Acta Math., 163 (1989), 151–180

Solving the quintic by iteration

by

PETER DOYLE[1] and CURT McMULLEN[2]

Princeton University
Princeton, NJ, U.S.A.

Princeton University
Princeton, NJ, U.S.A.

1. Introduction

According to Dickson, Euler believed every algebraic equation was solvable by radicals [2]. The quadratic formula was known to the Babylonians; solutions of cubic and quartic polynomials by radicals were given by Scipione del Ferro, Tartaglia, Cardano and Ferrari in the mid-1500s. Abel's proof of the insolvability of the general quintic polynomial appeared in 1826 [1]; later Galois gave the exact criterion for an equation to be solvable by radicals: its Galois group must be solvable. (For a more complete historical account of the theory of equations, see van der Waerden [20], [21].)

In this paper, we consider solving equations using *generally convergent purely iterative algorithms*, defined by Smale [17]. Such an algorithm assigns to its input data v a rational map $T_v(z)$, such that $T_v^n(z)$ converges for almost all v and z; the limit point is the *output* of the algorithm.

This context includes the classical theory of solution by radicals, since nth roots can be reliably extracted by Newton's method.

In [12] a rigidity theorem is established that implies the maps $T_v(z)$ for varying v are all conformally conjugate to a fixed model $f(z)$. Thus the Galois theory of the output of T must be implemented by the conformal automorphism group $\mathrm{Aut}(f)$, a finite group of Möbius transformations.

The classification of such groups is well-known: $\mathrm{Aut}(f)$ is either a cyclic group, dihedral group, or the group of symmetries of a regular tetrahedron, octahedron or

[1] On leave from Bell Labs; research supported by an N.S.F. Postdoctoral Fellowship.

[2] Research supported by the Institute for Advanced Study.

icosahedron. Of these, all but the icosahedral group are solvable, leading to the necessary condition:

An equation is solvable by a tower of algorithms only if its Galois group G is *nearly solvable*, i.e. admits a subnormal series

$$G = G_n \rhd G_{n-1} \rhd \ldots \rhd G_1 = \mathrm{id}$$

such that each G_{i+1}/G_i is either cyclic or A_5. Incomputability of the sextic and higher polynomials follows as in ordinary Galois theory.

This necessary condition proves also *sufficient*; in particular, *the quintic equation can be solved by a tower of algorithms.*

The quintic equation and the icosahedron are of course discussed at length in Klein's treatise [10] (see also Klein [8], Dickson [2], Green [5], and especially Serre's letter to J.D. Gray [14]). Our solution relies on the classical reduction of the quintic equation to the icosahedral equation, but replaces the transcendental inversion of the latter (due to Hermite and Kronecker) with a purely iterative algorithm.

To exhibit this method, we must construct rational maps with the symmetries of the icosahedron. It proves useful to think of a rational map $f(z)$ on $\hat{\mathbf{C}}$, symmetric with respect to a finite group $\Gamma \subset \mathrm{PSL}_2\mathbf{C}$, as a projective class of *homogeneous* 1-*forms* on $\mathbf{C}^2$, invariant with respect to the linear group $\tilde{\Gamma} \subset \mathrm{SL}_2\mathbf{C}$. Then exterior algebra can be used to describe the space of all such maps in terms of the classical theory of invariant polynomials.

From this point of view, a rational map of degree n is canonically associated to any $(n+1)$-tuple of points on the sphere, and inherits the symmetries of the latter. The iterative scheme we use to solve the quintic relies on the map of degree 11 associated to the 12 vertices of the icosahedron. Its Julia set is rendered in Figure 1; every initial guess in the white region (which has full measure) converges to one of the 20 vertices of the dual dodecahedron.

Outline of the paper. §2 develops background in algebra and geometry. §3 introduces purely iterative algorithms, and §4 characterizes computable fields, given the existence of a certain symmetric rational map. §5 contains a description of all rational maps with given symmetries, which completes the proof and leads to an explicit algorithm for solving quintic equations, computed in the Appendix.

Remarks. (1) Comparison should be made with the work of Shub and Smale [16] in which successful *real algebraic* algorithms are constructed for a wide class of problems (in particular, finding the common zeros of n polynomials in n variables with no

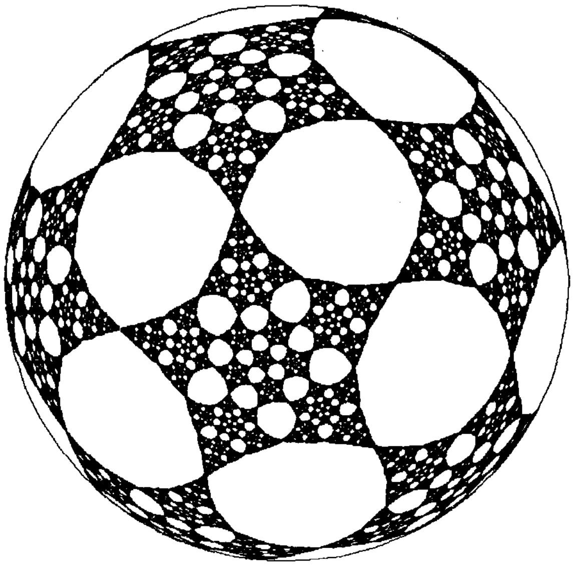

Fig. 1. An icosahedral iterative scheme for solving the quintic.

restrictions on degree). These algorithms exhibit much of the flexibility of smooth dynamical systems (in fact they are discrete approximations to the Newton vector field).

(2) One can also consider more powerful algorithms which are still complex algebraic, e.g. by allowing more than one number to be updated during iterations. Tools for pursuing this direction (such as the theory of iterated rational functions on $\mathbf{P}^n$, $n>1$) have yet to be fully developed.

2. Galois theory of rigid correspondences

In this section we set up the Galois theory and birational geometry that will be used to describe those field extensions that can be reached by a tower of generally convergent algorithms.

All varieties will be irreducible and complex projective. Let V be a variety, $k=K(V)$ its function field.

An irreducible polynomial p in $k[z]$ determines a finite field extension $k(\alpha)$, where α is a root of p; the extension is unique up to isomorphism over k.

To obtain a geometric picture for the field extension, consider $p(z)$ as a family of polynomials $p_v(z)$ whose coefficients are rational functions of v. The polynomial p determines a subvariety $W\subset V\times\hat{\mathbf{C}}$ which is the closure of the set of (v,z) such that $p_v(z)=0$. The function field $K(W)=k(\alpha)$ where α denotes the rational function obtained by projecting W to $\hat{\mathbf{C}}$.

W may be thought of as the graph of a multi-valued function $W(v)$ which sends v to the roots of p_v. We call such a multi-valued map a *rational correspondence*.

We say W is a *rigid correspondence* if its set of values assumes only one conformal configuration on the Riemann sphere: i.e. there exists a finite set $A\subset\hat{\mathbf{C}}$ such that the set $W(v)$ is equal to $\gamma(A)$ for some Möbius transformation γ depending on v. In this case we say the field extension $k(\alpha)$ is a *rigid extension*.

Now let k' denote a finite Galois extension of k with Galois group G.

THEOREM 2.1. *The field extension k'/k is the splitting field of a rigid extension if and only if there exists:*

(a) *a faithful homomorphism $\varrho:G\rightarrow \mathrm{PSL}_2\mathbf{C}$ and*

(b) *an element ϕ in $\mathrm{PSL}_2(k')$ such that*

(c) *$\phi^g=\varrho(g)\circ\phi$ for all g in G.*

Proof. Let k' be the splitting field of a rigid correspondence $k(\alpha)$. For simplicity, assume $[k(\alpha):k]$ is at least 3. Let α_i, $i=1,2,3$ denote three distinct conjugates of α under G. $\mathrm{PSL}_2(k')$ acts triply transitively on the projective line $\mathbf{P}(k'^2)\supset\mathbf{P}(\mathbf{C}^2)=\hat{\mathbf{C}}$; take ϕ to be the unique group element which moves $(\alpha_1,\alpha_2,\alpha_3)$ to $(0,1,\infty)$.

We claim that $\phi(\alpha^g)$ is in $\hat{\mathbf{C}}$ for all g in G. Indeed, $\phi(\alpha^g)$ is just the cross-ratio of α^g and $(\alpha_1,\alpha_2,\alpha_3)$, which is constant by rigidity. Let $A=\phi(\alpha^G)$ be the image under ϕ of the conjugates of α.

Define $\varrho(g)=\phi^g\circ\phi^{-1}$. Then $\varrho(g)$ permutes A, so it is an element of $\mathrm{PSL}_2\mathbf{C}$. Because G acts trivially on $\mathrm{PSL}_2\mathbf{C}$, ϱ is a homomorphism; e.g.

$$\phi^g\circ\phi^{-1}\circ\phi^h\circ\phi^{-1}=(\phi^g\circ\phi^{-1})^h\circ\phi^h\circ\phi^{-1}=\phi^{gh}\circ\phi^{-1}$$

and since $\varrho(g)$ fixes A pointwise only if g fixes the conjugates of α, it is faithful; thus we have verified (a)–(c).

