26. J. E. McKenna, Computers and experimentation in mathematics, this MONTHLY, 79 (1972) 294–295.
27. E. W. McWhorter, The small electronic calculator, Scientific American, 234 (1976) 88–98.
28. M. S. Menzin, Use of canned computer programs in freshman calculus, this MONTHLY, 83 (1976) 375–378.
29. E. P. Miles, Jr., Calculus and the computer, the CRICISAM calculus project—Past, present and portent, this MONTHLY, 78 (1971) 284–291.
30. R. V. Morgan and T. T. Warnock, Derivatives on the hand-held calculator, Mathematics Teacher, 71 (1978) 532–537.
31. T. O'Loughlin, Using electronic programmable calculators (mini-computers) in calculus instruction, this MONTHLY, 83 (1976) 281–283.
32. B. L. Osofsky, Small calculators for the mathematician, Notices of the American Mathematical Society, 23 (1976) 422–430.
33. L. Råde, Take a Chance with Your Calculator: Probability Problems for Programmable Calculators, Dilithium Press, Forest Grove, Ore., 1977.
34. L. B. Rall, ed., Error in Digital Computation, vol. 1, Wiley, New York, 1965.
35. J. B. Rosser, Mathematics courses in 1984, this MONTHLY 79 (1972) 635–648.
36. J. B. Scarborough, Numerical Mathematical Analysis, 5th ed., Johns Hopkins Press, Baltimore, 1962.
37. Scientific calculators, Consumer Reports, 41 (1976) 86–87.
38. C. J. Sippl, Calculator Users Guide and Dictionary, Matrix Publishers, Inc., Champaign, Ill., 1978.
39. R. J. Sippl and C. J. Sippl, Programmable Calculators: How to Use Them, Matrix Publishers, Inc., Champaign, Ill., 1978.
40. D. A. Smith, Numerical differentiation for calculus students, this MONTHLY, 82 (1975) 284–287.
41. J. M. Smith, Scientific Analysis on the Pocket Calculator, Wiley, New York, 1975.
42. ______, Financial Analysis and Business Decisions on the Pocket Calculator, Wiley, New York, 1976.
43. I. A. Stegun and M. Abramowitz, Pitfalls in Computation, J. Soc. Indust. Appl. Math., 4 (1956) 207–219.
44. W. B. Stenberg and R. J. Walker, Calculus: A Computer Oriented Presentation, CRICISAM, Florida State University, Tallahassee, Fla., 1968.
45. G. L. Thesing and C. A. Wood, Using the computer as a discovery tool in calculus, this MONTHLY, 81 (1974) 163–168.
46. S. Thiagarajan and H. D. Stolovitch, Games with the Pocket Calculator, Dilithium Press, Forest Grove, Ore., 1976.
47. N. Ya. Vilenkin, Successive Approximation, translated and adapted from the Russian by M. B. P. Slater and J. W. Teller, Pergamon Press, distributed by Macmillan Company, New York, 1964.
48. J. H. Wilkinson, Rounding Errors in Algebraic Processes, Prentice-Hall, Englewood Cliffs, N.J. 1963.
49. D. Williams and A. Tobin, Philadelphia minicalculator program, Mathematics Teacher, 71 (1978) 471–472.
50. H. E. Williams and D. De Boer, Teaching a computer-oriented laboratory course for ordinary differential equations, this MONTHLY, 80 (1973) 933–937.

DEPARTMENT OF MATHEMATICAL SCIENCES, UNIVERSITY OF NEVADA, LAS VEGAS, NV 89154.

WHEN IS $f(f(z)) = az^2 + bz + c$?

R. E. RICE, B. SCHWEIZER, AND A. SKLAR

1. Introduction. The surprising answer to the title question is: *never*. In this paper we prove this assertion and more: we prove that a quadratic polynomial defined on the entire complex

---

Richard E. Rice received his Ph.D. from the University of Massachusetts in 1977 with B. Schweizer. He has taught at Union College and is now with the Boeing Company. His main interests are functional equations, combinatorics, and graph theory.

Berthold Schweizer received his Ph.D. from the Illinois Institute of Technology in 1956 with K. Menger. He has taught at the University of California at Los Angeles and the University of Arizona, and is now a professor at the University of Massachusetts. His principal interests are functional equations and inequalities, function systems, and probabilistic geometry.

Abe Sklar received his Ph.D. from the California Institute of Technology in 1956 with T. M. Apostol. He has taught at the University of Arizona and is now a professor at the Illinois Institute of Technology. His principal interests are analytic number theory, functional equations, function systems, and probabilistic geometry.—*Editors*

plane has no iterative roots whatever.

