# Solving the Quintic Polynomial by Geometry, Algebra, and Iteration

Jerry Shurman

Willamette Valley REU Talk

August 2, 2007

## The quadratic polynomial

Start from

$$X^2 + aX + b = 0.$$

Let $X = Y - a/2$ to complete the square:

$$Y^2 = c.$$

Find $Y$ by taking a square root, and then $X$.

## The cubic polynomial

Start from

$$X^3 + aX^2 + bX + c = 0.$$

Let $X = Y - a/3$ to complete the cube:

$$Y^3 + pY + q = 0.$$

Let $Y = Z + W$:

$$Z^3 + W^3 + (3ZW + p)(Z + W) + q = 0.$$

Specialize $W = -p/(3Z)$ so that $3ZW = -p$:

$$Z^3 - \frac{p^3}{27Z^3} + q = 0,$$

or

$$(Z^3)^2 + qZ^3 - \frac{p^3}{27} = 0.$$

Find $Z^3$ by solving a quadratic, then $Z$ by taking a cube root, then $W$, then $Y$, then $X$.

## The quartic polynomial

Complete the fourth power and then slightly adjust the resulting quartic polynomial with no $X^3$ term:

$$X^4 + 2aX^2 + a^2X^2 = (a^2 + b)X^2 + cX + d,$$

or

$$(X^2 + aX)^2 = (a^2 + b)X^2 + cX + d.$$

Granting this relation, consider the auxiliary relation

$$(X^2 + aX + Y)^2 = (eX + f)^2.$$

Because of the relation satisfied by X, the left side expands to

$$(a^2 + b + 2Y)X^2 + (c + 2aY)X + (d + Y^2),$$

and the right side to

$$e^2X^2 + 2efX + f^2.$$

(Continued on next slide.)

## The quartic polynomial (continued)

So we need

$$\begin{aligned} a^2 + b + 2Y &= e^2, \\ c + 2aY &= 2ef, \\ d + Y^2 &= f^2, \end{aligned}$$

or

$$(c + 2aY)^2 = 4(a^2 + b + 2Y)(d + Y^2).$$

Solve this cubic polynomial to find $Y$, then find $e$ and $f$, then we have

$$X^2 + aX + Y = \pm(eX + f),$$

which we can solve for $X$.

*But what on earth is going on?!*

This is *bad mathematics*.

What is the *shape* of these ideas?

Their *scope*?

Should we seek ever more Byzantine calculations with basic algebra and extracting roots in order to solve polynomials of higher and higher degree?

**Galois**: No.

Beyond degree four, such calculations *can not succeed* for the general polynomial of degree $n$.

Galois associated a *finite group* to each polynomial, and he showed that the polynomial's solvability is equivalent to a group-theoretic condition. Then general polynomial of degree $n$ has group $S_n$, and $S_n$ does not satisfy the group-theoretic solvability criterion for $n \geq 5$.

Galois essentially had to create group theory to do this, and the scope of his ideas is very broad.

After Galois: People reduced high-degree polynomials to specific forms and then solved those specific forms with various transcendental functions (i.e., functions that transcend the mere algebra of radicals).

**Brioschi** reduced the general quintic polynomial to the form

$$b_w(T) = T^5 - 10wT^3 + 45w^2T - w^2.$$

In terms of Galois theory, this polynomial is no simpler than the general quintic polynomial, but in terms of *parameter-count* it is much simpler: its coefficients depend only on the *single* symbol $w$.