Conversely, given the data (a)–(c), set $\alpha=\phi^{-1}(x)$ for any x in $\hat{\mathbf{C}}$ with trivial stabilizer in $\varrho(G)$; then α is rigid over k and $k'=k(\alpha)$. □

Cohomological interpretation. The map ϱ determines an element $[\varrho]$ of the Galois cohomology group $H^1(G,\mathrm{PSL}_2k')$, which is naturally a subgroup of the Brauer group of k; condition (c) simply says ϱ is the coboundary of ϕ, so $[\varrho]=0$.

A geometric formulation of the vanishing of this class is the following. Let $W \to V$ denote the rational map of varieties corresponding to the field extension $k \subset k'$. Form the *Severi-Brauer* variety $P_\varrho = (W \times \hat{\mathbf{C}})/G$, where G acts on W by birational transformations and on $\hat{\mathbf{C}}$ via the representation ϱ. Then $P_\varrho \to V$ is a flat $\hat{\mathbf{C}}$ bundle outside the branch locus of the map $W \to V$. We can factor $W \to V$ through the inclusion $W \cong W \times \{x\} \subset P_\varrho$ for any x in $\hat{\mathbf{C}}$ with trivial stabilizer.

The cohomology class of ϱ vanishes if and only if P_ϱ is birational to $V \times \hat{\mathbf{C}}$; in which case $W \subset P_\varrho \cong V \times \hat{\mathbf{C}}$ presents W as a rigid correspondence.

More on Galois cohomology and interpretations of the Brauer group can be found in papers of Grothendieck [6], [7] and Serre's book [15].

3. Purely iterative algorithms

In this section, generally convergent purely iterative algorithms are introduced and we prove that the correspondences they compute are rigid.

Definitions. A *purely iterative algorithm* $T_v(z)$ is a rational map

$$T: V \to \mathrm{Rat}_d$$

carrying the *input variety* V into the space Rat_d of rational endomorphisms of the Riemann sphere of degree d. To avoid special considerations of 'elementary rational maps', we will always assume that d is >1.

Let k denote the function field $K(V)$; then T is simply an element of $k(z)$.

The algorithm is *generally convergent* if $T_v^n(z)$ converges for all (v, z) in an open dense subset of $V \times \hat{\mathbf{C}}$. (Here T^n denotes the nth iterate of the map T.)

The map $T_v(z)$ can be thought of as a fixed procedure for improving the *initial guess* z. The *output* of the algorithm is described by the set

$$W = \{(v, z) \in V \times \hat{\mathbf{C}} \mid z \text{ is the limit of } T_v^n(w) \text{ for some open set of } w\}.$$

Since different w may converge to different limits, the output can be multivalued.

A family of rational maps is *rigid* if there is a fixed rational map $f(z)$ such that T_v is conjugate to $f(z)$ for all v in a Zariski open subset of V.

THEOREM 3.1. *A generally convergent algorithm is a rigid family of rational maps.*

This is a consequence of the general rigidity theorem for stable algebraic families, exactly as in [12], Theorem 1.1.

COROLLARY 3.2. *The output of a purely iterative algorithm is a finite union of rigid correspondences.*

Proof. The output W is a finite union of components of the algebraic set $\{(v, z)| T_v(z)=z\}$; each component is a variety. The Möbius transformation conjugating T_v to the fixed model $f(z)$ carries the output of T_v to the attractor A of f, so each component is a rigid correspondence. □

To make examples of generally convergent algorithms, one must check that a given iteration will converge for most initial guesses. Here is one special but useful criterion. A rational map $f(z)$ is *critically finite* if every critical point c is eventually periodic (there exist $n>m>0$ such that $f^n(c)=f^m(c)$). A periodic cycle which includes a critical point is said to be *superattracting*.

THEOREM 3.3. *Let $f(z)$ be a critically finite rational map, A the union of its superattracting cycles. Then either*

(a) *A is empty and the action of f on $\hat{\mathbf{C}}$ is ergodic, or*

(b) *A is nonempty, and $f^n(z)$ tends to a cycle of A for all z in an open, full measure subset of $\hat{\mathbf{C}}$.*

In case every critical point eventually lands in A, $f(z)$ belongs to the general class of 'expanding' rational maps, for which the result is proven by Sullivan [18]. The general case can be handled similarly, using orbifolds. This is sketched for polynomials by Douady and Hubbard [3]; the orbifold approach for general critically finite maps is discussed by Thurston [19].

All examples of generally convergent algorithms we will consider employ critically finite maps. In practical terms, these maps have two benefits: convergence is assured almost everywhere, not just on an open dense set; and convergence is asymptotically quadratic (for a fixed convergent initial guess, 2^N digits of accuracy are obtained in $O(N)$ iterations).

Examples of purely iterative algorithms. (1) *Newton's method.* Let $V=\mathrm{Poly}_d$ and let $T_p(z)=z-p(z)/p'(z)$. Then T is a purely iterative algorithm, and it is generally convergent for $d=2$ but not for $d=3$ or more (Figure 2; see also Smale [17]).

(2) *Extracting radicals.* Let $V\subset\mathrm{Poly}_d$ denote the set of polynomials $\{p(X)=X^d-a| a\in\mathbf{C}\}$. The restriction of Newton's method to V is generally convergent; thus one can reliably extract radicals. The critical points of T_p occur at the roots of p (which are fixed) and at $z=0$ (which maps to ∞ under one iteration, and then remains fixed); thus

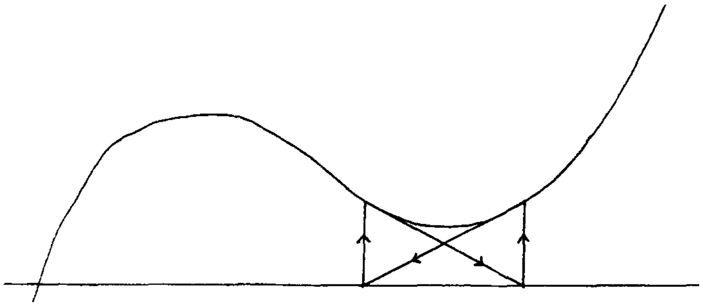

Fig. 2. Newton's method can fail for cubics.

T_p is critically finite, and by Theorem 3.3, almost every initial guess converges to a root.

Rigidity of the algorithm T_p is easily verified, using the *affine invariance* of Newton's method.

(3) *Solving the cubic.* The roots of $p(X)=X^3+aX+b$ can be reliably determined by applying Newton's method to the rational function

$$r(X)=\frac{(X^3+aX+b)}{(3aX^2+9bX-a^2)}.$$

The critical points of T_p coincide with the roots of p, and are fixed, so again Theorem 3.3 may be applied to verify convergence.

(4) *Insolvability of the quartic.* Since the roots of two quartics are generally not related by a Möbius transformation (the cross-ratio of the roots must agree), the roots of polynomials of degree 4 (or more) cannot be computed by a generally convergent algorithm.

A more topological discussion of the insolvability of the quartic, using braids, appears in [11].

4. Towers of algorithms

Let V be a variety, k its function field. From a computational point of view, k is the set of all possible outputs of decision-free algorithms which perform a finite number of arithmetic operations on their input data. The graph of an element of k in $V\times\hat{\mathbf{C}}$ describes the output of such an algorithm.

Let T be a generally convergent algorithm with output $W\subset V\times\hat{\mathbf{C}}$. Assume for simplicity that W is irreducible, and let $k \subset k(\alpha)$ be the corresponding field extension. Then elements of $k(\alpha)$ describe all possible outputs which are computed rationally from the output of T and the original input data. We refer to $k(\alpha)$ as the *output field* of T.

If W is reducible then T has an output field for each component of W. All algorithms which we consider explicitly will have irreducible output.

If $f(z)$ is a rational map, let $\mathrm{Aut}(f)$ denote the group of Möbius transformations commuting with f. If Γ is a group acting on a set, $\mathrm{Stab}(a,\Gamma)$ will denote the subgroup stabilizing the point a.

THEOREM 4.1. *Every generally convergent algorithm T in $k(z)$ can be described by the following data:*

(a) *A rational map $f(z)$ and a finite set $A \subset \hat{\mathbf{C}}$ such that $f^n(z)$ converges to a point of A for all z in an open dense set; and*

(b) *A finite Galois extension k'/k with Galois group G, an isomorphism $\varrho : G \rightarrow \Gamma \subset \mathrm{Aut}(f)$ and an element ϕ in $\mathrm{PSL}_2(k')$; such that*

(c) *$\phi^g = \varrho(g) \circ \phi$ for all g in G; and*

(d) *$T = \phi^{-1} \circ f \circ \phi$.*

The output fields of T are the fixed fields of $\varrho^{-1}\,\mathrm{Stab}(a,\Gamma)$, as a ranges over the points of A. If Γ acts transitively on A then the output of T is irreducible and the output field is unique up to isomorphism over k.

