots, \alpha_{m_r}$ are roots of h_r belonging to distinct orbits, then, in the extension $K(\alpha_1)$, the polynomial h_r splits as follows

$$h_r(x) = (x - \alpha_1)(x - f(\alpha_1)) \cdots (x - f^{n-1}(\alpha_1))g(x)$$

where $g(x)$ has degree $N_r - n$. By repeating this process m_r times, we obtain the bound

$$[\Sigma_r : K] \leq N_r(N_r - n)(N_r - 2n) \cdots (N_r - (m_r - 1)n) = n^{m_r} m_r!. \tag{2.5}$$

If $f(h_r) \neq h_r$, then (2.5) is replaced by $[\Sigma_r : K] \leq N_r!$, with N_r a proper divisor of mn. In either case the bound on the degree of the splitting field is stronger than that of a generic polynomial of degree mn, which is $[\Sigma : K] \leq (nm)!$.

The problem of determining the pattern of factorization for a mapping depending upon parameters appears to be difficult. In section 5 we will consider the quadratic family $f(x) = x^2 + c$ with rational c, we will provide evidence that, at least for small values of n, the polynomials H_n are irreducible with probability one, and we will single out some cases where factorization takes place.

The feasibility of a computation depends on the degree of the irreducible factors of the polynomial H_n, the most difficult case being the irreducible one. To give an idea of the scale of magnitudes involved, we display in table 1 the values of ∂H_n and m, for ∂f and n less than six, as computed from formula (2.3).

Table 1.

	$\partial f = 2$		$\partial f = 3$		$\partial f = 4$		$\partial f = 5$	
n	∂H_n	m	∂H_n	m	∂H_n	m	∂H_n	m
1	2	2	3	3	4	4	5	5
2	2	1	6	3	12	6	20	10
3	6	2	24	8	60	20	120	40
4	12	3	72	18	240	60	600	150
5	30	6	240	48	1020	204	3120	624

One sees that the periodic orbits of period 1 for mappings of degree less than 5, and those of period 2 for quadratic mappings are roots of polynomials of degree four or less. This means that they can be expressed explicitly in terms of radicals, using standard formulae [16]. In section 3 we will show that the solubility of H_n coincides with that of certain polynomials of the smaller degree m, so that a *sufficient* condition for solubility by radicals is that $m \leq 4$. From table 1, it will then follow that solubility extends to three additional cases, namely $n = 3$ and 4 for quadratic maps, and $n = 2$ for cubic ones. We will produce insoluble cases for $\partial f = 2$ and $n = 5$, showing that this condition cannot be improved in general.

3. Galois groups

In this section we consider the case in which the polynomial H_n is irreducible of degree mn. This appears to be the typical situation (see section 5). We exclude from our considerations the analysis of fixed points ($n = 1$), as the latter is just the general problem of solving polynomial equations of degree ∂f.

Let Ω be the set of roots of H_n, and let $F = \{f, f^2, \ldots, f^n\}$ be the collection of the first n iterates of the mapping. Then F—like the Galois group G—acts on Ω as a group of permutations, with identity f^n. Because H_n is irreducible, the group G is transitive over Ω, while F clearly is not (unless $m = 1$, which corresponds to just one case—see table 1). The action of F induces a partition of Ω into *blocks*

$$\Omega = \Omega_1 \cup \Omega_2 \cup \cdots \cup \Omega_m \qquad \Omega_i \cap \Omega_j = \emptyset, \text{ if } i \neq j \tag{3.1}$$

each block being a dynamical orbit

$$\Omega_k = \{\alpha_k, f(\alpha_k), \ldots, f^{n-1}(\alpha_k)\}$$

with initial condition α_k. As observed in the previous section, f commutes with each element of G. This implies that each automorphism of G maps blocks into blocks, that is, G is *imprimitive* ([20], section 49). This fact will simplify the problem considerably.

The action of G can be viewed as the composition of action within blocks and permutation of blocks. We shall demonstrate that the former mimics the dynamics, in the sense that for each orbit, the Galois group contains a subgroup which acts in the same way as the mapping f. The permutation of blocks, which maps the orbits into one another, describes relations existing among them.

Let G_k be the subgroup of G which fixes the block Ω_k *setwise*. The imprimitivity of G implies that G_k is a non-trivial subgroup of G, and that the G_ks are conjugate subgroups. Let $\alpha_k \in \Omega_k$. Because G is transitive, there exists a permutation $g \in G$ carrying α_k to its image under the mapping f, that is $g(\alpha_k) = f(\alpha_k)$, and since f commutes with g, f and g must have the same action on the entire block Ω_k. It follows that $g \in G_k$. In other words, the subgroup G_k consists of all those elements in G which act *locally*—on the kth orbit—in the same way as the mapping f and its iterates.

The restriction of G_k to the kth orbit is a homomorphism of G into the group of permutations of the elements of Ω_k. Its kernel L_k is the subgroup of G_k fixing Ω_k *pointwise*. Then L_k is a proper normal subgroup of G_k, and $G_k/L_k \cong C_n$, the cyclic group of n elements. The L_ks are conjugate subgroups, and their intersection is trivial.

We observe that if $g \in G$ fixes a root of H_n, i.e. $g(\alpha_k) = \alpha_k$, then g must fix its entire orbit under f, that is $g \in L_k$. In other words, the subgroup of G which fixes α_k concides with that which fixes Ω_k pointwise, which is L_k. Because an irreducible polynomial is normal if and only if the stabilizer of one (whence all) of its roots is trivial, it follows that the polynomial H_n is normal precisely when the subgroups L_k are trivial.