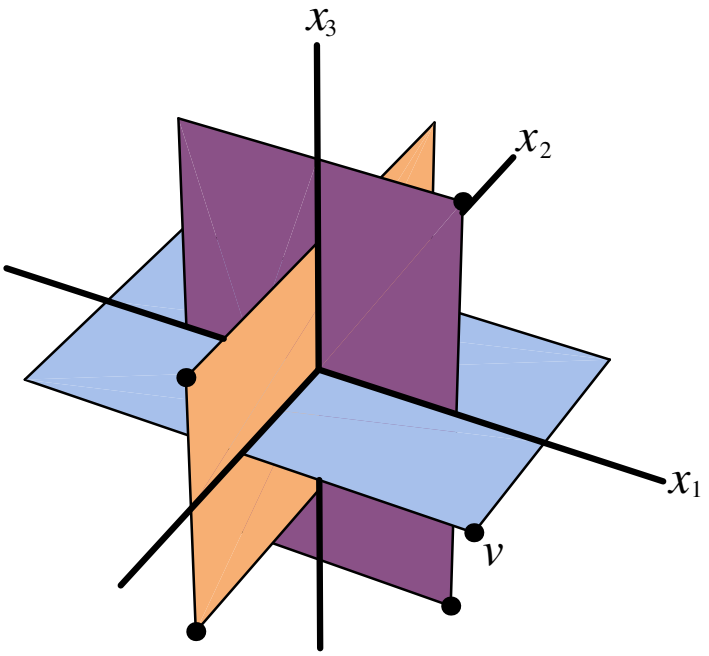
**Klein** observed that a one-parameter environment with the same group theory as the quintic polynomial arises naturally from geometry.

First, it is easy to reduce the general polynomial group from $S_n$ to $A_n$, so in particular, the relevant group for the quintic can be taken as $A_5$.

Second, the *icosahedron* has five orthogonal triples of golden rectangles sitting inside it—or, alternatively, five tetrahedra—and its rotation group is the group of their even permutations.

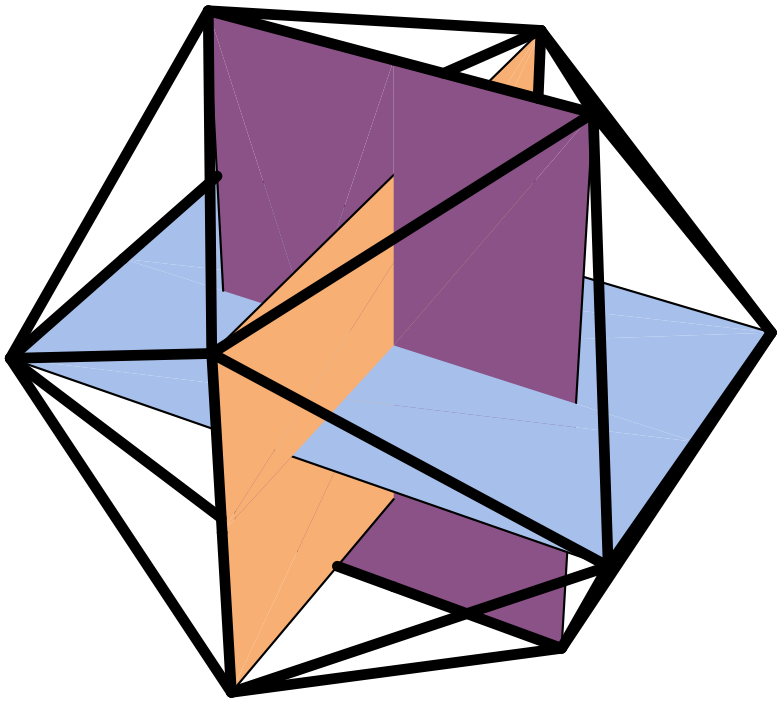
(Huh?)

Here is an orthogonal triple of rectangles, each in the golden ratio.