Proof. Given the rigidity of generally convergent algorithms, the proof follows the same lines as Theorem 2.1. □

A *tower of algorithms* is a finite sequence of generally convergent algorithms, linked together serially, so the output of one or more can be used to compute the input to the next. The final output of the tower is a single number, computed rationally from the original input and the outputs of the intermediate generally convergent algorithms.

A tower is described by rational maps $T_1(z), \ldots, T_n(z)$ and fields $k = k_1 \subset k_2 \subset \ldots \subset k_n$ such that T_i is an element of $k_i(z)$, and $k_{i+1}(z)$ is one of the output fields of T_i. The field k_n is the *final output field* of the tower. The field extension k'/k is *computable* if it is isomorphic over k to a subfield of k_n for some tower of algorithms.

If we require that every algorithm employed has irreducible output, then there is a one-to-one correspondence between the elements of all computable fields over k, and the 'graphs' $W \subset V \times \hat{\mathbf{C}}$ of the final output of all towers of algorithms. In general, if W is reducible, then each component of W corresponds to an element of a computable field.

Our main goal is to characterize computable field extensions.

Möbius groups. S_d and A_d will denote the symmetric and alternating groups on d symbols. Let $\Gamma \subset \mathrm{PSL}_2\mathbf{C}$ be a finite group of Möbius transformations. As an abstract group, Γ is either a cyclic group, a dihedral group, the tetrahedral group A_4, the octahedral group S_4, or the icosahedral group A_5. We refer to such groups as Möbius groups. Note that

(1) any subgroup or quotient of a Möbius group is again a Möbius group; and

(2) every Möbius group other than A_5 is solvable.

Near solvability. Suppose a group G admits a subnormal series

$$G = G_n \rhd G_{n-1} \rhd \ldots \rhd G_1 = \mathrm{id}$$

such that each G_{i+1}/G_i is a Möbius group. By (2) the series may be refined so that successive quotients are either abelian or A_5. We will say such a group is *nearly solvable*. By (1) any quotient or subgroup of a nearly solvable group is also nearly solvable.

THEOREM 4.2. *A field extension k'/k is computable if and only if the Galois group of its splitting field is nearly solvable.*

Since S_n is nearly solvable if and only if $n \leqslant 5$, we have the immediate:

COROLLARY 4.3. *Roots of polynomials of degree d can be computed by a tower of algorithms if and only if $d \leqslant 5$.*

Proof of Theorem 4.2: *one direction.* Suppose k' is computable. Let $k_1 \subset k_2 \subset \ldots \subset k_n$ be a tower of output fields such that k' is isomorphic over k to a subfield of k_n. Define inductively k'_{i+1} to be the splitting field of k_{i+1} over k'_i, and let

$$G = G_n \rhd G_{n-1} \rhd \ldots \rhd G_1 = \mathrm{id}$$

be the corresponding subnormal series for $G = \mathrm{Gal}(k'_n/k)$. G_i/G_{i+1} is the same as the Galois group of k'_{i+1}/k'_i, which faithfully restricts to a subgroup of the Galois group of the splitting field of k_{i+1} over k_i. By Theorem 4.1, the latter group is isomorphic to a finite group of Möbius transformations, so G is nearly solvable. □

To complete the proof we must exhibit algorithms for producing field extensions. It turns out that, in addition to the basic tool of Newton's method for radicals, only one other generally convergent algorithm is required.

LEMMA 4.4. *If k'/k is a cyclic Galois extension, then k' is computable.*

Proof. Since k contains all roots of unity, $k'=k(\alpha)$ for some element α such that α^n is in k. As we have seen, Newton's method is generally convergent when applied to extract nth roots. Thus k' is the output field to T in $k(z)$ where T is Newton's method applied to the polynomial $X^n-\alpha^n$.

LEMMA 4.5 (*Existence of an icosahedral algorithm*). *There is a critically finite rational map $f(z)$ with* Aut(f) *isomorphic to A_5, whose superattracting fixed points A comprise a single orbit under A_5 with stabilizer A_3.*

This will be established in the following section.

LEMMA 4.6. *If k'/k is a Galois extension with Galois group $G=A_5$, then k' is computable.*

Proof. To construct an algorithm to compute k', we need only provide data as in (a) and (b) of Theorem 4.1. For $f(z)$, we take the rational map given by the preceding lemma, and A its superattracting fixed points. Since f is critically finite, Theorem 3.3 guarantees an open, full measure set of z converge to A.

Let ϱ be any isomorphism between G and Aut(f). As shown in Serre's letter [14], there is a degree 2 cyclic extension of k in which the cohomology class $[\varrho]$ becomes trivial. Since cyclic extensions are computable, we may assume this is true in our original field k. Thus there is an element ϕ such that $\phi^g=\varrho(g)\circ\phi$, and $T=\phi^{-1}\circ f\circ\phi$ is a generally convergent algorithm over k.

Since the stabilizer of a point in A is an A_3 subgroup of A_5, the output field to T is the fixed field of A_3. As k' is a cyclic extension of this fixed field, it is computable. □

The result of Serre's quoted above has been generalized by Merkurev and Suslin to show that any Severi-Brauer variety has a solvable splitting field [13]. (This reference was supplied by P. Deligne.)

The lemma can also be established somewhat less conceptually without appeal to [14]. Any element α generating the fixed field of $A_4 \subset A_5$ satisfies a quintic polynomial $p(z)$ in $k(z)$. Since A_4 is solvable, to compute the extension k' it suffices to compute a root of p.

In the Appendix we will give an explicit algorithm for solving quintic polynomials. To carry out the solution, the quintic must be normalized so that Σr_i and Σr_i^2 are both equal to zero, where r_i denote the roots of p. This normalization is easily carried out by a Tschirnhaus transformation, but it requires the computation of a square root. The square root, which Klein calls the 'accessory irrationality', furnishes the predicted degree 2 extension.

Completion of the proof of Theorem 4.2. Replacing k' by its splitting field, we may assume k'/k is Galois with nearly solvable Galois group. Then k' is obtained from k by a sequence of Galois extensions, each of which is cyclic or A_5. By the preceding lemmas, each such extension is computable, so k' is computable as well. □

Remark on the quartic. Let $k'=\mathbf{C}(r_1, r_2, r_3, r_4)$, and let k be the subfield of symmetric functions. Then the problem of computing k'/k is the same as that of finding the roots of a general fourth degree polynomial. Since the Galois group G here is S_4, Theorem 4.2 guarantees this is possible by a tower of algorithms.

S_4 is actually isomorphic to a Möbius group, namely the symmetries of an octahedron, or its dual, a cube. Is k' the output field of a generally convergent algorithm? If so, the roots of quartic polynomials would be computable as *rational functions* of the output of a *single* purely iterative algorithm (we have already seen the roots cannot actually be the *output* of such an algorithm).

Unfortunately, this is impossible; although the Galois group is isomorphic to a Möbius group, the potential obstruction in Galois cohomology is nonzero, and k'/k is *not a rigid extension*.

The analogous case of polynomials of degree 5 is discussed by Serre [14]. Here we will sketch a picture of the obstruction from a topological point of view.

The field extension k'/k corresponds to the rational map $\mathrm{Roots}_4 \to \mathrm{Poly}_4$ from the space of roots to the space of polynomials. Let $\varrho: G \to \Gamma$ be an isomorphism between the Galois group G of k'/k and the octahedral group $\Gamma \subset \mathrm{PSL}_2\mathbf{C}$.

If k'/k is rigid, then the Severi-Brauer variety $P_\varrho \to \mathrm{Poly}_4$ associated to ϱ is birational to the product $\mathrm{Poly}_4 \times \hat{\mathbf{C}}$.

Now P_ϱ is a flat $\hat{\mathbf{C}}$ bundle outside of the branch locus of the map $\mathrm{Roots}_4 \to \mathrm{Poly}_4$, which is the subvariety Δ of polynomials with vanishing discriminant. The fundamental group $\pi_1(\mathrm{Poly}_4 - \Delta, p)$ is naturally identified with B_4, the braid group of four points in the plane: Over a loop based at p, the roots of $p(z)$ move without collision and return to their original positions, describing a braid.

There is a natural map $B_4 \to G \cong S_4$ which records how the roots of p are permuted by the braid. Under the identification $\varrho: G \to \Gamma$, this map records how the fiber of P_ϱ is twisted by monodromy along a loop.