To make this statement precise, we need a few definitions. Let E be a set and let f,g be functions mapping E into itself. The *composite* of f and g is the function $f\circ g$ defined by

$$(f\circ g)(x)=f(g(x)),\quad \text{for all } x \text{ in } E. \tag{1.1}$$

The *iterates* of f are the functions f^n defined recursively by:

$$f^0(x)=x,\quad \text{for all } x \text{ in } E, \tag{1.2}$$

$$f^{n+1}=f\circ f^n,\quad \text{for any nonnegative integer } n. \tag{1.3}$$

And, for any integer $r\geqslant 2$, f is an *iterative root of order* r *of* g, or an rth *iterative root of* g, if

$$f^r=g. \tag{1.4}$$

We can now formally state our principal result as:

THEOREM 1. *Let P be a polynomial of degree 2 defined on the entire complex plane C. Then P has no iterative roots of any order whatever; i.e., for any integer $r\geqslant 2$, there exists no function f whatever mapping C into itself such that $f^r=P$.*

It must be emphasized that the phrase "no function f whatever" is to be taken literally and does not mean merely "no entire function" or "no continuous function," etc. From this it is to be expected that none of the usual methods of analysis or topology play a role in what follows. This is the case. The proof of Theorem 1 is, in essence, purely combinatorial. The necessary tools for this proof are developed in Sections 2 and 3. Iterative square roots are discussed in Section 4, which culminates in the answer to the title question. The proof of Theorem 1 is completed in Section 5. Section 6 contains supplementary material, stated without proof; in particular, the conclusion of Theorem 1 is contrasted to the quite different situation for real quadratic polynomials.

Experience has shown that many mathematicians, analysts in particular, when confronted by the statement of Theorem 1, respond with the following instant "counterexample":

"Take $P(z)=z^2$, and let f be a branch, say, the principal one, of the $\sqrt{2}$th power, i.e., let $z\neq 0$ be expressed in the form

$$z=re^{i\theta},\quad r>0,\quad -\pi<\theta\leqslant\pi. \tag{1.5}$$

Define $f: C\to C$ by

$$f(0)=0,\quad f(z)=r^{\sqrt{2}}e^{i\theta\sqrt{2}} \text{ for } z\neq 0. \tag{1.6}$$

Then $f(f(0))=0=0^2$ and for any $z\neq 0$,

$$f(f(z))=f\left(r^{\sqrt{2}}e^{i\theta\sqrt{2}}\right)=\left(r^{\sqrt{2}}\right)^{\sqrt{2}}e^{i\theta\sqrt{2}\sqrt{2}}=r^2e^{2i\theta}=z^2. \tag{1.7}$$

Thus f is an iterative square root of P, contradicting the alleged Theorem 1."

The flaw in this argument lies in the fact that the second equality in (1.7) fails when $f(z)$, as defined in (1.6), is not in the same standard form as z in (1.5). Indeed, an explicit calculation, with proper attention paid to necessary details, yields:

$$f^2(z)=\begin{cases} z^2e^{i2\pi\sqrt{2}}, & -\pi<\theta\leqslant -\dfrac{\pi}{\sqrt{2}},\\ z^2, & -\dfrac{\pi}{\sqrt{2}}<\theta\leqslant\dfrac{\pi}{\sqrt{2}} \text{ or } z=0,\\ z^2e^{-i2\pi\sqrt{2}}, & \dfrac{\pi}{\sqrt{2}}<\theta\leqslant\pi, \end{cases}$$

whence $f^2 \neq P$, since, e.g., $f^2(-1) = e^{-i2\pi\sqrt{2}} = -.858216 - i.513288 \neq 1 = P(-1)$. (The fact that f^2 and P coincide on part of their common domain is irrelevant: equality of functions means equality *everywhere*.)

(The same flaw has often affected the discussion of certain real quadratic polynomials, e.g., x^2-2. See this MONTHLY, problem E984 [1951, 564] and its treatment [1952, 252; 1976, 567; 1977, 739; 1980, 303].)

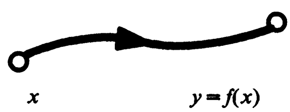
On the other hand, the validity of statements such as Theorem 1 is heavily domain-dependent. On the real line, for example, the function f_r defined by $f_r(x) = |x|^{2^{1/r}}$ for any $r \geqslant 2$ is an iterative rth root of the polynomial P given by $P(x) = x^2$.

The problem of finding iterative roots of functions dates back at least to Abel [1] and Babbage [2] (see also [5], especially Chapters 4 and 7). Since then it has attracted the attention of many authors. A comprehensive survey of the theory of iteration of continuous real functions, together with an extensive bibliography, is given in [7]. Further references may be found in the papers [3] and [6].

2. Orbits. Let E be a set, f a function from E into E, and $\sim_f$ the relation on E defined via:

$$x \sim_f y \text{ if and only if } f^m(x) = f^n(y) \tag{2.1}$$

for some nonnegative integers m, n. It is immediate that $\sim_f$ is an equivalence relation. Each equivalence class of $\sim_f$ determines a directed graph, called an *orbit of f* or *f-orbit*, which is constructed as follows: With each element x of an equivalence class, associate a point, called a *vertex*; and if $f(x) = y$, join the vertex representing x to the one representing y by an arc, called an *edge*, directed from x to y, thus:



In view of (2.1), an f-orbit is connected. It is also maximal in the sense that no further vertices or edges can be added. Since f is a function, and thus single-valued by definition, it is clear that while a finite, countable, or uncountable number of edges can enter a given vertex, exactly one edge exits. (Note that a point on the conventional graph of a real function, since it has coordinates of the form $(x, f(x))$, corresponds to an edge of an f-orbit.)