Every automorphism $g \in G$ naturally induces a permutation of the set of blocks $\{\Omega_1, \ldots, \Omega_m\}$, and the mapping carrying a root permutation to a block permutation is a group homomorphism, which we denote by Θ. Its kernel is the normal subgroup D of G which fixes simultaneously all blocks, namely

$$\operatorname{Ker}\Theta = D = \bigcap_k G_k. \tag{3.2}$$

Because G is transitive over Ω, the factor group $G/D \cong \Theta(G)$ permutes the blocks transitively.

We investigate some more specific properties of the various subgroups of G. We begin to show that D is *Abelian*, by representing it additively as a $\boldsymbol{Z}$-module. This will imply that G is soluble precisely when G/D is ([16], ch 13), and will allow us to shift our attention from G to G/D. We have seen that on each block Ω_k every element of $g \in D$ restricts to some power f^{l_k} of f, so that we can associate with each such g a string of m integers

$$\phi(g) = \{l_1, l_2, \ldots, l_m\} \qquad l_k \in \{0, 1, \ldots, n-1\} \qquad k = 1, \ldots, n. \tag{3.3}$$

Equation (3.3) defines a mapping ϕ of D into the $\boldsymbol{Z}$-module $O \cong \boldsymbol{Z}^m/n\boldsymbol{Z}^m$. One can verify that composition in D corresponds to addition in O, and that the kernel of ϕ is trivial, i.e. ϕ is a monomorphism. It follows that D is Abelian and its image $\phi(D)$ is a submodule of O.

Some relationships between various subgroups of G are expressed by the following propositions, which are proven in appendix 2.

(i) If $D \supseteq F$ then $G_k = L_k D$.
(ii) If $D = F$ then $G_k = L_k \otimes D$.
(iii) If $D \not\supseteq F$ then G is not Abelian.
(iv) $|G/D| = m$ if and only if $G_k = D$.

Thus the structure of G is considerably simpler if D coincides with, or at least contains, the dynamics F.

4. Fields

In this section we use the Galois correspondence to translate the results about the Galois group of H_n obtained in section 3 into statements about the structure of the subfields of its splitting field Σ.

We consider the fixed fields of G, D, G_k, L_k, respectively (see figure 1)

$$\Sigma = \mathrm{Fix}(G) \qquad \Delta = \mathrm{Fix}(D) \qquad \Gamma_k = \mathrm{Fix}(G_k) \qquad \Lambda_k = \mathrm{Fix}(L_k). \tag{4.1}$$

Under the Galois correspondence, conjugacy of subgroups is carried ('belongs') to conjugacy of subfields. This implies that the Γ_ks are conjugate subfields, and so are the Λ_ks.

We recall that the intersection of subgroups belongs to the field generated by the union of the corresponding fixed fields and, conversely, the intersection of fields belongs to (the group generated by the) union of groups. In particular, the intersection of all conjugates of a subgroup belongs to the normal closure of its fixed field.

This implies that the subgroups DL_k and $D \cap L_k$ belong to the fields $\Delta \cap \Lambda_k$ and $\Delta\Lambda_k$, respectively. Also, Δ is the normal closure of Γ_k, from the definition of D (see (3.2)), i.e. the extension $\Delta : K$ is normal. Because D is a normal subgroup of G_k, all relative extensions $\Delta : \Gamma_k$ are normal. The extensions $\Lambda_k : \Gamma_k$ are also normal (because $L_k \lhd G_k$) as well as cyclic (because their Galois group is $G_k/L_k \cong C_n$).

Let us consider the extension $\Lambda_k : \Gamma_k$. Since it is normal, we have

$$\Lambda_k = \Gamma_k(\alpha_k). \tag{4.2}$$

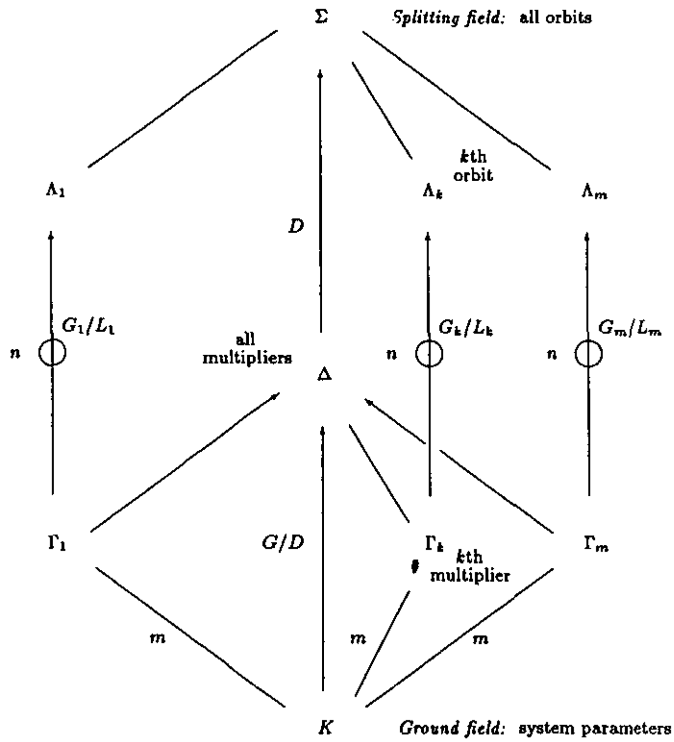

Figure 1. The structure of the subfields of the splitting field Σ of the polynomials H_n over the ground field K. Segments connecting fields denote field extensions, with the larger field above the smaller one. Information about extensions includes arrows (a normal extension), circles (a cyclic extension), upper case italics (the Galois group), and lower case italics (the degree).