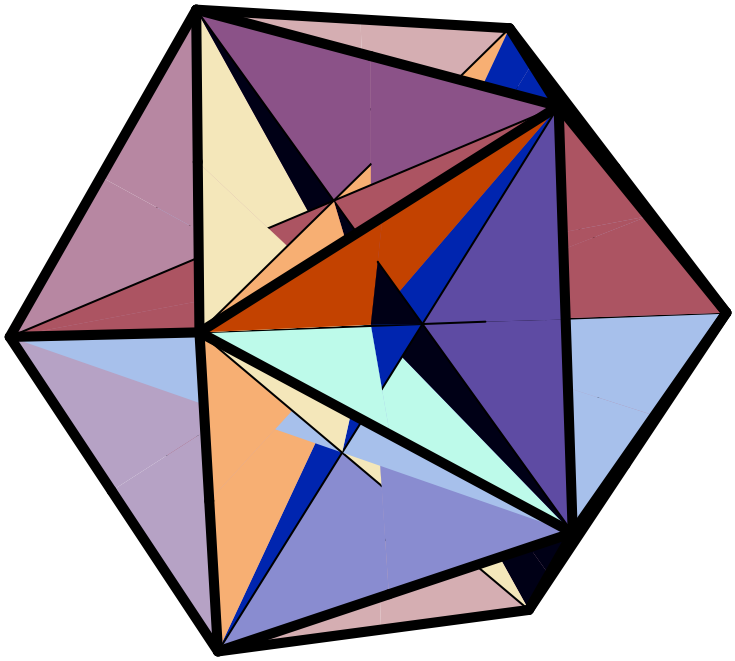

The quadratic condition defining the golden ratio shows that the rectangle corner $v$ has distance 1 from the other four corners emphasized in the picture.

That is, the rectangle corners form the vertices of an icosahedron.

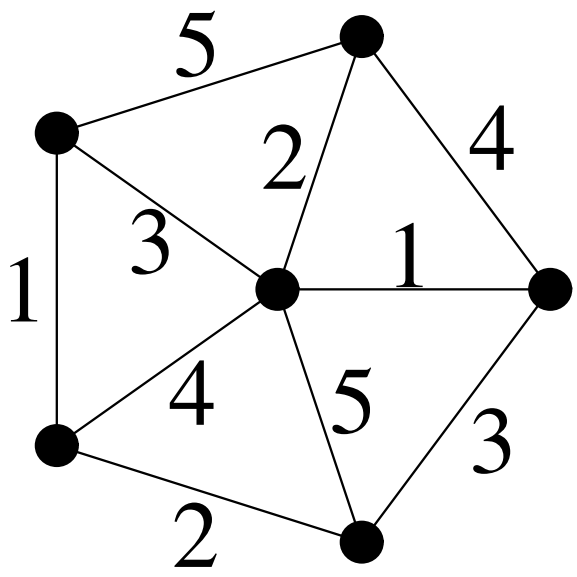


Indeed, this argument shows that the icosahedron *exists*.

In the configuration just shown, the rectangle edges “fill” only six of the icosahedron’s thirty edges, i.e., one-fifth of them. So in fact there are five such configurations in the icosahedron.



With a bit of thought, one can convince oneself that the rotation group of the icosahedron consists of all even permutations of the five golden configurations.




Rotate about the center vertex: $(1,2,3,4,5)$.

Rotate about the 1-edge: $(2,3)\,(4,5)$.

Rotate about the $(1,2,4)$-triangle: $(1,2,4)$.

The group $A_5$ has order $5!/2 = 60$.

Each icosahedral face is left in place by three rotations, each icosahedral edge is left in place by two rotations, and each icosahedral vertex is left in place by five rotations.

So the icosahedron has

$60/3 = 20$ faces (hence its name),
$60/2 = 30$ edges, and
$60/5 = 12$ vertices.

These numbers become coherent in light of group theory.

Returning to Klein's program: We said. . .