Orbits are divided into two types: cyclic (see Figs. 2 and 3) and acyclic (see Fig. 1). An f-orbit is *cyclic* if it contains a vertex x such that $f^n(x) = x$ for some $n > 0$. The vertices $x, f(x), \ldots, f^{n-1}(x), f^n(x) = x$ form a *cycle*. There is no "escape" from a cycle, whence an f-orbit cannot contain more than one cycle. The number of distinct vertices in the cycle of a cyclic orbit is the *order* of the cycle; a cycle of order n is called an *n-cycle*; and the orbit containing it, an *n-cyclic* orbit. Note that a 1-cycle corresponds to a fixed point of the function f and that the vertices of an n-cycle of f correspond to fixed points of its nth iterate f^n.

An orbit which is not cyclic is *acyclic*. An acyclic orbit must have at least countably many vertices whereas a cyclic orbit may have as few as one.

Iteration of a function generally splits its orbits. For the second iterate f^2, we have:

LEMMA 1. *For any function f*:

(a) *An acyclic f-orbit is the union of two acyclic f^2-orbits* (*see Fig. 1*).

(b) *A cyclic f-orbit of even order, say* $2m$, *is the union of two cyclic f^2-orbits of order m* (*see Fig. 2*).

(c) *A cyclic f-orbit of odd order, say* $2m+1$, *is a cyclic f^2-orbit of the same order. The graphs of these orbits are generally different* (*see Fig. 3*).

Proof. Suppose $y \sim_f x$. Then there are non-negative integers m, n such that $f^m(x) = f^n(y)$. If m and n are both even or both odd, then $y \sim_{f^2} x$; otherwise $y \sim_{f^2} f(x)$. On the other hand, it is