To construct the minimal polynomial $\gamma_k(x)$ of α_k over Γ_k it is sufficient to note that its roots—the algebraic conjugates of α_k over Γ_k—are the points of the kth orbit

$$\begin{aligned}\gamma_k(x) &= (x-\alpha_k)(x-f(\alpha_k))\cdots(x-f^{n-1}(\alpha_k)) \\ &= x^n - s_{n-1}x^{n-1} + \cdots + (-1)^n s_0.\end{aligned} \tag{4.3}$$

The coefficients s_r of γ_k are the elementary symmetric functions of the points of the kth orbit, which generate Γ_k over the ground field K, since H_n is irreducible ([20], section 51).

Because the extension $\Lambda_k : \Gamma_k$ is cyclic, the points of an orbit can always be computed as radical expressions of the s_ks. This can be done by the classical technique of the Lagrange resolvent, which may require the adjunction of the nth roots of unity to the field Γ_k ([20], section 55). So an orbit is radical if its symmetric functions are.

Our main concern is to construct the fields Γ_k explicitly, thereby constructing G/D and examining the solubility of G. The general strategy will be that developed in [21], which involves two steps.

First, determine an element in Γ_k which generates Γ_k over K, and represent it explicitly as a polynomial $w(\alpha_k)$ in α_k over K (any element of Λ_k admits such representation, by definition). We have $w(\alpha_k) = w(f^t(\alpha_k))$ for all t, since $w(\alpha_k)$ is invariant under cyclic permutations of the points of the kth orbit. In other words, the generating element does not depend on the particular choice of a point in the kth orbit. On the other hand, if α_l belongs to another orbit, $w(\alpha_l)$ generates the conjugate field Γ_l, because $w(\alpha_k)$ is carried into $w(\alpha_l)$ by an element of the Galois group that permutes blocks. It follows that if $\alpha_1, \ldots, \alpha_m$ are representative points of the m orbits, chosen arbitrarily, $w(\alpha_1), \ldots, w(\alpha_m)$ are conjugate elements, and are therefore roots of the same irreducible polynomial.

Second, construct the irreducible monic polynomial $\delta(x)$ over K of degree m having $w(\alpha_1), \ldots, w(\alpha_m)$ as root, i.e.

$$\Gamma_k = K(w(\alpha_k)) \qquad \delta(w(\alpha_k)) = 0 \qquad k = 1, \ldots, m. \tag{4.4}$$

Then the splitting field of $\delta(x)$ is the field generated by $w(\alpha_1), \ldots, w(\alpha_m)$ over K, namely Δ, and its Galois group is G/D, from the Galois correspondence. Such a group permutes the elements $w(\alpha_k)$ in the same ways as it permutes the blocks Ω_k.

As a candidate for $w(\alpha_k)$, we look for an element of Σ that is invariant under cyclic permutations of the points of the kth orbit. A prominent symmetric function of the points of an orbit is the *multiplier* of the orbit (the derivative of the composite mapping f^n at any of its points). This is a polynomial in α_k, whose invariance under permutations of the points of the orbit derives from the chain rule of differentiation. Accordingly, we define (tentatively) $w(\alpha_k)$ as

$$w(\alpha_k) = \left.\frac{\mathrm{d}f^n(x)}{\mathrm{d}x}\right|_{\alpha_k} = \prod_{t=0}^{n-1} \frac{\mathrm{d}f}{\mathrm{d}x}\left(f^t(\alpha_k)\right). \tag{4.5}$$

The polynomials $w(\alpha_k)$ can be computed explicitly by means of expression (4.5). All polynomial arithmetic is to be performed modulo $H_n(x)$, so that the degrees involved in the calculation will never exceed mn (see later).

It remains to be shown that $w(\alpha_k)$ generates the whole of Γ_k, and not one of its proper subfields. All we know at this stage is that $w(\alpha_k)$ is a polynomial in the elementary symmetric functions s_i (cf (4.3)). For instance, for the quadratic family $f(x) = x^2 + c$, the derivative of the n-cycle Ω_k is an integral multiple of the product s_0 of the roots of $\gamma_k(x)$

$$w(\alpha_k) = 2^{-n}\left.\frac{\mathrm{d}f^n(x)}{\mathrm{d}x}\right|_{\alpha_k} = \prod_{k=1}^{m} \alpha_k = s_0 \tag{4.6}$$

where, for convenience, we have removed from $w(\alpha_k)$ the integral coefficient 2^n.

The final step is the construction of the minimal polynomial $\delta(x)$ of $w(\alpha_k)$. Its degree equals the degree of the extension $K(w(\alpha_k)) : K$, and since $K(w(\alpha_k))$ is a subfield of Γ_k, we conclude that $\delta(x)$ generates Γ_k when $\partial\delta = m = [\Gamma_k : K]$ (this happens when all numbers $w(\alpha_k)$, $k = 1, \ldots, m$ are distinct). If this is not the case, we replace α_k with $\alpha_k + r$ for a suitable integer r. It can be shown that for almost any value of r, the polynomial $w(\alpha_k - r)$ will have the desired property [21].

To construct δ from w we use a standard technique of linear algebra ([22], p 16). We note that for any $\zeta \in \Lambda_k$ the transformation $\zeta \mapsto w(\alpha_k)\zeta$ is a linear transformation M of Λ_k into itself. The field Λ_k, as a vector space of degree n over Γ_k, decomposes into the direct sum

$$\Lambda_k = V_1 \oplus \cdots \oplus V_n$$

where each module V_i is isomorphic to Γ_k, whence invariant under multiplication by $w(\alpha_k)$.