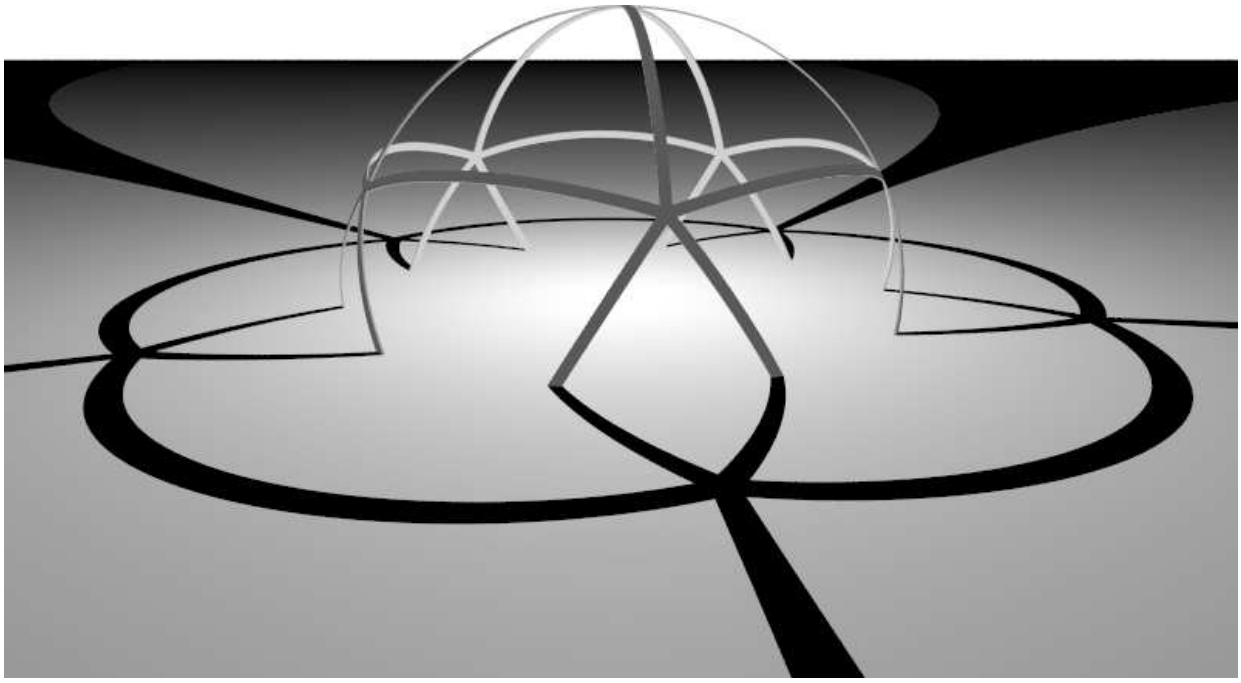
First, it is easy to reduce the general polynomial group from $S_n$ to $A_n$, so in particular, the relevant group for the quintic can be taken as $A_5$.

Second, the icosahedron has five orthogonal triples of golden rectangles sitting inside it—or, alternatively, five tetrahedra—and its rotation group is the group of their even permutations.

. . . And now:

Third, projecting the icosahedron radially to the sphere and then projecting it stereographically to the extended plane lets all of this geometry and group theory be expressed and analyzed further in terms of *complex analysis*.

(Continued on next slide.)



(This figure was created by Josh Levenberg, a Reed College student who was studying the Klein material at the time. He used a ray-tracing program.)

Klein found a rational function $f_I$ (of the complex variable $Z$) that is invariant under the icosahedral rotation group. Specifically,

$$f_I = \frac{(-Z^{20} + 228Z^{15} - 494Z^{10} - 228Z^5 - 1)^3}{1728Z^5(Z^{10} + 11Z^5 - 1)^5}.$$

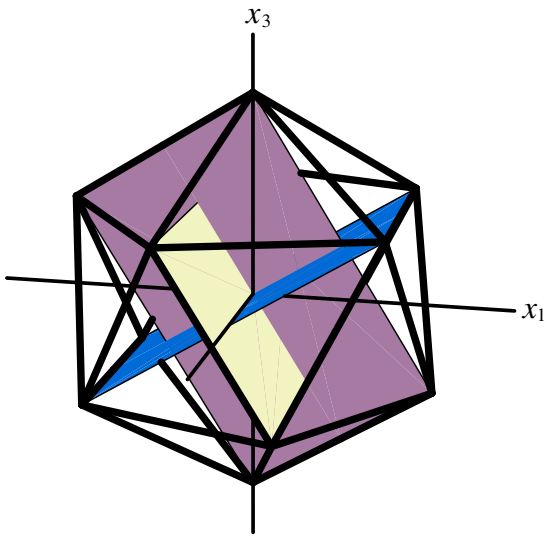
This function is *Klein's icosahedral invariant*.

It takes the value $\infty$ at the icosahedral vertices, the value 0 at the icosahedral face-centers, and the value 1 at the icosahedral mid-edge points.

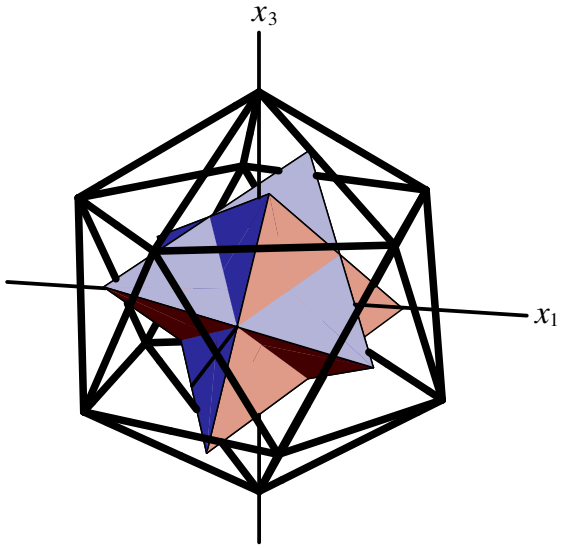
It has degree 60, as it must.