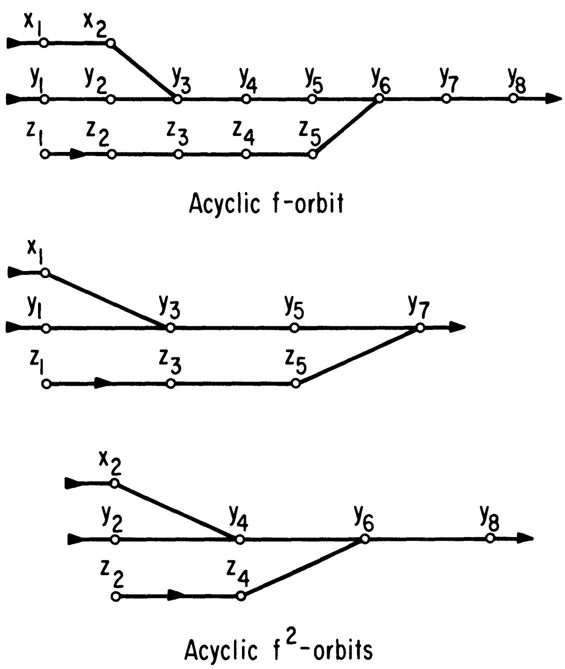

Acyclic f-orbit
Acyclic f²-orbits

FIG. 1

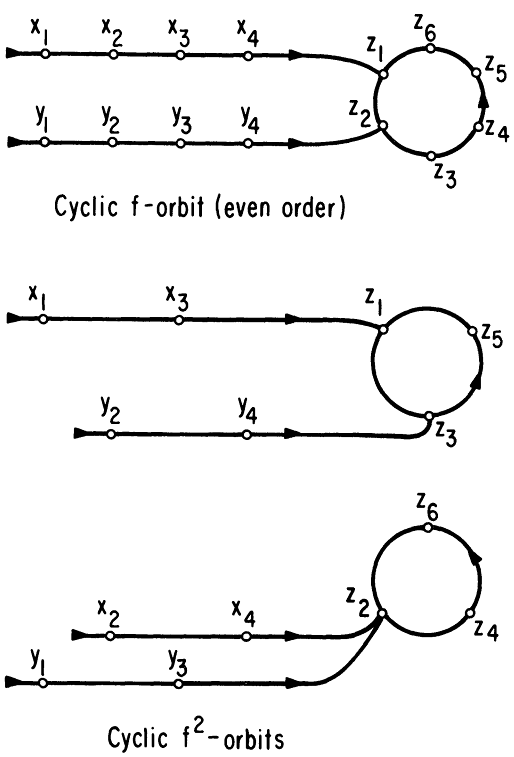

Cyclic f-orbit (even order)
Cyclic f²-orbits

FIG. 2

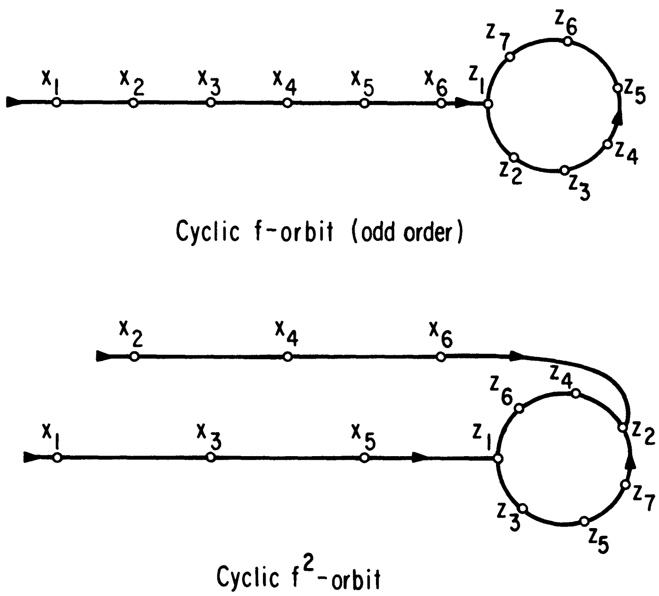


FIG. 3

immediate that either $y \sim_{f^2} x$ or $y \sim_{f^2} f(x)$ implies $y \sim_f x$. It follows that the f-orbit containing x is the (set-theoretical) union of the f^2-orbit containing x and the f^2-orbit containing $f(x)$. These two f^2-orbits coincide if and only if $x \sim_{f^2} f(x)$, i.e., if and only if there are nonnegative integers m, n such that

$$f^{2m}(x) = f^{2n+1}(x). \tag{2.2}$$

Let $p = \min(2m, 2n+1)$ and $q = |2n+1-2m|$. Note that q is odd, hence necessarily positive. Note also that $p+q = \max(2m, 2n+1)$, whence (2.2) is equivalent to

$$f^p(x) = f^{p+q}(x).$$

Hence upon setting $w = f^p(x)$, we have

$$f^q(w) = f^{p+q}(x) = f^p(x) = w,$$

which means that the f-orbit containing x is cyclic, and that its order, which must divide q, is odd. This proves (a), and, apart from the exact orders of the f^2-cycles, (b) and (c) as well.

To determine these orders, let x_0 be a vertex in the cycle of a cyclic f-orbit, and set $x_p = f^p(x_0)$ for every nonnegative integer p. If the order of the cyclic f-orbit is $2m$, then it is easily seen that $\{x_0, x_2, \ldots, x_{2m-2}\}$ is the cycle, of order m, of the f^2-orbit containing x_0, and $\{x_1, x_3, \ldots, x_{2m-1}\}$ is the cycle, of order m, of the f^2-orbit containing $f(x_0) = x_1$. If the order of the cyclic f-orbit is $2m+1$, then

$$x_{2m+2} = f^{2m+2}(x_0) = f(f^{2m+1}(x_0)) = f(x_0) = x_1,$$

whence it follows that $\{x_0, x_2, \ldots, x_{2m}, x_1, x_3, \ldots, x_{2m-1}\}$ is the cycle, of order $2m+1$, of the f^2-orbit containing x_0. This completes the proof.

Note that in cases (a) and (b) each f^2-orbit consists of "every other" vertex of the f-orbit. Note also that the property of being in or not in the cycle of a cyclic orbit is preserved under iteration.

Lemma 1 shows that a cyclic f^2-orbit of even order, say $2m$, can only arise from the splitting of a cyclic f-orbit of order $4m$. But since such an f-orbit splits into two f^2-orbits, it follows that the number, if finite, of $2m$-cyclic f^2-orbits must be even. Hence we have:

LEMMA 2. *Let g be a function. Then a necessary condition for g to have an iterative square root, i.e., for there to exist a function f such that $f^2=g$, is that for any positive even integer 2m the number (if finite) of 2m-cyclic g-orbits is even.*

The equivalence relation (2.1) was introduced by K. Kuratowski in a brief remark at the end of [**12**]. It was apparently G. T. Whyburn [**14**] (see also [**15**, Chapter 12, § 6]) who extended the term *orbit*, already used in related connections, to cover Kuratowski's definition. In [**6**], a basic and beautiful paper which deserves to be much better known, R. Isaacs obtained conditions on orbits that are both necessary and sufficient for the existence of iterative square roots of arbitrary functions. (In contrast, our Lemma 2 only yields a necessary condition; but this is adequate for our purpose.) Recently G. Zimmermann (née Riggert) has significantly extended Isaacs's results (see [**11**] and [**16**, § 1]).

3. Conjugacy. Let g be a function mapping a set E_1 into itself, and h a function mapping a set E_2 into itself. We say that g and h are *conjugate* if there exists a one-to-one function f mapping E_1 onto E_2 such that

$$f\circ g=h\circ f. \tag{3.1}$$

Equivalently, we could write either

$$g=f^{-1}\circ h\circ f \quad \text{or} \quad h=f\circ g\circ f^{-1}, \tag{3.2}$$

where f^{-1} is the inverse of f. Clearly, conjugacy is an equivalence relation among functions. Furthermore, we have:

THEOREM 2. *Let g be a function mapping a set E_1 into itself, and h a function mapping a set E_2 into itself. Then g and h are conjugate if and only if g and h are (orbit-)* isomorphic, *i.e., if and only if there exists a one-to-one function f mapping E_1 onto E_2 such that, for any x,y in E_1, and any nonnegative integers m,n we have*

$$g^m(x)=g^n(y) \quad \text{if and only if } h^m(f(x))=h^n(f(y)). \tag{3.3}$$

Proof. If g and h are conjugate, then an induction using (3.1) yields $f\circ g^m=h^m\circ f$ for any nonnegative integer m. Hence $f(g^m(x))=f(g^n(y))$ if and only if $h^m(f(x))=h^n(f(y))$. But since f is one-to-one, $f(g^m(x))=f(g^n(y))$ if and only if $g^m(x)=g^n(y)$. Therefore g and h are (orbit-) isomorphic.