It follows that the Jordan form of M over K has n identical blocks along the diagonal, and its characteristic polynomial $\lambda(x)$ is the nth power of the minimal polynomial $\delta(x)$ of $w(\alpha_k)$ over K ([23], ch 11; [24], section 2.6)

$$\lambda(x) = \mathrm{Det}(M - x\mathbf{I}) = (\delta(x))^n . \tag{4.7}$$

In actual computations, the field Λ_k is represented canonically as the residue field of the polynomial ring $K[x]$ modulo the maximal ideal $(H_n(x))$ ([20], section 32)

$$\Lambda_k \cong \frac{K[x]}{(H_n(x))} \tag{4.8}$$

(this representation makes it quite clear that this construction is independent from k). Under this isomorphism, the number α_k is identified with the residue class of x, and, more in general, any polynomial $g(\alpha)$ over K is replaced by the remainder of $g(x)$ after dividing by $H_n(x)$.

The set $1, x, x^2, \ldots, x^{mn-1}$ forms a basis for $K[x]/(H_n(x))$ over K, to be used in the computation of M. Specifically, the mn entries in the rth column of M are the coefficients of the mn-degree polynomial $w(x) \cdot x^{r-1}$, which must be suitably reduced modulo $H_n(x)$.

5. The quadratic family: factorization

A quadratic mapping with coefficients in a field K can be reduced, via a linear conjugacy, to the canonical form

$$f(x) = x^2 + c \qquad c \in K. \tag{5.1}$$

The simplest cases are $K = \mathbb{Q}$ and $c = 0, -2$, where the Julia set is smooth.

5.1. *The case* $c = 0$

The Julia set is the unit circle, over which the map f restricts to a binary Bernoulli shift: $F(\theta) \equiv 2\theta \pmod 1$ (the 'doubling map'). The periodic points are rational points on the circle, which are roots of unity, plus the superstable fixed point $x = 0$. We have

$$P_n(x) = x^{2^n} - x = x \prod_{d|2^n-1} F_d(x) \tag{5.2}$$

where $F_m(x)$ is the mth order *cyclotomic* polynomial ([20], section 36)

$$F_m(x) = \prod_{d|m} (x^d - 1)^{\mu(m/d)} \tag{5.3}$$

whose roots are the primitive mth roots of unity, namely the numbers $\mathrm{e}^{2\pi \mathrm{i}k/m}$ with k and m coprime integers. Combining (2.2), (5.2) and (5.3) we obtain

$$H_n(x) = \prod_{d|n} \left(x \prod_{d_1|2^d-1} F_{d_1}(x) \right)^{\mu(n/d)} = x^{\sum_{d|n} \mu(n/d)} \prod_{d|n} \left(\prod_{d_1|2^d-1} F_{d_1}(x) \right)^{\mu(n/d)}$$

whence

$$H_n(x) = \begin{cases} xF_1(x) & n = 1 \\ \prod_{d|n} \left(\prod_{d_1|2^d-1} F_{d_1}(x) \right)^{\mu(n/d)} & n > 1 \end{cases} \tag{5.4}$$

where we have used the fact that the sum $\sum_{d|n} \mu(n/d)$ vanishes unless $n = 1$, when it is equal to 1 ([19], theorem 2.1).

Formula (5.4) implies that H_n is irreducible over $\boldsymbol{Z}$ (and consequently over $\boldsymbol{Q}$) if and only if $2^n - 1$ is a Mersenne prime (whence $n = p$ is prime), in which case the splitting field Σ is the $(2^p - 1)$th cyclotomic field $\boldsymbol{Q}(\exp(2\pi i/(2^p - 1)))$. Thus only a finite set of prime periods p are known for which H_p is irreducible [25].

5.2. *The case* $c = -2$

This is the 'Ulam point' of the quadratic mapping. The Julia set is the interval $[-2, 2]$, which contains all periodic orbits. This mapping is semi-conjugate to the doubling map via the function $g(\theta) = 2\cos(2\pi\theta)$.

Let m be a positive integer and ϕ the Euler's function ([19], ch 2). We define

$$\Psi_m(x + x^{-1}) = F_m(x) x^{-\phi(m)/2}. \tag{5.5}$$

We find

$$\Psi_1(x) = \sqrt{x - 2} \qquad \Psi_2(x) = \sqrt{x + 2}$$

while for $m > 2$, Ψ_m is a monic polynomial in $x + x^{-1}$. This can be established from the fact that

$$x^{\phi(m)} F_m(x^{-1}) = F_m(x)$$

and the repeated use of the identity

$$x^k + x^{-k} = (x + x^{-1})(x^{k-1} + x^{1-k}) - (x^{k-2} + x^{2-k}) \qquad k > 0$$

([26], p 37). The polynomials Ψ_1^2, Ψ_2^2, and $\Psi_m(x)$ for $m > 2$ are irreducible and generate the largest real subfield of the mth cyclotomic field, namely $\boldsymbol{Q}(\cos(2\pi/m))$.

Let $f(x) = x^2 - 2$, and g and F as above. Then

$$(f^n \circ g)(\theta) = e^{2\pi i 2^n \theta} + e^{-2\pi i 2^n \theta} = (g \circ F^n)(\theta).$$

From (1.2) we obtain

$$P_n \circ g(\theta) = g \circ F^n(\theta) - g(\theta) = X^{2^n} + X^{-2^n} - (X + X^{-1})$$

where $X = e^{2\pi i\theta}$. This can be rewritten as

$$\left(P_n \circ g\right)(X) = X^{-\frac{1}{2}(2^n-1)-\frac{1}{2}(2^n+1)}(X^{2^n-1} - 1)(X^{2^n+1} - 1). \tag{5.6}$$

By substituting

$$2^n \pm 1 = \sum_{d|2^n \pm 1} \phi(d) \qquad X^{2^n \pm 1} - 1 = \prod_{d|2^n \pm 1} F_d(X)$$

into (5.6) we get

$$\left(P_n \circ g\right)(X) = \prod_{d_1|2^n-1} \Psi_{d_1}(X+X^{-1}) \prod_{d_2|2^n+1} \Psi_{d_2}(X+X^{-1})$$

but $X+X^{-1} = g(\theta)$ whence

$$P_n(x) = \prod_{d_1|2^n-1} \Psi_{d_1}(x) \prod_{d_2|2^n+1} \Psi_{d_2}(x).$$

Note that in this expression Ψ_1 always appears as a square, while Ψ_2 never occurs.