Before continuing, here is a little more geometry. As already shown in Josh's figure, before projecting the icosahedron to the plane, we repositioned it to have vertices at the north and south poles.

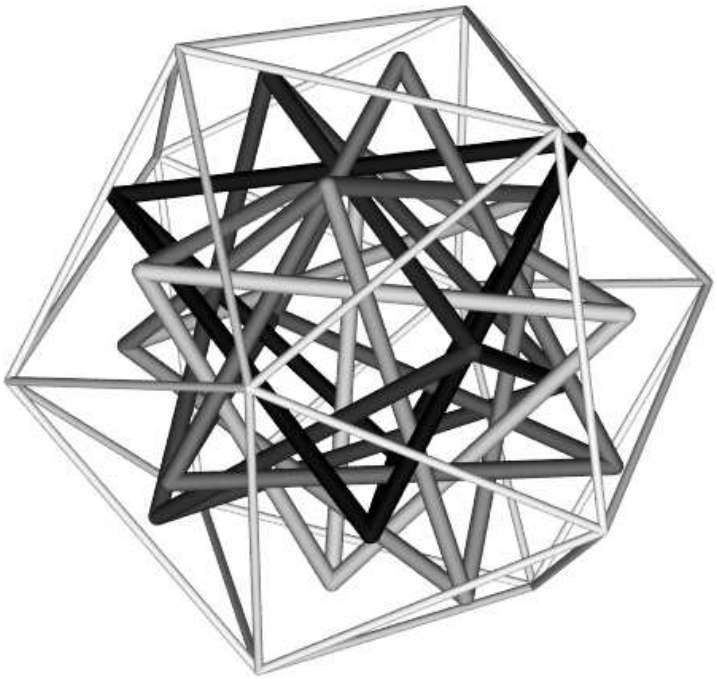
Here is the rotated icosahedron.



Two tetrahedra, one counter to the other, sit naturally in the rotated icosahedron.



In fact, rather than five golden configurations, we can embed five tetrahedra in the icosahedron.



A very similar picture would show the *countertetrahedron* and its four translates embedded instead.

Klein singled out the tetrahedron with vertex $(1, 1, 1)$ (up to scaling). Its rotation group is a subgroup of the icosahedral rotation group, naturally isomorphic to $A_4$. The four objects being permuted here can be viewed the tetrahedron vertices, or the tetrahedron faces, or the four diagonals of the cube whose vertices form the tetrahedron and countertetrahedron.

Klein computed a complex analytic function that is invariant under the group of tetrahedral rotations,

$$f_T = \left( \frac{Z^4 + 2i\sqrt{3}Z^2 + 1}{Z^4 - 2i\sqrt{3}Z^2 + 1} \right)^3 .$$

This is Klein's tetrahedral invariant. Its degree is 12, as it must be.

Klein used the transcendental function $f_I^{-1}$ (a 1-to-60 multiple-valued function) to solve the Brioschi quintic, as follows.

Given the Brioschi quintic

$$b_w(T) = T^5 - 10wT^3 + 45w^2T - w^2$$

with the parameter $w$ determining its coefficients.

- The icosahedral inverse gives 60 values $z$ in $f_I^{-1}(w)$.

- Then $f_T(z)$ for these 60 $z$-values gives 5 $t$-values.

- The Brioschi quintic's roots are certain rational functions of the $t$-values.

For the sextic (degree 6) polynomial, an analogue of the icosahedron exists in two-dimensional complex projective space, and its rotation group is $A_6$.

The general sextic reduces to a two-parameter form, which can be solved by geometric methods analogous to Klein's icosahedron techniques for the quintic. **Fricke** did so early in the 20th century.