If P_ϱ is birational to the trivial bundle, then its restriction to some Zariski open subset U is topologically trivial. If that subset were as large as possible—i.e., if U were

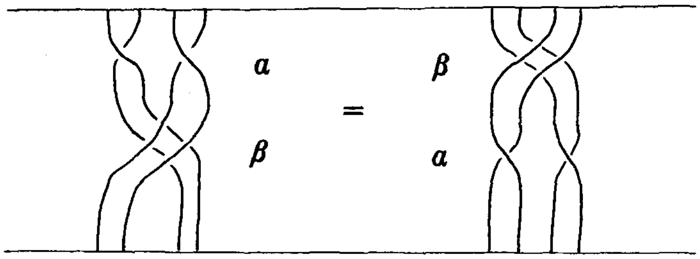

Fig. 3. Commuting braids.

equal to the complement of the discriminant locus—then it would be possible to lift the map $B_4 \to \Gamma$ to $\tilde{\Gamma} \subset SL_2\mathbf{C}$, a two-fold cover of Γ.

But this is impossible: There are two commuting elements α and β in the braid group (see Figure 3), whose images in Γ (thought of as Euclidean symmetries of a cube) are 180° rotations about perpendicular axes. Such rotations cannot be lifted to commuting elements of $\tilde{\Gamma}$.

There is a torus in the complement of Δ whose fundamental group is generated by α and β. One can show that this torus can be moved slightly to avoid any finite set of other hypersurfaces in Poly_4. Thus the obstruction persists on any Zariski open set, and P_ϱ is not birationally trivial.

5. Rational maps with symmetry

To compute A_5 extensions, one must use rational maps with icosahedral symmetry. In this section we will construct all rational maps with given symmetries, using invariant polynomials. We then give a conceptual proof of the existence of the map claimed in Lemma 4.5, and also obtain concrete formulas for use in the solution of the quintic.

Let Γ be a finite group of Möbius transformations. How can we construct rational maps such that $\text{Aut}(f) \supset \Gamma$?

Here are three ways to construct such f.

I. *Projectively natural Newton's method.* Ordinary Newton's method applied to a rational function $p(z)$ can be thought of as the map which sends z to $A(z)^{-1}(0)$, where $A(z)$ is the unique automorphism of $\mathbf{C}$ whose 1-jet matches that of p at z. If one replaces $A(z)$ by the unique Möbius transformation of $\hat{\mathbf{C}}$ whose 2-jet agrees with that of p, then

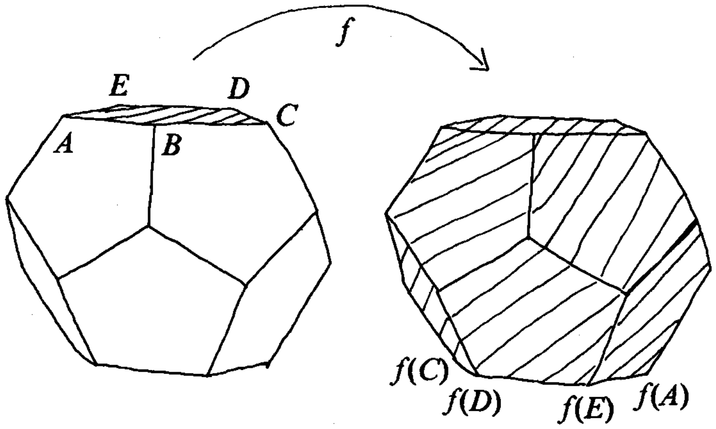

Fig. 4. Geometric construction of a rational map.

the resulting iteration,

$$N_p(z) = z - \frac{p(z)p'(z)}{p'(z)^2 - \frac{1}{2}p''(z)p(z)}$$

is 'projectively natural', in the sense that $N_{po\gamma}(\gamma z) = \gamma \circ N_p(z)$ for any Möbius transformation γ. Thus $\mathrm{Aut}(N_p)$ contains Γ whenever $p(z)$ is Γ-invariant (and such p are easily constructed).

II. *Geometric constructions.* Consider, for example, the case of the icosahedral group. Tile the Riemann sphere by congruent spherical pentagons, in the configuration of a regular dodecahedron (the dual to the icosahedron). Construct a conformal map from each face of the dodecahedron to the complement of its opposite face, taking vertices to opposite vertices. (See Figure 4.) The maps piece together across the boundaries of the faces, yielding a degree 11 rational map $f(z)$ with fixed points at the face centers and critical points at each vertex. Since the notions of 'opposite face' and 'opposite vertex' are intrinsic, the map commutes with the icosahedral group.

This construction has many variants. For example, it can be applied to the 20 faces of the icosahedral triangulation, giving a rational map of degree 19, or to the tiling by 30 rhombuses, giving a map of degree 29. (This last tiling, which may be unfamiliar, is by Dirichlet fundamental domains for the 30 edge-midpoints of the dodecahedron. Each rhombus marks the territory which is closer (in the spherical metric) to one of the 30 points than to any other.)

III. *Algebraic constructions.* Our final method suffices to produce *all* rational maps with given symmetries. It will make clear, for example, that the three maps just constructed, together with the identity, are the *only* maps of degree <31 with icosahedral symmetry.

Let E be a 2-dimensional complex vector space.

A point p on $\mathbf{P}E$ corresponds to a line in E hence to a linear functional with this line as its kernel. A collection of n points corresponds to a homogeneous polynomial of degree n, vanishing along the lines corresponding to the n points. Like the linear map corresponding to a single point, this polynomial is only well-defined up to multiplication by an element of $\mathbf{C}^*$.

A *rational map* $f:\mathbf{P}E\rightarrow\mathbf{P}E$ corresponds to a homogeneous polynomial map $X:E\rightarrow E$. X can be obtained by homogenizing the numerator and denominator of f.

Since the tangent space to any point of E is canonically isomorphic to E, X can also be considered as a *homogeneous vector field* on E.

Now let $\Gamma\subset\mathrm{Aut}(\mathbf{P}E)$ be a finite group, $\bar{\Gamma}\subset\mathrm{SL}(E)$ its pre-image in the group of linear maps of determinant 1. A vector field X on E is *invariant* if there exists a character $\chi:\bar{\Gamma}\rightarrow\mathbf{C}^*$ such that $\gamma_* X=\chi(\gamma)X$ for all γ in $\bar{\Gamma}$. X is *absolutely invariant* if the character is trivial.

The action of $\bar{\Gamma}$ on vector fields goes over to the action of Γ *by conjugation* on rational maps, establishing:

PROPOSITION 5.1. $\mathrm{Aut}(f(z))$ *contains* Γ *if and only if the corresponding vector field* $X(v)$ is Γ*-invariant.*

Remarks. (1) The possibility of a character arises because $f(z)$ determines $X(v)$ only up to scale.

(2) For a 2-dimensional vector space, $\mathbf{P}E$ and $\mathbf{P}E^*$ are canonically isomorphic; thus a rational map $f:\mathbf{P}E\rightarrow\mathbf{P}E\cong\mathbf{P}E^*$ also determines a homogeneous *1-form* $\theta(v):E\rightarrow E^*$, unique up to scale.

(3) A rational map of degree n determines a 1-form θ which is homogeneous of degree $n+1$; the converse is true unless $\theta=g\alpha$ for some homogeneous polynomial g and 1-form α with $\deg(\alpha)<\deg(\theta)$. In this case the numerator and denominator of the corresponding rational function are not relatively prime.

(4) A homogeneous polynomial $h(v)$ determines an *exact* 1-form $dh(v)$; thus *a configuration of* $n+1$ *points on* $\hat{\mathbf{C}}$ *naturally determines a rational map of degree n.*

Let x and y be a basis for E^*. The 1-form

$$\lambda(x, y) = (xdy - ydx)/2$$

is an absolute $\mathrm{SL}(E)$ invariant, as well as a primitive for the invariant volume from $\omega = dx \wedge dy$. The rational map corresponding to λ is the identity ($\lambda(v)$ annihilates the line through v).

THEOREM 5.2. *A homogeneous 1-form θ is invariant if and only if*

$$\theta = f(v)\lambda + dg(v)$$

where f and g are invariant homogeneous polynomials with the same character and $\deg(f) = \deg(g) + 2$.

Proof. Suppose θ is invariant. The exterior derivative $d\theta = h(v)\omega$, where $h(v)$ is a homogeneous polynomial. Since ω is an absolute invariant of $\mathrm{SL}(E)$, $h(v)$ is invariant with the same character as θ. Setting $f(v) = h(v)/(\deg(h)+1)$, it is easy to check that $df(v)\lambda = h(v)\omega$ and hence $\theta - f(v)\lambda$ is closed. Integrating this closed form along lines from the origin yields its unique homogeneous primitive $g(v)$; by uniqueness, $g(v)$ is invariant with the same character as θ.

The converse is clear; the condition on degrees assures that the sum is homogeneous. □

The construction of invariant rational maps is thus reduced to the problem of invariant homogeneous polynomials. The latter correspond simply to *finite sets of points on* $\hat{\mathbf{C}}$, invariant under Γ, and are easily described.