Finally, Möbius inversion gives

$$H_n(x) = \prod_{d|n} \left(\prod_{d_1|2^d-1} \Psi_{d_1}(x) \prod_{d_2|2^d+1} \Psi_{d_2}(x) \right)^{\mu(n/d)}$$

One finds that $H_1 = \Psi_1^2\Psi_3$, $H_2 = \Psi_5$ is irreducible, while for $n > 2$ H_n is never irreducible.

5.3. Rational values of c

We examine the factorization of $H_n(x)$ over the rationals, for $n \leq 3$. From (2.2) and (5.1) we obtain

$$H_1(x) = x^2 - x + c$$

$$H_2(x) = x^2 + x + (c+1)$$

$$H_3(x) = x^6+x^5+(3c+1)x^4+(2c+1)x^3+(3c^2+3c+1)x^2+(c^2+2c+1)x+(c^3+2c^2+c+1).$$

The quadratic polynomials $H_1(x)$ and $H_2(x)$ factor over Q when their discriminants are squares of rational numbers. (The discriminant $d(f)$ of a monic polynomial f with roots $\theta,\ldots,\theta_n$ is the product $d(f) = \prod_{i<k}(\theta_i - \theta_k)^2$—see [20], section 26.)

Letting $d(H_1) = 1-4c = (2k-1)^2$ and $d(H_2) = -3-4c = (2k+1)^2$, with k rational, we obtain $c = -k^2+k$ and $c = -k^2+k-1$, respectively. For these values of the parameter c we have the factorization

$$H_1(x) = (x-k)(x+k-1) \qquad c = -(k^2-k)$$

$$H_2(x) = (x+k)(x-k+1) \qquad c = -(k^2-k+1).$$

In particular, no factorization takes place for c greater than $\frac{1}{4}$ and $-\frac{3}{4}$, respectively.

For $n = 3$ we consider the factorization of H_3 into two cubic factors (which covers all but one possibility, see (2.4)). Letting $H_3(x) = h(x)l(x)$, we obtain for the discriminant

$$d(H_3) = d(h)d(l)\,\mathrm{Res}(h,l)^2 \tag{5.7}$$

where $\mathrm{Res}(h,l)$ is the resultant of h and l ([20], section 27; [27], section 7.4). The polynomials h and l are normal, since $f(h) = h$ and $f(l) = l$ (with the notation of

Table 2.

n	$\delta(x)$
1	$x^2 - x + c$
2	$x - (c+1)$
3	$x^2 - (c+2)x + (c^3 + 2c^2 + c + 1)$
4	$x^3 + (c^2 - 3)x^2 + (-c^4 - c^3 + c^2 + 3)x - (c^6 + 3c^5 + 3c^4 + 3c^3 + 2c^2 + 1)$
5	$x^6 + k_5x^5 + k_4x^4 + k_3x^3 + k_2x^2 + k_1x + k_0$
	$k_5 = c^2 - c - 6;$
	$k_4 = 3c^5 + 3c^4 - 6c^3 - 2c^2 + 5c + 15;$
	$k_3 = 2c^7 + 9c^6 + 17c^5 + 21c^4 + 13c^3 - 2c^2 - 10c - 20;$
	$k_2 = 3c^{10} + 11c^9 + 6c^8 - 20c^7 - 42c^6 - 53c^5 - 37c^4 - 3c^3 + 8c^2 + 10c + 15;$
	$k_1 = c^{12} + 7c^{11} + 20c^{10} + 33c^9 + 40c^8 + 37c^7 + 21c^6 + 7c^5 - c^4 - 9c^3 - 7c^2 - 5c - 6;$
	$k_0 = c^{15} + 8c^{14} + 28c^{13} + 60c^{12} + 94c^{11} + 116c^{10} + 114c^9 + 94c^8 + 69c^7 + 44c^6$
	$+26c^5 + 14c^4 + 5c^3 + 2c^2 + c + 1.$

section 2). This means that their Galois group is either C_3, which contains only even permutations, or it is trivial if their roots are rational. In either case both $d(h)$ and $d(l)$ must be squares of rational numbers, and so must $d(H_3)$, from (5.7). The discriminant of H_3 is

$$d(H_3) = -(16c^2 + 4c + 7)^2(4c + 7)^3$$

which is the square of a rational number provided that $-(4c + 7)$ is, from unique factorization. Letting $4c + 7 = -(2k - 1)^2$, k rational, we obtain $c = -k^2 + k - 2$ (i.e. $c \leq -\frac{7}{4}$) and the factorization

$$H_3(x) = h_k(x)h_{1-k}(x) \qquad c = -k^2 + k - 2 \tag{5.8}$$

where

$$h_k(x) = x^3 + kx^2 - (k^2 - 2k + 3)x - (k^3 - 2k^2 + 3k - 1).$$

All factorizations considered here are exceptional in that in the intervals where they take place they have the density of the squares. In other words, H_n is irreducible with probability one.

For $n > 3$ the conditions for factorization become more stringent. Apart from the already known cases ($c = 0$ and $c = -2$), we have only found numerically seemingly isolated cases, such as $c = -5$ for $n = 4$.

6. The quadratic family: periodic orbits

In this section we apply the theory developed in the previous sections to the study of the periodic orbits of the quadratic family (5.1). Because the quadratic map depends on a single parameter, we may regard $f(x)$ as a map over the polynomial ring $\boldsymbol{Z}[c]$. When no value is specified, c should be regarded as an arbitrary complex number.