In the other direction, if g and h are isomorphic, let x be any element of E_1 and let $y=g(x)$. Then, using (3.3) with $m=1$ and $n=0$, we have

$$h(f(x))=f(y)=f(g(x)),$$

which yields (3.1), since x is arbitrary. Note that Theorem 2 can be compactly summarized by the statement: "The diagram in Figure 4 commutes."

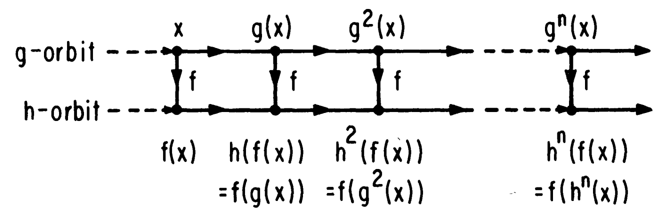


FIG. 4

In other words, two functions are conjugate if and only if their orbit structures are identical. This result goes back at least to 1960: it appears, e.g., in [**13**, Chapter 6, § 2], with orbits entering under the name "trees."

As an immediate consequence of Theorem 2 we have:

LEMMA 3. *If g and h are conjugate, and r is any integer* $\geqslant 2$, *then g has an iterative rth root if and only if h has an iterative rth root.*

Proof. Let g and h be conjugate via f and suppose that $\phi^r = g$. Let $\psi = f\circ\phi\circ f^{-1}$. Then $\psi^r = f\circ\phi^r\circ f^{-1} = f\circ g\circ f^{-1} = h$.

It follows from Theorem 2 and Lemma 3 that the existence or nonexistence of iterative roots of a function depends only on its orbit structure.

Two functions f and g defined on the complex plane C are *linearly conjugate* if there exists a nonconstant linear function L such that

$$L\circ f = g\circ L. \tag{3.4}$$

Since any such function L is a one-to-one mapping of C onto itself, it is clear that linear conjugacy is a special case of conjugacy.

We now turn our attention to quadratic polynomials P defined on C. Since we are interested in fixed points, i.e., roots of the equation $P(z) = z$, we use the standard form

$$P(z) = az^2 + (b+1)z + c, \tag{3.5}$$

where a, b, c are in C and $a \neq 0$. For any such polynomial P we define $\Delta(P)$, the *iterative discriminant* of P, by

$$\Delta(P) = b^2 - 4ac. \tag{3.6}$$

We then have the following basic:

LEMMA 4. *If P and Q are quadratic polynomials on C, then P and Q are linearly conjugate if and only if* $\Delta(P) = \Delta(Q)$; *i.e.,* Δ *is a complete invariant for linear conjugacy of quadratic polynomials.*

Proof. Let $P(z) = az^2 + (b+1)z + c$ and $Q(z) = a'z^2 + (b'+1)z + c'$. Then P and Q are linearly conjugate if and only if there exists a linear function $L(z) = Az + B$, with $A \neq 0$, such that for all z in C,

$$\begin{aligned} L(P(z)) &= Aaz^2 + A(b+1)z + Ac + B = Q(L(z)) \\ &= A^2a'z^2 + [2ABa' + A(b'+1)]z + B^2a' + B(b'+1) + c'. \end{aligned} \tag{3.7}$$

Now (3.7) holds for all z in C if and only if

$$Aa = A^2a', \tag{3.8}$$

$$A(b+1) = A(2Ba' + b' + 1), \tag{3.9}$$

$$Ac + B = B^2a' + B(b'+1) + c'. \tag{3.10}$$

Solving (3.8) and (3.9) for A and B yields,

$$A = a/a' \quad \text{and} \quad B = (b-b')/2a', \tag{3.11}$$

whence the system (3.8), (3.9), (3.10) has a solution if and only if the substitution of A and B, as given by (3.11), into (3.10), yields an identity—that is, upon simplification, if and only if $b^2 - 4ac = b'^2 - 4a'c'$ or, equivalently, $\Delta(P) = \Delta(Q)$.

Now consider the family $\{P_\lambda\}$ of quadratic polynomials given by

$$P_\lambda(z) = z^2 + (1-\lambda)z = z(z-\lambda) + z, \tag{3.12}$$

where $\lambda = \mu + i\nu$ is such that either $\mu > 0$, or $\mu = 0$ and $\nu \geqslant 0$. We have $\Delta(P_\lambda) = \lambda^2$, whence the family $\{P_\lambda\}$ contains a single representative from each linear conjugacy class. Consequently, the problem of determining those quadratic polynomials which have iterative roots reduces at once to the problem of determining those values of λ for which P_λ has iterative roots.