Example: The icosahedral group. Identify the Riemann sphere with a round sphere in $\mathbf{R}^3$ so that 0 and ∞ are poles and $|z| = 1$ is the equator. Inscribe a regular icosahedron in the sphere normalized so one vertex is at 0 and an adjacent vertex lies on the positive real axis (in $\hat{\mathbf{C}}$). Then the isometries of the icosahedron act on $\hat{\mathbf{C}}$ by a group $\Gamma \subset \mathrm{PSL}_2\mathbf{C}$ isomorphic to A_5. This particular normalization agrees with the conventions of Klein and Dickson [10], [2].

Since the abelianization of the binary icosahedral group $\bar{\Gamma}$ is zero, every invariant is an absolute invariant.

We identify $\hat{\mathbf{C}}$ with $\mathbf{P}E$, and choose a basis $\{x, y\}$ for E^* such that the coordinate z on $\hat{\mathbf{C}}$ is equal to x/y.

There are three special orbits for the action of Γ: the 12 vertices, 20 face-centers and 30 edge-midpoints of the icosahedron. The corresponding invariant polynomials, derived in [10], are:

$$f = x^{11}y + 11x^6y^6 - xy^{11}$$
$$H = -x^{20} - y^{20} + 228(x^{15}y^5 - x^5y^{15}) - 494x^{10}y^{10}$$
$$T = x^{30} + y^{30} + 522(x^{25}y^5 - x^5y^{25}) - 10005(x^{20}y^{10} + y^{10}y^{20}).$$

Every other orbit has cardinality 60, and corresponds to a linear combination of the degree 60 invariants f^5, H^3 and T^2 (which satisfy the relation $T^2 = 1728f^5 - H^3$). Thus *every homogeneous polynomial invariant under the binary icosahedral group is a polynomial in f, H and T.*

PROPOSITION 5.3. *There are exactly four rational maps of degree* <31 *which commute with the icosahedral group. These four maps, of degree* 1, 11, 19 *and* 29 *respectively, are:*

$$f_1(z) = z$$
$$f_{11}(z) = \frac{z^{11} + 66z^6 - 11z}{-11z^{10} - 66z^5 + 1}$$
$$f_{19}(z) = \frac{-57z^{15} + 247z^{10} + 171z^5 + 1}{-z^{19} + 171z^{14} - 247z^9 - 57z^4}$$
$$f_{29}(z) = \frac{87z^{25} - 3335z^{20} - 6670z^{10} - 435z^5 + 1}{-z^{29} - 435z^{24} + 6670z^{19} + 3335z^9 + 87z^4}.$$

Proof. An invariant rational map of degree <31 corresponds to an invariant 1-form of degree <32. The only invariant homogeneous polynomials of degree <32 are f, H and T. Since no two of their degrees differ by 2, we conclude from Theorem 5.2 that the invariant 1-forms of degree <32 are proportional to either $g(v)\lambda$ or $dg(v)$, where g is equal to f, H or T. The rational maps corresponding $g(v)\lambda$ are the identity, while those corresponding to df, dH and dT are the other three maps computed above. □

Remark. One may glean from the footnote on page 345 of [9] that these maps were known as well to Klein.

Proof of Lemma 4.5 *(Existence of an icosahedral algorithm).* Consider the map $f_{11}(z)$. We claim the critical points of f_{11} reside at the 20 vertices of a spherical regular dodecahedron, and are each mapped to their antipodal vertices under one iteration. This is clear from the geometric construction of f_{11} (method II above).

It can also be verified by counting. f_{11} has 20 critical points, which must be a union of orbits of Γ; the only such orbit corresponds to the vertices of a dodecahedron. Each vertex has an A_3 stabilizer in Γ; since f_{11} commutes with the group action, the image vertex is fixed by the same subgroup. A simple critical point which is fixed cannot commute with the A_3 action; hence the corresponding critical value must be the antipodal vertex.

Thus f_{11} is critically finite, and almost every point is attracted to periodic cycles of order two lying at pairs of antipodal vertices. The map $f_{11} \circ f_{11}$ satisfies the hypotheses of the lemma. □

Remarks. (1) There is a one-parameter family of invariant rational maps of degree 31, which will be used to construct ϕ in $\mathrm{PSL}_2 k'$ in our explicit solution of the quintic.

(2) Let $p(z)$ be a polynomial of degree d. Consider *radically modified Newton's method:*

$$R_p(z) = z - d\frac{p(z)}{p'(z)}.$$

R_p is the unique rational map of degree $d-1$ with fixed points at the roots of p and derivative $1-d$ at each fixed point. When $d=2$, R_p is a Möbius transformation of order two fixing the roots of p; for $d>2$ the roots are repelling. (Thus R_p is not suggested as a method to find roots of p.)

R_p coincides with the rational map naturally associated to the roots of p by exterior derivative of the corresponding homogeneous polynomial, as discussed above. This observation will simplify the description of our explicit iterative scheme for the quintic: we need only specify p.

Appendix

In this appendix we will describe a concrete algorithm for solving the general quintic equation. This algorithm is based on Klein's theory of the connection between the general quintic and the icosahedral equation, described in his famous lectures on the icosahedron [10]. See also Fricke [4] (from which we take the illustration below), and Dickson [2]. We begin by reviewing this theory.

The icosahedral equation

Associated with the icosahedron (normalized as in §5) is a tiling of the Riemann sphere by 120 spherical triangles, 60 black and 60 white (Figure 5). This configuration is

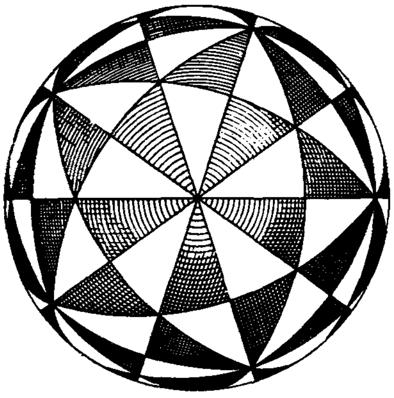

Fig. 5. The icosahedral tiling.

invariant under the icosahedral group, represented as a group Γ_{60} of Möbius transformations. Each triangle has angles $\pi/2$, $\pi/3$, $\pi/5$ corresponding to the 30 edge midpoints, 20 face centers, and 12 vertices of the icosahedron. We will refer to these special points as 2-, 3-, and 5-vertices.

Map each white triangle conformally to the upper half-plane, and map each black triangle conformally to the lower half-plane, so that the 3-, 5-, and 2-vertices map to 0, 1, ∞. These 120 separate mappings piece together to give a rational function of degree 60, the *icosahedral function*. This function, denoted by Z_{60}, is right-invariant under the icosahedral group Γ_{60}:

$$Z_{60} \circ \gamma = Z_{60} \quad \text{for all} \quad \gamma \in \Gamma_{60};$$

it gives the quotient map $\hat{\mathbf{C}} \to \hat{\mathbf{C}}/\Gamma_{60}$.

To write down the icosahedral function explicitly, recall that every homogeneous polynomial invariant under the binary icosahedral group $\Gamma_{2\cdot 60}$ is a polynomial in F_{12}, H_{20}, and T_{30}, where

$$F_{12}(z_1, z_2) = z_1^{11} z_2 + 11 z_1^6 z_2^6 - z_1 z_2^{11},$$

$$H_{20}(z_1, z_2) = -z_1^{20} + 228 z_1^{15} z_2^5 - 494 z_1^{10} z_2^{10} - 228 z_1^5 z_2^{15} - z_2^{20},$$

$$T_{30}(z_1, z_2) = z_1^{30} + 522 z_1^{15} z_2^5 - 10005 z_1^{20} z_2^{10} - 10005 z_1^{10} z_2^{20} - 522 z_1^5 z_2^{25} + z_2^{30}.$$

The polynomials F_{12}, H_{20}, and T_{30} vanish at the 5-, 3-, and 2-vertices respectively. They satisfy the identity

$$T_{30}{}^{2}+H_{20}{}^{3}-1728F_{12}{}^{5}=0.$$

The icosahedral function $Z_{60}(z)$ is

$$Z_{60}=\frac{-H_{20}{}^{3}}{T_{30}{}^{2}}.$$

To check this, note that the top and bottom are homogeneous of degree 60 (so the ratio is a rational function of $z=z_1/z_2$), the zeros and poles occur at the 3- and 2- vertices, and by the identity

$$Z_{60}-1=\frac{-H_{20}{}^{3}-T_{30}{}^{2}}{T_{30}{}^{2}}=\frac{-1728F_{12}{}^{5}}{T_{30}{}^{2}}$$

the 5-vertices of the icosahedron are mapped to 1.