From table 1 and the results of section 3 we see that for periods less than 5 the equation $H_n(x) = 0$ is soluble by radicals. We compute the polynomial $w(\alpha_k) = s_0$, as defined in (4.6), and from it we calculate the multiplier polynomials $\delta(x)$ as the minimal polynomial of M (cf (4.7)). (Note that for computational purposes, exploiting the block structure of M is essential.) The results are reported in table 2.

The degree of δ is m, in agreement with the first column of table 1.

The δ-polynomial for $n = 5$ will be used at the end of this section. We first consider the case $n = 3$ in some detail. There are two orbits of period 3, whence $\delta(x)$ has degree 2. The discriminant of $\delta(x)$ is given by

$$d = -c^2(4c + 7). \tag{6.1}$$

For rational c, the multiplier of a periodic orbit of period 3 generates a quadratic extension $\boldsymbol{Q}(\sqrt{d})$ unless the parameter c is such that d is the square of a rational number. The determinant vanishes for $c = 0$ (the Bernoulli shift), and $c = -\frac{7}{4}$. In both cases H_3 factors. From the previous section we also know that H_3 factors when $c = -k^2+k-2$, k rational, and indeed for these values of c we have $d = d(k) = (2k-1)^2(k^2-k+2)^2$. Thus $\delta(x)$ is irreducible over $\boldsymbol{Q}$ when H_3 is, that is with probability one.

Besides the polynomial $\delta(x)$ for s_0, we compute those for s_1 and s_2 (cf (4.3)). By considering all possible triples of roots, we construct six distinct cubic polynomials $\gamma(x)$ from (4.3). Two of these have the periodic orbits of period three as roots. Once one of them is found (by trial an error, say), the other one is obtained applying the group G/D to the the s_i.

To give an idea of the expressions involved, we consider the parameter value $c = 1$. The polynomial H_3 reads

$$H_3(x) = x^6 + x^5 + 4x^4 + 3x^3 + 7x^2 + 4x + 5 \tag{6.2}$$

and the discriminant of $\delta(x)$ is $d = -11$. From (6.2) we see that the product of the points of the 3-cycles is the prime 5. The latter splits in $\boldsymbol{Z}(\sqrt{-11})$ (a principal ideal domain) into the product of two primes

$$5 = \pi_1\pi_2 = \left(\frac{3+\sqrt{-11}}{2}\right)\left(\frac{3-\sqrt{-11}}{2}\right). \tag{6.3}$$

By construction, $\pi_1\pi_2 = w(\alpha_1)w(\alpha_2)$ is the product of the roots of δ. From unique factorization and the fact that the units in $\boldsymbol{Z}(\sqrt{-11})$ are just ± 1, we conclude that the roots of $\delta(x)$ coincide with the prime factors of 5, with a possible sign difference. Verification shows that the sign agrees. Thus the primes π_i are the derivatives of the mapping $f(x) = x^2 + 1$ at the 3-cycles, divided by 2^3.

After computing the analogous solutions for s_1 and s_2, we construct the minimal polynomials $\gamma_{1,2}$ for α_1 and α_2 over Δ, as in (4.3)

$$\gamma_{1,2}(x) = x^3 + \frac{-1\pm\sqrt{-11}}{2}x^2 + \frac{1\mp\sqrt{-11}}{2}x^2 + \frac{3\pm\sqrt{-11}}{2} \tag{6.4}$$

whose solution gives an expression for a representative point for each orbit of period 3

$$\alpha_{1,2} = \frac{\pm 1}{6}\sqrt[3]{4\left(\pm 26 + 7\sqrt{-11} \pm 3\sqrt{3(-5\pm 8\sqrt{-11})}\right)}$$
$$\frac{\pm 1}{6}\sqrt[3]{4\left(\pm 26 + 7\sqrt{-11} \mp 3\sqrt{3(-5\pm 8\sqrt{-11})}\right)} \pm \frac{\sqrt{-11}}{6} - \frac{1}{6}. \tag{6.5}$$

The three points in an orbit correspond to the three choices of the cubic roots. The action of G/D interchanges the orbits, and it amounts to interchanging all $\pm$ signs (which is just complex conjugation).

We have seen that the splitting of the constant term of H_3 in the ring $Z[\sqrt{d}]$, with d given by (6.1), is closely related to the value of the multipliers. It must be pointed out, however, that this value is known only within a unit factor. Thus in the case of real fields (i.e. $c \leq -2$), where non-trivial units exist with absolute value different from 1, factorizations of the type (6.3) do not suffice to compute multipliers.

We now demonstrate that already for $n = 3$, the polynomial $H_n(x)$ may not give rise to normal extensions. From (2.5) we find that for $n = 3$, $\partial f = 2$ and H_n irreducible, $|G|$ cannot exceed 18. On the other hand $|G|$ is a multiple s of 6, the degree of H_3, and s must divide 3, the period. Thus $|G| = 6$ or 18. Because $G/D \cong C_2$, $G_1 = G_2 = D$, necessarily, so $|D|$ is either equal to 3 or to 9. In the former case $D = F \cong C_3$ and $G = C_6$ or S_3. In the latter case we have $D \cong C_3 \otimes C_3$, which means that $D \nsubseteq F$. We conclude that G is not Abelian, from proposition (iii) of section 3, and that it has a non-trivial centre, because the latter contains F. This suffices to establish that $G \cong C_3 \otimes S_3$ [28].