4. Iterative square roots. To answer the question of the title, we begin with:

LEMMA 5. *A quadratic polynomial P has at most one 2-cyclic orbit.*

Proof. The two vertices in the 2-cycle of any 2-cyclic P-orbit are distinct solutions of the equation

$$P^2(z)=z. \tag{4.1}$$

But any fixed point of P is also a solution of (4.1), and by the Fundamental Theorem of Algebra, P has at least one fixed point. Thus if P had two or more 2-cyclic orbits then (4.1) would have 5 or more distinct solutions. But this is impossible since P^2 is a polynomial of degree 4.

If P has one 2-cyclic orbit, then Lemma 2 shows that P has no iterative square roots. Hence the only quadratic polynomials which can conceivably have iterative square roots are those which have no 2-cyclic orbits. To find such polynomials, we consider the family $\{P_\lambda\}$ defined in (3.12). A straightforward computation yields

$$P_\lambda^2(z)=z(z-\lambda)\left[z^2+(2-\lambda)z+(2-\lambda)\right]+z. \tag{4.2}$$

The roots of the equation $P_\lambda^2(z)=z$ are $0,\lambda$,

$$z_3=(\lambda-2+\sqrt{\lambda^2-4})/2 \quad \text{and} \quad z_4=(\lambda-2-\sqrt{\lambda^2-4})/2.$$

Now, 0 and λ are the fixed points of P_λ. Thus, since $P(z_3)=z_4$ and $P(z_4)=z_3$, P has no 2-cyclic orbit if and only if $z_3=z_4$; and this is the case if and only if $\lambda^2=4$. Since $\Delta(P_\lambda)=\lambda^2$, this yields:

LEMMA 6. *If P is a quadratic polynomial defined on C and if $\Delta(P)\neq 4$, then P has exactly one 2-cyclic orbit and hence no iterative square root.*

Lemma 6 shows that—up to linear conjugacy—there is exactly one complex quadratic polynomial which has no 2-cyclic orbit. This result is not new. Indeed, in **[3]** I. N. Baker has shown that, with the sole exception of P_2, which lacks only a 2-cyclic orbit, all complex polynomials have cyclic orbits of all orders. Also, it should be remarked that R. Isaacs noted in **[6]** that $P(z)=z^2$ has exactly one 2-cycle (the complex cube roots of unity) and hence no iterative square roots.

For $\Delta(P)=4$ we have $\lambda=2$, $P_2(z)=z^2-z$ and $z_3=z_4=0$. We now dispose of this one remaining case by proving:

LEMMA 7. *If P is a complex quadratic polynomial with $\Delta(P)=4$, then P has three 4-cyclic orbits. Hence by Lemma 2, P has no iterative square roots.*

Proof. If P is any complex quadratic polynomial, then P^4 is a polynomial of degree $2^4=16$. Since P has at least one fixed point, a counting argument similar to the one used in the proof of Lemma 5 shows that P has at most three 4-cyclic orbits. Turning specifically to P_2, we find after some computation that

$$P_2^4(z)=z^3(z-2)Q(z)+z,$$

where

$$Q(z)=\left[z^2(z-2)+1\right]^3(z^3+1)+1.$$

Thus the solutions of the equation $P_2^4(z)=z$, i.e., the fixed points of P_2^4, are 0, 2, and the roots of the equation $Q(z)=0$. Of these, 0 and 2 are the fixed points of P_2, and direct evaluation shows that neither is a root of $Q(z)=0$. Consequently, since P_2 has no 2-cycle, the roots of $Q(z)=0$ are precisely the vertices in the 4-cycles of P_2. It remains to show that these roots are all distinct. Suppose they are not. Then Q and its derivative Q' have a common factor. Now

$$Q'(z)=6z\left[z^2(z-2)+1\right]^2[2z^4-3z^3+2z-2].$$

It is immediate that the roots of $z^2(z-2)+1=0$ are not roots of $Q(z)=0$. Since we already know that 0 is not a root of $Q(z)=0$, it follows that any common factor of Q and Q' must be a common factor of Q and B, where

$$B(z)=2z^4-3z^3+2z-2.$$

But B is a polynomial of degree 4, and $Q(z)=0$ has either 4, 8, or 12 *distinct* roots (since these roots, being the vertices in the 4-cycles of P_2, come in bunches of 4). Thus if Q and Q' have one common factor, then Q and Q' must have four distinct common factors, whence B must divide Q. However, by direct calculation we find that

$$2^9Q(z)=B(z)D(z)+R(z), \tag{4.3}$$

where

$$D(z)=256z^8-1152z^7+1344z^6+736z^5-2096z^4$$
$$+504z^3+852z^2-498z-275,$$

and

$$R(z)=527z^3-372z^2-446z+474.$$

Thus B does not divide Q, the roots of $Q(z)=0$ are all distinct, and P_2 has three 4-cyclic orbits. Since the same conclusion holds for any P linearly conjugate to P_2, the proof of Lemma 7 is complete.

The long division indicated in (4.3) can be avoided by noting that Q and B are both primitive polynomials. If B divides Q, then $Q(z)=B(z)A(z)$, where A has rational coefficients. By a variant of Gauss's Lemma (see e.g., [**4**, pp. 168–169]), it follows that A has integer coefficients. Consequently, the leading coefficient of B, namely, 2, divides the leading coefficient of Q, namely, 1, which is false.