Returning to Klein, he expressed his transcendental function $f_I^{-1}$ in two ways:

- using hypergeometric series,

- using elliptic modular functions.

Another way to construct transcendental functions is by *iteration*, a process ideally suited for computers.

**Doyle** and **McMullen** showed how to solve the quintic by iteration in a late-1980's paper.

## Newton's method for $n$th roots

Solve the equation

$$p(T) = 0$$

where

$$p(T) = T^n - 1.$$

Newton: Define

$$\begin{aligned} f(T) &= T - \frac{p(T)}{p'(T)} \\ &= \frac{(n-1)T^n + 1}{nT^{n-1}}. \end{aligned}$$

Iterate $f$. That is, take an initial guess $t_0$, and then let

$$t_1 = f(t_0), \quad t_2 = f(t_1), \quad \text{etc.}$$

For "every" initial guess, the iteration will converge to some $n$th root of 1.

## A family of related problems

Solve the equation

$$p_w(T) = 0$$

where

$$p_w(T) = T^n - w.$$

Newton: Define

$$\begin{aligned} F_w(T) &= T - \frac{p_w(T)}{p'_w(T)} \\ &= \frac{(n-1)T^n + w}{nT^{n-1}}. \end{aligned}$$

For that matter, treat the parameter $w$ as another formal symbol,

$$F_W(T) = \frac{(n-1)T^n + W}{nT^{n-1}}.$$

(Continued on next slide.)

The sets

$$\{n\text{th roots of } w\}$$

and

$$\{n\text{th roots of } 1\}$$

are the *same shape*. Dividing the first pointwise by any of its elements gives the second.

To express this in formal symbols, introduce $Z$ where $Z^n = W$, and define

$$\phi_Z(T) = \frac{T}{Z},$$

so that

$$\phi_Z^{-1}(T) = ZT.$$

(So,

- $W$ is a formal symbol for the problem-parameter,
- $Z$ is a formal symbol for a root,
- $T$ is a formal symbol for the iteration-variable.)

Then a direct calculation shows that

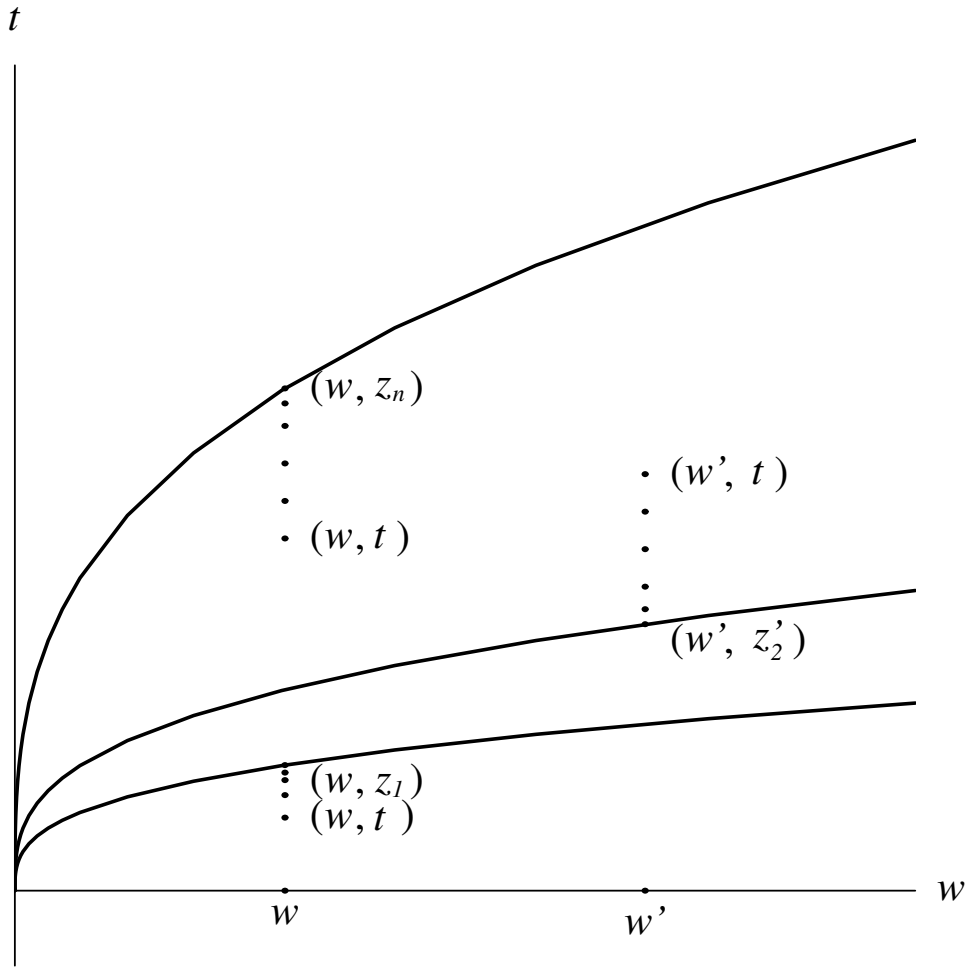
$$F_W(T) = (\phi_Z^{-1} \circ f \circ \phi_Z)(T).$$