The equation

$$Z_{60}(z)=Z$$

is called the *icosahedral equation*. Solving the icosahedral equation amounts to finding one of the 60 points that map to Z under the icosahedral function. Given one such point, the 59 others can be found by determining the images of the first under the group Γ_{60}.

Please note that our normalization of the icosahedral function differs from the normalizations of Klein [10] and Dickson [2]:

$$Z_{\text{Klein}}=\frac{H_{20}{}^{3}}{1728F_{12}{}^{5}}=\frac{Z_{60}}{Z_{60}-1};$$

$$Z_{\text{Dickson}}=\frac{F_{12}{}^{5}}{T_{30}{}^{2}}=\frac{1-Z_{60}}{1728}.$$

From the general quintic to the icosahedral equation

In this section we give a brief account of the classical reduction of the general quintic equation

$$p(x)=x^{5}+a_1x^{4}+a_2x^{3}+a_3x^{2}+a_4x+a_5=0$$

to the icosahedral equation, following Klein [10]. As Klein emphasized, this reduction is best understood geometrically.

The first step in the reduction dates back to 1683, when Tschirnhaus showed that by making a substitution of the form

$$x \leftarrow x^2+ax+b,$$

the general quintic can be reduced to a quintic for which $a_1=a_2=0$. Here a and b are determined by solving an auxiliary quadratic equation. Such a quintic is called a *principal quintic*.

Equivalently, a principal quintic is one normalized so its roots satisfy $\Sigma x_i=\Sigma x_i^2=0$. These homogeneous equations determine a quadric surface in the projective space of roots. Viewed geometrically, the Tschirnhaus transformation moves an *ordered* set of roots to one of the two points of intersection of this quadric with the line determined by allowing a and b to vary. Which point depends on the choice of auxiliary root.

The symmetric group S_5 acts on the quadric by permuting the roots. An odd permutation interchanges the two rulings of the quadric by lines; adjoining the square-root of the discriminant reduces the action to the alternating group A_5, which preserves the rulings.

The space of lines in a given ruling is isomorphic to the Riemann sphere $\hat{\mathbf{C}}$, and in appropriate coordinates the action of A_5 is none other than the icosahedral action. From the original principal quintic and the square-root of its discriminant, we may determine a point Z on the quotient such that a solution to

$$Z_{60}(z)=Z$$

corresponds to a line containing the point $(x_1{:}x_2{:}x_3{:}x_4{:}x_5)$ for some ordering of the roots. Then the roots themselves can be found by elimination.

Perhaps the most intriguing part of this whole story is the square root used in the Tschirnhaus transformation to obtain a principal quintic. This square root is an *accessory irrationality*, as it does not diminish the Galois group of the equation, and as such is not expressible in terms of the roots of the equation. Rather, its function (as pointed out by Serre [14]) is to eliminate the cohomological obstruction described in §2. The culmination of Klein's lectures on the icosahedron is the result, which Klein calls *Kronecker's theorem*, that without the introduction of such an accessory irrationality the general quintic equation cannot be reduced to a resolvent equation that depends —like the icosahedral equation—on a single parameter. While this result was stated by Kronecker, the first correct proof was given by Klein. Apparently, Kronecker felt that accessory irrationalities were 'algebraically worthless', and proposed what he called the 'Abelian Postulate', requiring that such accessory irrationalities be avoided at all costs. According to this view, the reduction of the quintic to the icosahedral equation is inadmissible. Arguing against this point of view, Klein [9, p. 504] writes:

> Soll man, wo sich neue Erscheinungen (oder hier die Leistungsfähigkeit der akzessorischen Irrationalitäten) darbieten, zugunsten einer einmal gefassten systematischen Ideenbildung die Weiterentwicklung abschneiden, oder vielmehr das systematische Denken als zu eng zurückschieben und den neuen Problemen unbefangen nachgehen? Soll man Dogmatiker sein oder wie ein Naturforscher bemüht sein, aus den Dingen selbst immer neu zu lernen?
>
> (When new phenomena appear, like the efficacy of the accessory irrationality, should we halt our investigations because the facts fail to agree with our preconceived notions, or should we cast aside those preconceived notions as being too narrow, and pursue the new problems wherever they lead? Should we be dogmatists, or should we—like natural scientists—try always to learn from the facts themselves?)

Quintic resolvents of the icosahedral equation

The algorithm we are going to develop to solve the general quintic proceeds by computing a root, not of the icosahedral equation itself, but of a certain *quintic resolvent*.

Algebraically, the icosahedral equation determines an A_5 extension of function fields k'/k, where $k=\mathbf{C}(Z)$ and $k'=\mathbf{C}(Z,z)/(Z_{60}(z)-Z)$. A quintic resolvent is the irreducible polynomial satisfied by an element of k' of degree 5 over k.

In this section, we will derive formulas for the *tetrahedral* and *Brioschi* resolvents, again following Klein [10]. The Brioschi resolvent is a one parameter family of quintics, to which the general quintic may be reduced; it is this equation we will actually solve. The tetrahedral resolvent is used to determine a root from the limit point of an iteration.

The root of a quintic resolvent is stabilized by an A_4 subgroup of A_5. There are five such tetrahedral subgroups in Γ_{60}, all conjugate. One tetrahedral subgroup, which we denote Γ_{12}, is distinguished because it leads to a resolvent defined over $\mathbf{R}$.

Γ_{12} can be described geometrically as follows. There are five cubes whose vertices lie on the vertices of a regular dodecahedron. Of these, exactly one is symmetric with respect to reflection through the real axis; the intersection of its symmetry group with Γ_{60} is Γ_{12}. The vertices of this cube, and the one-skeleton of its dual octahedron (which includes the real axis), appear in Figure 6.

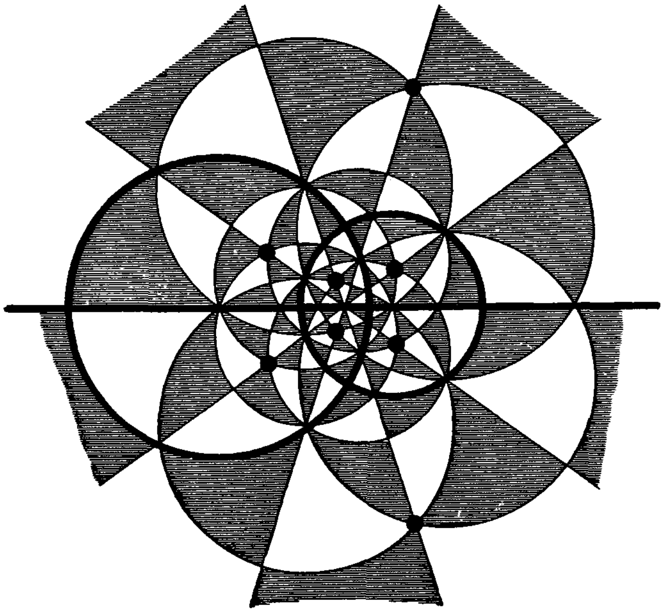

Fig. 6. A cube inscribed in the dodecahedron.

Γ_{12} permutes the 12 pentagons that correspond to faces of the dodecahedron, and any one of them is a fundamental domain for Γ_{12}.

Γ_{12} preserves the 6 vertices of the dual octahedron, and the 4 vertices of each tetrahedron inscribed in the cube; the stabilizers of all other points are trivial. Note that only half of the symmetries of the cube (and octahedron) are symmetries of the icosahedron; otherwise Γ_{60} would have a subgroup of order 24.

Besides the special orbits of Γ_{12}, we need to pay attention to two orbits of order 12: the face centers of the dodecahedron, i.e., the 5-vertices, and the $20-8=12$ *complementary* 3-vertices—the vertices of the dodecahedron which do not lie on the cube.

There is a tetrahedral function r_{12}, analogous to the icosahedral function Z_{60}, which gives the quotient map $\hat{\mathbf{C}}\rightarrow\hat{\mathbf{C}}/\Gamma_{12}$. By composing with a Möbius transformation, this function can be normalized to take specified values on any three orbits of Γ_{12}. We choose the normalization so that the 5-vertices map to ∞, the vertices of the octahedron map to 0, and the complementary 3-vertices map to 3.

To write down a formula for r_{12}, we call forth some of the invariant forms for the binary tetrahedral group $\Gamma_{2\cdot 12}$. Fortunately, all the forms that we need to work with are absolute invariants (no character of $\Gamma_{2\cdot 12}$ appears). Those we use,

$$t_6(z_1, z_2) = z_1^6+2z_1^5 z_2-5z_1^4 z_2^2-5z_1^2 z_2^4-2z_1 z_2^5+z_2^6,$$
$$W_8(z_1, z_2) = -z_1^8+z_1^7 z_2-7z_1^6 z_2^2-7z_1^5 z_2^3+7z_1^3 z_2^5-7z_1^2 z_2^6-z_1 z_2^7-z_2^8,$$

and

$$\begin{aligned}\chi_{12}(z_1, z_2) &= \frac{H_{20}(z_1,z_2)}{W_8(z_1,z_2)} \\ &= z_1^{12}+z_1^{11} z_2-6z_1^{10} z_2^2-20z_1^9 z_2^3+15z_1^8 z_2^4-24z_1^7 z_2^5+11z_1^6 z_2^6 \\ &\quad +24z_1^5 z_2^7+15z_1^4 z_2^8+20z_1^3 z_2^9-6z_1^2 z_2^{10}-z_1 z_2^{11}+z_2^{12}\end{aligned}$$

vanish at the vertices of the octahedron, the cube, and the complementary 3-vertices respectively.