Combining Lemmas 6 and 7, we obtain:

THEOREM 3. *Let P be a quadratic polynomial defined on the complex plane C. Then P has no iterative roots of order 2, i.e., there exists no function f whatever such that*

$$f(f(z))=P(z) \quad \text{for all } z \text{ in } C. \tag{4.4}$$

5. Proof of Theorem 1. For any vertex x of a cyclic f-orbit there is a smallest nonnegative integer m such that $f^m(x)$ is in the cycle of the orbit; this integer is the *f-height of x*, written $\mathrm{ht}(f;x)$. An n-cyclic f-orbit contains exactly n vertices of f-height 0 (the vertices in the n-cycle) but for an arbitrary function f the only restriction on the number of vertices of any given positive f-height is the obvious one: if there is a vertex of f-height $m\geqslant 2$, then for each positive integer $k\leqslant m$ there must be at least one vertex of f-height k.

The next lemma makes precise the fact that since f^r strides toward the cycle in r-league boots it takes roughly $1/r$ as many steps as f to get there.

LEMMA 8. *Let x be a vertex in a cyclic f-orbit and r an integer $\geqslant 2$. Then*

$$\mathrm{ht}(f^r;x)=\lceil(\mathrm{ht}(f;x)/r)\rceil \tag{5.1}$$

where, for any real number a, $\lceil a\rceil$ denotes the least integer $\geqslant a$.

Proof. If $\mathrm{ht}(f;x)=0$, then (5.1) is trivial. Otherwise, let $\mathrm{ht}(f;x)=p\geqslant 1$. Then $p/r\leqslant\lceil p/r\rceil<(p/r)+1$, whence $r\lceil p/r\rceil\geqslant p$. Thus $f^{r\lceil p/r\rceil}(x)$ is in the cycle of the f-orbit containing x, and so in the cycle of the f^r-orbit containing x. Consequently $\mathrm{ht}(f^r;x)\leqslant\lceil p/r\rceil$. In the other direction, if q is a nonnegative integer less than $\lceil p/r\rceil$, then

$$rq\leqslant r\lceil p/r\rceil-r<p.$$

Since p is the *least* integer such that $f^p(x)$ is in the cycle of the f-orbit containing x, it follows that $f^{rq}(x)$ is *not* in this cycle and hence not in the cycle of the f^r-orbit containing x.

LEMMA 9. *Let $r\geqslant 2$ and let x be a vertex of a 1-cyclic f^r-orbit. Then x is in a d-cyclic f-orbit where d is a divisor of r; and if $y\sim_f x$, then y is in a 1-cyclic f^r-orbit.*

Proof. Let z be the vertex in the 1-cycle of the f^r-orbit containing x. Then $f^r(z)=z$. Now let d be the least positive integer such that $f^d(z)=z$. Then $d\leqslant r$, and there are integers p,q with $p\geqslant 1$ and $0\leqslant q\leqslant d-1$ such that $r=pd+q$. Consequently,

$$z=f^r(z)=f^{q+pd}(z)=f^q(f^{pd}(z))=f^q(z),$$

whence $q=0$ and d divides r. Next, if $y\sim_f x$, then there is a positive integer m such that $f^{mr}(y)=w$ is in the d-cycle of the f-orbit containing x and y. Thus $y\sim_{f^r} w$. Finally, w is a fixed point of f^r since $f^r(w)=f^{pd}(w)=w$.

LEMMA 10. *If for some integer $r\geqslant 2$, there is a 1-cyclic f^r-orbit containing a vertex x of f^r-height 2, then the number of vertices of f^r-height 1 in all the 1-cyclic f^r-orbits is at least r.*

Proof. From (5.1) we obtain $r<\mathrm{ht}(f;x)\leqslant 2r$, whence $\mathrm{ht}(f;x)\geqslant r+1$. Thus with $q=\mathrm{ht}(f;x)-r-1$ the r vertices $f^{q+1}(x),f^{q+2}(x),\ldots,f^{q+r}(x)$ are all distinct, have respective f-heights $r,r-1,\ldots,1$, and consequently all have f^r-height 1. These vertices need not be in the same f^r-orbit; but by Lemma 9, the f^r-orbits containing them are all 1-cyclic.

A restatement of Lemma 10 yields:

LEMMA 11. *Let g be a function and r an integer $\geqslant 2$. Suppose g has a 1-cyclic orbit containing a vertex of g-height 2. Then a necessary condition for g to have an iterative rth root is that the number of vertices of g-height 1 in all the 1-cyclic g-orbits be at least r.*

We now apply these results to polynomials, beginning with:

THEOREM 4. *Let P be a polynomial of degree $d\geqslant 2$ defined on the complex plane C, and let r be an integer $\geqslant 2$. If P has an iterative rth root, then $r\leqslant d(d-1)$.*

Proof. We shall show that: (a) P has at least 1 and not more than d 1-cyclic orbits; (b) at least one of the 1-cyclic P-orbits contains a vertex of P-height 2; (c) the total number of vertices of P-height 1 in all the 1-cyclic P-orbits is $\leqslant d(d-1)$. The conclusion of the theorem then follows immediately from Lemma 11.