That is, the *general* $W$-parameterized iteration equals a $Z$-parameterized *conjugate* of *one model iteration*.

And so, since $f$ is generally convergent, so is $F_W$.

Whatever else it may accomplish, **iteration subsumes adjoining radicals**.

Here is a schematic of the configuration.



Each vertical section is the iteration environment for one value of the parameter $w$. The vertical sections all look the same, and the general iteration consists of conjugating to one particular vertical section, iterating there, and then conjugating back. In symbols,

$$F_W^j(T) = (\phi_Z^{-1} \circ f^j \circ \phi_Z)(T), \quad j \geq 1.$$

But this is all invisible to us computationally! We don't know $z$. We just iterate $F_w$ happily.

Still, study the situation a bit further.

Since $\phi_Z^{-1} f \phi_Z$ depends only on $W = Z^n$, necessarily for $k = 0, 1, \ldots, n-1$ (letting $\zeta = e^{2\pi i/n}$),

$$\phi_Z^{-1} f \phi_Z = \phi_{\zeta^k Z}^{-1} f \phi_{\zeta^k Z}.$$

That is, for $k = 0, 1, \ldots, n-1$,

$$\rho(k)^{-1} f \rho(k) = f,$$

where

$$\rho(k) = \phi_{\zeta^k Z} \cdot \phi_Z^{-1},$$

i.e.,

$$\rho(k)(T) = \frac{1}{\zeta^k Z} \cdot ZT = \frac{T}{\zeta^k}.$$

That is, $\rho$ is a *representation* from $\mathbf{Z}/n\mathbf{Z}$ to the automorphism group of $T$-space.

Each $\rho(k)$ is an automorphism of $T$-space that commutes with the iteration model $f$.

These ideas are quite general.

Suppose that we have symbols $W_1, \ldots, W_m$ and $Z_1, \ldots, Z_m$, where we think of the $W$'s as known parameters for a family of polynomials, and as the $Z$'s as the corresponding unknown roots. Let $Z$ be shorthand for $(Z_1, \ldots, Z_m)$ and similarly for $W$. Assume that $\mathbf{C}(Z)$ is Galois over $\mathbf{C}(W)$ with Galois group $\Gamma$.

Suppose also that we have

- A *model iteration*

$$f \in \mathbf{C}(T).$$

- A *conjugating transformation*

$$\phi_Z(T) \in \mathbf{C}(Z)(T).$$

- A *representation* (injective homomorphism)

$$\rho : \Gamma \longrightarrow \mathrm{Aut}(\mathbf{P}^1\mathbf{C}).$$

(Continued on next slide.)

Our model iteration $f$, our conjugating transformation $\phi_Z$, and our representation $\rho$ are assumed to satisfy the following conditions:

- $\phi_{\gamma(Z)} = \phi_Z \circ \rho(\gamma)$ for all $\gamma$,
- $\rho(\gamma)^{-1} f \rho(\gamma) = f$ for all $\gamma$,
- $f$ is generally convergent.

Then the conjugate

$$F(T) = (\phi_Z^{-1} f \phi_Z)(T)$$

lies in $\mathbf{C}(W)(T)$ (i.e., we can *compute* it), and it is generally convergent.

McMullen showed that the converse holds too.