Any invariant form of degree 12 is a linear combination of the forms t_6^3, χ_{12}, and F_{12}, which satisfy the identity

$$t_6^2-\chi_{12}-3F_{12} = 0.$$

Thus

$$r_{12} = \frac{t_6^2}{F_{12}},$$

since this expression has zeros and poles in the right places, and the identity

$$r_{12}-3 = \frac{t_6^2-3F_{12}}{F_{12}} = \frac{\chi_{12}}{F_{12}}$$

shows the complementary 3-vertices are mapped to 3 as desired.

Under r_{12}, the 60 roots of the icosahedral equation

$$Z_{60}(z) = Z$$

map in groups of 12 to 5 distinct points. In terms of a single root z, these 5 images are

$$r_{12}^{(k)}(z) = r_{12}(\varepsilon^k z) = \frac{(t_6^{(k)}(z_1, z_2))^2}{F_{12}(z_1, z_2)}, \quad k = 0, \dots, 4,$$

where

$$t_6^{(k)}(z_1, z_2) = t_6(\varepsilon^{3k} z_1, \varepsilon^{2k} z_2)$$

and ε is a fifth root of unity. (The rotation $z \mapsto \varepsilon z$ is an element of Γ_{60}.)

The quintic resolvent for $r_{12}(z)$ turns out to be

$$(r-3)^3(r^2-11r+64)=\frac{-1728Z}{Z-1}.$$

We will call this equation the *tetrahedral resolvent*. Algebraically, the functions $r_{12}^{(k)}(z)$ are just the roots of the tetrahedral resolvent in the function field setting. This equation can be derived entirely geometrically, without recourse to the explicit formulas for r_{12}. (See Klein [10, pp. 100–102].)

The related function $s_{24}(z)$ given by

$$s_{24}=\frac{t_6{F_{12}}^2}{T_{30}}=\frac{1}{{r_{12}}^2-10r_{12}+45}$$

satisfies the *Brioschi* resolvent

$$s^5-10Cs^3+45C^2s-C^2=0,$$

where $C=(1-Z)/1728$; the roots of this equation are:

$$s_{24}^{(k)}(z)=s_{24}(\varepsilon^k z)=\frac{t_6^{(k)}(z_1,x_2)\,(F_{12}(z_1,z_2))^2}{T_{30}(z_1,z_2)},\quad k=0,\dots,4.$$

Any principal quintic can be reduced to the Brioschi resolvent for some particular choice of C, determined rationally in terms of the original coefficients and the square-root of the discriminant. This reduction appears in detail in Dickson [2].

The icosahedral iteration

We are now ready to concoct a generally convergent algorithm for the icosahedral field extension k'/k. The ingredients for such an algorithm are given in Theorem 4.1; note that the Galois group, Γ_{60}, is tautologically identified with a group of Möbius transformations.

The algorithm itself is specified by

(a) a rational map $f(w)$ commuting with Γ_{60}, and

(b) a Möbius transformation $\phi_z(w)$, depending on a root z of the icosahedral equation, such that

$$\phi_{\gamma z}(w)=\gamma\circ\phi_z(w)$$

for all γ in Γ_{60}.

The coordinate w can be thought of as residing on a separate Riemann sphere where the iteration is performed. The algorithm is given by

$$T_z(w) = \phi_z^{-1} \circ f \circ \phi_z;$$

by (a) and (b) $T_{\gamma z}=T_z$ and so T only depends upon $Z=Z_{60}(z)$.

To make the formulas as simple as possible, we will choose $f=f_{11}$, the unique lowest degree rational map with icosahedral symmetry and a non-trivial attractor (see §5). (The attractor of f_{11} is periodic of order 2, so we will actually iterate $f_{11} \circ f_{11}$.)

As for ϕ_z, note that for each fixed w the map $z \mapsto \phi_z(w)$ is a rational map with icosahedral symmetry. As mentioned in Remark 1 of §5, there is a one-parameter family of symmetric maps of degree 31 (and none of smaller degree); this provides the simplest candidate for ϕ. There are three points at which this family degenerates to maps of lower degree f_1, f_{11}, and f_{19}; we arrange that these degenerations occur at $w=\infty$, 0 and 1.

To derive a formula for T_z in terms of Z, we begin by expressing ϕ in homogeneous coordinates

$$\phi_z(w) = [\Phi_{(z_1,z_2)}(w_1, w_2)];$$

then

$$[\Phi_{(z_1,z_2)}(w_1, w_2)] = \left[w_1(-T_{30}\cdot(z_1, z_2)) + w_2\left(H_{20}\cdot\left(-\frac{\partial F_{12}}{\partial z_2}, \frac{\partial F_{12}}{\partial z_1}\right)\right)\right].$$

To check this formula, we just need to verify that it degenerates as described above. Clearly this is true for $w=0$ and ∞. For $w=1$ the rational map we get is

$$\left[-T_{30}\cdot(z_1, z_2) + H_{20}\cdot\left(-\frac{\partial F_{12}}{\partial z_2}, \frac{\partial F_{12}}{\partial z_1}\right)\right],$$

which agrees with f_{19} by virtue of the identity

$$-T_{30}\cdot(z_1, z_2) + H_{20}\cdot\left(-\frac{\partial F_{12}}{\partial z_2}, \frac{\partial F_{12}}{\partial z_1}\right) = \frac{3}{5}F_{12}\cdot\left(-\frac{\partial H_{20}}{\partial z_2}, \frac{\partial H_{20}}{\partial z_1}\right).$$

To get the formula for T_Z, we note f_{11} is canonically associated to the 12 vertices of the icosahedron, so T is canonically associated to their images under ϕ_z^{-1}. By Remark 2 at the end of §5, all we must do to specify T_Z is to give a polynomial $g(Z, w)$ having these 12 points as its roots.

This leads us to look at the form $G=F_{12}\circ\Phi$, where Φ is the homogeneous version of ϕ given above. The form G is homogeneous of degree $12\cdot 31=372$ in z_1, z_2 and of degree 12 in w_1, w_2. This polynomial is symmetric under the action of $\Gamma_{2\cdot 60}$ on z_1, z_2. Because the ring of $\Gamma_{2\cdot 60}$-symmetric forms is generated by F_{12}, H_{20}, and T_{30}, and because $372=6\cdot 60+12$, it follows on numerological grounds that G is divisible by F_{12}, and that the quotient G/F_{12} can be written as a homogeneous polynomial of degree 6 in $-H_{20}^3, T_{30}^2$ and of degree 12 in w_1, w_2. This polynomial can be found by solving a large system of linear equations. Dividing the resulting expression for G/F_{12} through by $T_{30}^{12}w_2^{12}$ and using the fact that $Z_{60}=-H_{20}^3/T_{30}^2$, we get

$$\frac{F_{12}\circ\Phi}{F_{12}T_{30}^{12}w_2^{12}}=g(Z,w),$$

where g is a polynomial with integer coefficients, exhibited at the end of this Appendix. We found the coefficients of g by solving the relevant system of equations with the aid of a computer.

The map T_Z is now given by

$$T_Z(w)=w-12\frac{g(Z,w)}{g'(Z,w)},$$

where g' denotes the derivative of g with respect to w.

From the iteration to a root

Under the iteration $w\mapsto f_{11}(w)$ almost every starting guess is attracted to a cycle of period 2 consisting of one of the 10 pairs of antipodal 3-vertices. If instead of iterating f_{11} we iterate $f_{11}\circ f_{11}$, then almost every starting guess is attracted to a single one of the 20 3-vertices.

The map T_Z is just f_{11} transported to new coordinates by ϕ. For almost every Z, almost every starting guess converges under iteration of $T_Z\circ T_Z$ to

$$w_0=\phi_z^{-1}(e),$$

where e is one of the 20 3-vertices of the icosahedron in its standard location.

Of course to be able to write

$$w_0=\phi_z^{-1}(e),$$

we have to select some particular root z of the icosahedral equation, for we could equally well write

$$w_0 = \phi_{\gamma z}^{-1}(\gamma e).$$

Turning this around, we see that if we choose some particular 3-vertex e_0, there will be exactly three choices for the root z for which

$$w_0 = \phi_z^{-1}(e_0).$$

These three choices differ from one another by the action of the stabilizer A_3 of the 3-vertex e_0. Therefore from w_0 we can determine the values of *two* of the functions $s_{24}^{(k)}(z)$, and hence two roots s_1, s_2 of the Brioschi resolvent. These two values correspond to the two tetrahedral (A_4) subgroups of Γ_{60} that contain the stabilizer of e_0.