To decide among the possible Galois groups for $c = 1$, we factor $H_3(x)$ modulo a few primes p which are not discriminant divisors ([29], p 129). The discriminant of H_3 is equal to $-3^6 11^3$. For $p = 2$, H_3 is irreducible, so we gain no information. For $p = 5$ we obtain

$$H_3(x) \equiv x(x+3)(x+4)(x^3+4x^2+4x+2) \pmod 5 \tag{6.6}$$

and the appearance of irreducible factors of different degree indicates that the extension is not normal ([22], p 71), whence $|G| = 18$. The factorization (6.6) identifies the conjugacy class in G which fixes three roots of H_3 (the three linear factors), while permuting cyclically the other three (the cubic factor). It consists of the four generators of the subgroups L_1 and L_2, which we know to be non-trivial, since H_3 is not normal. Incidentally, this result implies that for $n = 3$ the estimate (2.5) cannot be strengthened.

We finally turn to the question of the solubility of the Galois group G, which was shown to coincide with that of the factor group G/D. When $n = 4$ we have $m = 3$ whence $G/D \cong C_3$ or S_3, which are soluble. When $n = 5$ we resort to computation. Using the expression for $\delta(x)$ displayed in table 2, we have computed G/D for all integral values of the parameter c less or equal to 100 in absolute value, using a procedure implemented in the algebraic manipulator MAPLE. In all cases (excluding $c = 0, -2$) the group G/D was found to be the symmetric group S_6 which is non-soluble, thereby establishing that the periodic orbits of period 5 of these systems cannot be expressed in terms of radicals.

7. Concluding remarks

We have studied the arithmetical properties of the periodic orbits of rational mappings, which lie in algebraic extensions of the field containing the parameters of the mapping. We have investigated the structure of these extensions by means of Galois theory, and addressed the classical question of solubility by radicals.

We have shown that the solubility of a periodic orbit in terms of radicals is (essentially) equivalent to that of its multiplier. We have developed an algorithm to compute the multipliers' minimal polynomials, which we have applied to the quadratic mapping. By determining the corresponding Galois groups, we have provided examples of orbits that cannot be expressed in term of radicals. These were periodic orbits of period 5 for some integral value of the parameter. This result does not preclude the possibility that particular parameter values may yield mappings with radical periodic orbits of large period. However, it seems unlikely that radical expressions will be a commonplace for orbits of large period.

In some cases solubility by radicals can be extended beyond periodic orbits. If the inverses f^{-1} of a rational mapping f can be expressed in terms of radicals (for instance when the degree of f is less or equal to four), the pre-images of periodic points lie in radical extensions of the field containing the periodic orbits. In this way a large family of points of Julia sets can be computed symbolically.

The computation of the δ-polynomials involves finding the determinant of a matrix M of size mn (cf (4.7)). Even if one exploits the block structure of M, the calculations become rapidly very substantial. A precise assessment of the computational complexity of this problem is not straightforward (there are also other types of algorithms), but it seems unlikely that this approach could replace the direct one in asymptotic computations, given the present developement of the theory. This question is currently being investigated.

Methods for computing statistical quantities from periodic orbits have been recently developed, based on the zeta function formalism [15]. Some zeta functions involve only information about multipliers of an orbit rather than the orbit itself, for instance in the stability of Julia sets. The use of δ-type polynomials seems appropriate for an algebraic development of this subject.

Acknowledgments

We thank Leonard Soicher for several clarifying comments, Patrick Morton for spotting an omission in section 6, and R W K Odoni for bringing references [17] and [18] to our attention. Many useful remarks of Predrag Cvitanović and Ian Percival have helped us improve the clarity of the manuscript. This work was supported by the Nuffield Foundation. One of us (SH) thanks SERC for partial support.

Appendix 1. Glossary of Galois theory

A *field* is a set equipped with two binary operations, called sum and multiplication, satisfying the commutative, associative and distributive properties of the corresponding operations among rationals. Let K be a field and $K[x]$ the set of polynomials with coefficients in K. The polynomial f is *monic* if it has unit leading coefficient and *irreducible* if $f = hg$ implies that g or h is constant.

Let f be irreducible and let $f(\alpha) = 0$. The set of all rational epressions in α with coefficients in K form a field, denoted by $K(\alpha)$. Clearly $K \subset K(\alpha)$. If f has degree n, $K(\alpha)$ consists of all linear combinations

$$\xi = k_0 + k_1\alpha + k_2\alpha^2 + \cdots + k_{n-1}\alpha^{n-1} \qquad k_i \in K$$

and every $\xi \in K$ admits a unique representation of this type. Thus $K(\alpha)$ is an n-dimensional linear space over K, called an *algebraic extension* of K. If L is an extension of K one writes $L : K$. The *minimal polynomial* for $\alpha \in L$ over K is the monic polynomial $f \in K[x]$ of smallest degree having α as a root.

Two algebraic numbers α_1 and α_2 are *conjugate* if they are roots of the same irreducible polynomial over K. The corresponding extensions $K(\alpha_1)$ and $K(\alpha_2)$ are also called conjugate.

A polynomial f *splits* in L, if L contains all its roots. The smallest field where f splits is called the *splitting field* of f. An extension $L : K$ is *normal* if any irreducible polynomial over K with a root in L splits in L. An extension is *separable* if for each $\alpha \in L$ the minimal polynomial for α over K has no multiple roots. A normal and separable extension is called a *Galois extension.*

An *automorphism* σ of a field K is a bijection of K into itself preserving both addition and multiplication: $\sigma(\alpha+\beta) = \sigma(\alpha)+\sigma(\beta)$ and $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$, for all α and β in K.

If $L : K$ is a Galois extension, the *Galois group* G is the set of automorphisms of L leaving each element of K fixed. The *order* (number of elements) $|G|$ of G is equal to the degree of the extension. An extension if *cyclic* if its Galois group is cyclic.