If $F_W(T)$ is generally convergent, then it takes the form

$$F_W = \phi_Z^{-1} f \phi_Z$$

for $f$, $\phi_Z$, and $\rho = \phi_{\gamma Z} \circ \phi_{Z^{-1}}$ as above.

This is exciting because it is *predictive*. It tells us what generally convergent algorithms can exist. And then to search for them, we take a representation $\rho$ and try to find $f$ and $\phi$ that commute with $\rho$ suitably.

Klein's Theorem: Representations

$$\rho : \Gamma \longrightarrow \mathrm{Aut}(\mathbf{P}^1\mathbf{C})$$

can exist only for

$\Gamma = C_n$ cyclic group,

$\Gamma = D_n$ dihedral group,

$\Gamma = A_4$ tetrahedral group,

$\Gamma = S_4$ octahedral group,

$\Gamma = A_5$ icosahedral group – bingo!

Doyle and McMullen used Klein's icosahedral calculations to find a model iteration $f$ and a conjugating transformation $\phi_Z$ for $\rho : A_5 \longrightarrow \Gamma_I$.

Recall that $W$ is the Brioschi parameter, describing the Brioschi quintic

$$b_W(T) = T^5 - 10WT^3 + 45W^2T - W^2,$$

and $Z$ is related to $W$ by the condition

$$f_I(Z) = W.$$

Doyle and McMullen expressed the composition

$$F(T) = (\phi_Z^{-1} f \phi_Z)(T)$$

as an element of $\mathbf{C}(W)(T)$, and thereby solved the Brioschi quintic by iteration.

The model for the Brioschi quintic iteration:

$$f_{11}(T) = -\frac{T^{11} + 66T^6 - 11T}{11T^{10} + 66T^5 - 1}.$$

## Solution of the Brioschi quintic

Define parameterized polynomials

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

and

$$
\begin{aligned}
k_{\widehat{W}}(T) = {} & 100\widehat{W}(\widehat{W} - 1)\cdot \\
& \Big[(1215T - 648)\widehat{W}^4 \\
& \quad + (-540T^3 - 216T^2 - 1152T + 640)\widehat{W}^3 \\
& \quad + (378T^5 - 504T^4 + 960T^3)\widehat{W}^2 \\
& \quad + (36T^7 - 168T^6)\widehat{W} - T^9\Big].
\end{aligned}
$$

To solve any specific Brioschi quintic

$$b_w(T) = T^5 - 10wT^3 + 45w^2T - w^2, \quad w \in \mathbf{C},$$

proceed as follows.

- Let $\widehat{w} = 1 - 1728w$ and specialize $h$ and $k$ to $h_{\widehat{w}}(T)$ and $k_{\widehat{w}}(T)$, polynomials in $\mathbf{C}[T]$.

- Iterate the rational function

$$F_{\widehat{w}}(T) = T - 12\frac{h_{\widehat{w}}(T)}{h'_{\widehat{w}}(T)} \in \mathbf{C}(T)$$

  an even number of times on a random initial guess $t$ until the iteration converges to some value $t_1$. Set $t_2 = F_{\widehat{w}}(t_1)$.

- Set

$$\mu_1 = \frac{k_{\widehat{w}}(t_1)}{h_{\widehat{w}}(t_1)} \quad \text{and} \quad \mu_2 = \frac{k_{\widehat{w}}(t_2)}{h_{\widehat{w}}(t_2)}.$$

Then

$$s_1 = \frac{9 - i\sqrt{15}}{90}\mu_1 + \frac{9 + i\sqrt{15}}{90}\mu_2,$$

and

$$s_2 = \frac{9 + i\sqrt{15}}{90}\mu_1 + \frac{9 - i\sqrt{15}}{90}\mu_2$$

are a pair of Brioschi roots.

Finding the other three roots now reduces to solving a cubic equation, a process that can be carried out by further iteration, or by radicals.

## Some References

- Klein's icosahedron book (early 1880's, now in Dover reprint)

- Dickson, *Modern Algebraic Theories* (1926)

- Doyle–McMullen, *Solving the Quintic by Iteration* (1988 or 1989)

- JS, *Geometry of the Quintic* (1995)

(And Doyle's student, Scott Crass, was continuing to work on iterative methods for solving polynomials when I lost touch with the subject some ten years ago.)