As w_0 ranges over the 20 attractors of T_Z, the pair (s_1, s_2) ranges over the 20 ordered pairs of roots of the resolvent. In particular, going from w_0 to the 'antipodal point' $T_Z(w_0)$, we get the same pair of roots in the opposite order.

To determine s_1 and s_2 explicitly in terms of w_0, we introduce the function

$$\mu(Z, w) = \sum_k (r_{12}^{(k)} - 3) \circ \phi_z(w) \cdot s_{24}^{(k)}(z).$$

While expressed in terms of z, this function really only depends on Z, because the action of Γ_{60} permutes the two sets of factors in the same way. The idea behind μ is that the first factor acts as a 'selector function' for the second: Recall that the value of function r_{12} is 3 at the complementary 3-vertices; at the vertices of the tetrahedron and the dual tetrahedron its values are

$$r = \frac{11}{2} + \frac{3\sqrt{-15}}{2}, \quad r = \frac{11}{2} - \frac{3\sqrt{-15}}{2},$$

which are the other two roots of

$$(r-3)^3(r^2 - 11r + 64) = Z_{60}(\text{3-vertex}) = 0.$$

Thus the factor $(r_{12}^{(k)} - 3) \circ \phi_z(w_0)$ vanishes for three values of k and takes on the values

$$\frac{1 + 3\sqrt{-15}}{2}, \quad \frac{1 - 3\sqrt{-15}}{2}$$

for the remaining two values of k. Consequently

$$\mu(Z, w_0) = \frac{1+3\sqrt{-15}}{2} s_1 + \frac{1-3\sqrt{-15}}{2} s_2$$

where s_1, s_2 are two roots of the Brioschi resolvent. Replacing w_0 with the 'antipodal' fixed point $T_Z(w_0)$ exchanges the roles of s_1 and s_2, so we have

$$\mu(Z, T_Z(w_0)) = \frac{1-3\sqrt{-15}}{2} s_1 + \frac{1+3\sqrt{-15}}{2} s_2.$$

Thus we get a pair of linear equations from which we can determine s_1 and s_2.

All that remains is to express μ in terms of Z and w. Let $\chi_{12}^{(k)}$ be defined analogously to $t_6^{(k)}$. Then

$$\begin{aligned}\mu &= \sum_k (r_{12}^{(k)} - 3) \circ \phi \cdot s_{24}^{(k)} \\ &= \sum_k \left(\frac{\chi_{12}^{(k)} \circ \Phi}{F_{12} \circ \Phi}\right) \cdot \frac{t_6^{(k)} {F_{12}}^2}{T_{30}} \\ &= \frac{\sum_k (\chi_{12}^{(k)} \circ \Phi) \cdot t_6^{(k)} \cdot F_{12}/({T_{30}}^{13} {w_2}^{12})}{(F_{12} \circ \Phi)/F_{12} {T_{30}}^{12} {w_2}^{12})}.\end{aligned}$$

The denominator here is our old friend $g(Z, w)$. The numerator can be expressed as a polynomial in Z and w, by the same technique used to determine g. We find

$$\mu(Z, w) = \frac{100 Z(Z-1) h(Z, w)}{g(Z, w)},$$

where $h(Z, w)$ is a polynomial with integer coefficients, exhibited below.

The algorithm

To solve the Brioschi resolvent

$$s^5 - 10Cs^3 + 45C^2 s - C^2 = 0$$

we proceed in five steps.

(1) Set $Z = 1 - 1\,728C$.

(2) Compute the rational function

$$T_Z(w) = w - 12\frac{g(Z, w)}{g'(Z, w)},$$

where $g(Z, w)$ is the polynomial in Z and w given below, and g' denotes the derivative of g with respect to w.

(3) Iterate $T_Z(T_Z(w))$ on a random starting guess until it converges. Call the limit point w_0, and set $w_1 = T_Z(w_0)$.

(4) Compute

$$\mu_i = \frac{100Z(Z-1)\,h(Z, w_i)}{g(Z, w_i)}$$

for $i=0, 1$, where h is the polynomial in Z and w given below.

(5) Finally compute

$$s_i = \frac{(9+\sqrt{-15})\mu_i + (9-\sqrt{-15})\mu_{1-i}}{90}$$

for $i=0, 1$. These are two roots of the Brioschi resolvent.

The key ingredients $g(Z, w)$ and $h(Z, w)$ are given by:

$$\begin{aligned} g(Z, w) = {} & 91125Z^6 \\ & +(-133650w^2+61560w-193536)Z^5 \\ & +(-66825w^4+142560w^3+133056w^2-61440w+102400)Z^4 \\ & +(5940w^6+4752w^5+63360w^4-140800w^3)Z^3 \\ & +(-1485w^8+3168w^7-10560w^6)Z^2 \\ & +(-66w^{10}+440w^9)Z \\ & +w^{12}, \end{aligned}$$

$$\begin{aligned} h(Z, w) = {} & (1215w-648)Z^4 \\ & +(-540w^3-216w^2-1152w+640)Z^3 \\ & +(378w^5-504w^4+960w^3)Z^2 \\ & +(36w^7-168w^6)Z \\ & -w^9. \end{aligned}$$

Remarks. (1) A quintic with real coefficients always has at least one real root. Curiously, when applied to a real quintic with real initial guess for step 3, our method returns a pair of conjugate roots.

(2) To find the remaining roots of the quintic, we can apply del Ferro's formula or

Example 3 of § 3 to solve the quotient cubic. We could also construct a single iteration that would find all five roots at once, but the formulas might be rather more complicated.

(3) Remarkably, one can also derive the formulas for g and h by hand, without even knowing the basic invariants F_{12}, H_{20} and T_{30} of the icosahedral group. This alternate approach exploits the large number of coefficients that vanish, and is based on a study of degenerations of g and h at $Z=0$, 1 and ∞.

References

[1] Abel, N. H., Beweis der Unmöglichkeit algebraische Gleichungen von höheren Graden als dem vierten allgemein aufzulösen. *J. Reine Angew. Math.*, 1 (1826), 65–84.

[2] Dickson, L., *Modern Algebraic Theories*. Benj. H. Sanborn & Co., 1930.

[3] Douady, A. & Hubbard, J., *Étude dynamique des polynômes complexes*. Publ. Math. d'Orsay, 1984.

[4] Fricke, R., *Lehrbuch der Algebra*, Vol. 2. Vieweg, 1926.

[5] Green, M., On the analytic solution of the equation of fifth degree. *Compositio Math.*, 37 (1978), 233–241.

[6] Grothendieck, A., Le groupe de Brauer I: Algèbres d'Azumaya et interpretations diverses. *Séminaire Bourbaki*, 290 (1965).

[7] — Le groupe de Brauer II: Théorie cohomologique. *Séminaire Bourbaki*, 297 (1965).

[8] Klein, F., *Elementary Mathematics from an Advanced Standpoint. Arithmetic, Algebra, Analysis*. McMillan Co., 1932.

[9] — *Gesammelte Mathematische Abhandlungen*. Vol. 2, Springer, 1922.

[10] — *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade*. B.G. Teubner, 1884.

[11] McMullen, C., Braiding of the attractor and the failure of iterative algorithms. *Invent. Math.*, 91 (1988), 259–272.

[12] — Families of rational maps and iterative root-finding algorithms. *Ann. of Math.*, 125 (1987), 467–493.

[13] Merkurev, A. S. & Suslin, A. A., K-cohomology of Severi-Brauer varieties and the norm residue homomorphisms. *Math. USSR-Izv.*, 21 (1983), 307–340.

[14] Serre, J. P., Extensions icosaédriques. In *Oeuvres* III, pp. 550–554. Springer-Verlag, 1986.

[15] — *Local Fields*. Springer-Verlag, 1979.

[16] Shub, M. & Smale, S., On the existence of generally convergent algorithms. *J. Complexity*, 2 (1986), 2–11.

[17] Smale, S., On the efficiency of algorithms of analysis. *Bull. Amer. Math. Soc.*, 13 (1985), 87–121.

[18] Sullivan, D., Conformal dynamical systems. In *Geometric Dynamics*, pp. 725–752. Lecture Notes in Mathematics, 1007 (1983). Springer-Verlag.

[19] Thurston, W. P., On the combinatorics and dynamics of iterated rational maps. Preprint.

[20] van der Waerden, B. L., *Geometry and Algebra in Ancient Civilizations*. Springer-Verlag, 1983.

[21] — *A History of Algebra: from al-Khwarizmi to Emmy Noether*. Springer-Verlag, 1985.

Received January 29, 1988