To each subgroup D of G we associate its *fixed field* $\mathrm{Fix}(D)$, which is the collection of the points of L that are invariant under all automorphisms of D. Thus K is the fixed field of G and L that of the identity. Conversely, to each subfield F of L we associate the largest subgroup F^* of G which leaves all its points invariant. The main theorem of Galois theory asserts that

$$D = (\mathrm{Fix}(D))^* \qquad F = \mathrm{Fix}(F^*).$$

In addition, D is a normal subgroup of G if and only if $\mathrm{Fix}(D)$ is a normal extension of K, in which case the Galois group of $\mathrm{Fix}(D)$ over K is isomorphic to the quotient group G/D.

Appendix 2.

We prove the propositions (i)–(iv) of section 3.

Proof of (i). Let $g \in G_k$. Then g restricts to f^{l_k} over Ω_k, so that $g = (gf^{-l_k})f^{l_k}$. We have $gf^{-l_k} \in L_k$ and $fl_k \in D$, by assumption, i.e. $L_kD = G_k$.

Proof of (ii). We note that if $D = F$ then $L_k \cap D = 1$, because the only element of F fixing the kth orbit is the identity, since all orbits have the same period. The assertion now follows from (i) and the fact that both L_k and D are normal subgroups of G_k.

Proof of (iii). The group F is represented in O as the submodule O_F generated by the vector $(1,1,\ldots,1)$. Assume that $\phi(D)$ is not contained in O_F. Then D contains an element d with $\phi(d) = (l_1,\ldots,l_m)$, such that at least two indices l_r and l_s are not congruent modulo n. Choose any $\alpha \in \Omega_r$ and $\beta \in \Omega_s$, and $g \in G$ such that $g(\alpha) = \beta$. We have

$$gd(\alpha) = gf^{l_r}(\alpha) = f^{l_r}(g(\alpha)) = f^{l_r}(\beta)$$

$$dg(\alpha) = d(\beta) = f^{l_s}(\beta)$$

and our assertion is proved.

Proof of (iv). From (3.2) it follows that $G_k = D$ if and only if all G_k coincide and are normal subgroups of G. But then G_k fixes a block if and only if it fixes all of them, that is G/D is a *regular* permutation of the blocks, and because it is transitive, its order is equal to the number m of blocks. Conversely, if $G/D = m$ then it is regular, which means that the only block stabilizer is the identity.

References

[1] Ford J 1983 How random is a coin toss? *Physics Today* **36** 40–7

[2] Knuth D E 1981 *The Art of Computer Programming* (Reading, MA: Addison-Wesley)

[3] Rannou F 1974 Numerical studies of discrete plane area-preserving mappings *Astron. Astrophys.* **31** 289–301

[4] Chirikov B V, Izrailev F M and Shepelyansky D L 1981 Dynamical stochasticity in classical and quantum mechanics *Soviet Scientific Reviews C* vol 2 (New York: Gordon and Breach) pp 209–67

[5] Karney C F F 1983 Long time correlations in the stochastic regime *Physica* **8D** 360–80

[6] Smith L A and Spiegel E A 1987 Strange accumulators *Ann. Phys., NY* **497** 61–5

[7] Kaneko K 1988 Symplectic cellular automata *Phys. Lett.* **129A** 9–16

[8] Earn D J D and Tremaine S 1992 Exact numerical studies of Hamiltonian maps: iterating without roundoff errors *Physica* **56D** 1–22

[9] Grebogi C, Hammel S M, Yorke J A and Sauer T 1990 Shadowing of physical trajectories in chaotic dynamics: containment and refinement *Phys. Rev. Lett.* **65** 1527–30

[10] Farmer J D and Sidorowich J J 1991 Optimal shadowing and noise reduction *Physica* **47D** 373–92

[11] Davenport H, Siret Y and Tournier E 1988 *Computer Algebra* (London: Academic)

[12] Percival I C and Vivaldi F 1987 Arithmetical properties of strongly chaotic motions *Physica* **25D** 105–30

[13] Bartuccelli M and Vivaldi F 1989 Ideal orbits of toral automorphisms *Physica* **39D** 194–204

[14] Vivaldi F 1992 Geometry of linear maps over finite fields *Nonlinearity* **5** 133–47

[15] Artuso R, Aurell E and Cvitanović P 1990 Recycling strange sets: I. Cycle expansions *Nonlinearity* **3** 325–59; 1990 Recycling strange sets: II. Applications *Nonlinearity* **3** 361–86

[16] Stewart I 1989 *Galois Theory* (London: Chapman and Hall)

[17] Morton P and Patel P 1991 The Galois theory of periodic points of polynomial maps *Preprint* Wellesley, MA

[18] Morton P 1991 Arithmetic properties of periodic points of quadratic maps *Preprint* Wellesley, MA

[19] Apostol T A 1984 *Introduction to Analytic Number Theory* (New York: Springer)

[20] van der Waerden B L 1953 *Modern Algebra* vol 1 (New York: Ungar)

[21] Dixon J D 1990 Computing subfields in algebraic number fields *J. Austral. Math. Soc.* **49** 434–48

[22] Marcus D A 1977 *Number Fields* (New York: Springer)

[23] Hartley B and Hawkes T O 1970 *Rings, Modules and Linear Algebra* (London: Chapman and Hall)

[24] Samuel P 1970 *Algebraic Theory of Numbers* (Paris: Hermann)

[25] Ribenboim P 1988 *The Book of Prime Number Records* (New York: Springer)

[26] Niven I 1956 *Irrational Numbers* (Washington, DC: The Mathematical Association of America)

[27] Cohn P M 1974 *Algebra* vol 1 (London: Wiley)

[28] Thomas A D and Wood G V 1980 *Group Tables* (Orpington, Kent: Shiva)

[29] Pohst M and Zassenhaus H 1989 *Algorithmic Algebraic Number Theory* (Cambridge: Cambridge University Press)