To prove (a), we need only observe that the number of 1-cyclic P-orbits is the same as the number of distinct solutions of the equation

$$P(z)=z. \tag{5.2}$$

By the Fundamental Theorem of Algebra, (5.2) has at least 1, and not more than d, distinct solutions. (Both extremes are attained: any polynomial linearly conjugate to z^d+z has precisely one 1-cyclic orbit, while any polynomial linearly conjugate to z^d has d 1-cyclic orbits.)

Turning to (b), we first note that if a 1-cyclic P-orbit contains a vertex z_0 of P-height 1, then it contains a vertex of P-height 2. For the equation $P(z)=z_0$ has at least one solution (Fundamental Theorem of Algebra again!) which cannot be equal to z_0, since z_0 is not a fixed point of P. Hence any such solution has P-height 2. Thus it remains to show that there is at least one 1-cyclic P-orbit which contains a vertex of P-height 1. Suppose the contrary, i.e., that there are no such vertices.

Let z_1 be a fixed point of P. Then z_1 is the only solution of the equation $P(z)=z_1$. And this is the case if and only if

$$P(z)=a(z-z_1)^d+z_1, \tag{5.3}$$

for some $a\neq 0$. But then

$$P(z)-z=(z-z_1)Q(z), \tag{5.4}$$

where

$$Q(z)=a(z-z_1)^{d-1}-1. \tag{5.5}$$

Since $d \geqslant 2$, the degree of Q is greater than 0. Let z_2 be a solution of the equation $Q(z)=0$. By (5.4), $P(z_2)=z_2$, whence z_2 belongs to a 1-cycle of P; and by (5.5), z_2 is distinct from z_1. Thus using the same argument as for z_1,

$$P(z)=a'(z-z_2)^d+z_2, \tag{5.6}$$

for some $a' \neq 0$. Equating coefficients of z^d in (5.3) and (5.6) yields $a=a'$; and then equating coefficients of z^{d-1} yields $z_1=z_2$, which is a contradiction. This proves (b).

As for (c), let z_0 be a fixed point of P. Then the 1-cyclic orbit containing z_0 cannot contain more than $d-1$ vertices of P-height 1, since every such vertex, *as well as* z_0 *itself*, is a solution of the equation $P(z)=z_0$, and this equation cannot have more than d solutions. Since (as we have already seen) there are no more than d 1-cyclic P-orbits, the total number of vertices of P-height 1 in all the 1-cyclic P-orbits cannot exceed $d(d-1)$, which proves (c) and completes the proof of the theorem.

When $d=2$, the upper bound in Theorem 4 is 2. Thus an immediate consequence is:

THEOREM 5. *If P is a quadratic polynomial defined on the complex plane C, then P has no iterative roots of order $\geqslant 3$.*

Combining Theorems 3 and 5 yields Theorem 1.

6. Epilogue. As pointed out in the introduction, the validity of results like Theorem 1 is a domain-dependent phenomenon. In the proof of Theorem 1 this domain dependence enters through unrestricted appeals to the Fundamental Theorem of Algebra (which implies, incidentally, that Theorem 1 holds in any algebraically closed field of characteristic 0). This domain dependence is further brought out by the following results, which show that the iterative root situation for real quadratic polynomials contrasts sharply with that for complex quadratic polynomials.

First a definition: Let E be a nonempty set. A *1-sided flow on E* is a family $\{f_t \mid t \geqslant 0\}$ of functions each mapping E into E such that

$$f_s(f_t(x))=f_{s+t}(x) \quad \text{for all } x \text{ in } E \text{ and all real } s,t \geqslant 0. \tag{6.1}$$

A *2-sided flow on E* is a similar family of functions in which the index t ranges over all real numbers.

Clearly, any function which is embeddable in a flow of either type has iterative roots of all orders.

THEOREM 6. *Let R be the real line. Let g be a real quadratic polynomial, so that*

$$g(x)=ax^2+(b+1)x+c,$$

for all real x, where $a \neq 0$, b,c are in R. As in the complex case, set $\Delta(g)=b^2-4ac$. If $\Delta(g)>1$, then g has no iterative roots of any order whatever. If $\Delta(g)=1$, then g can be embedded in a 2-sided flow on R, all of whose members are continuous functions. If $\Delta(g)<1$, then g can be embedded in a 1-sided flow on R, all of whose members are continuous functions; but g cannot be embedded in any 2-sided flow on R.

Lemmas 1 and 9 can be extended to:

LEMMA 12. *Let f be a function and r be an integer $\geqslant 2$. Then any acyclic f-orbit is, as a set, the union of r acyclic f^r-orbits. Correspondingly, any m-cyclic f-orbit is the union of d (m/d)-cyclic f^r-orbits, where d is the greatest common divisor of m and r.*

The notion of an iterative discriminant can be extended from quadratic polynomials to all polynomials defined on the complex plane as follows:

For any polynomial P of degree $d \geqslant 2$, let $z_1, \ldots, z_d$ be the d fixed points of P, i.e., the d (not necessarily distinct) roots of the equation $P(z) = z$. Set

$$\Delta(P) = a^d \prod_{m<n} (z_m - z_n)^2, \tag{6.2}$$

where $a \neq 0$ is the leading coefficient of P. A routine calculation shows that (6.2) reduces to (3.5) when $d = 2$. We then have the following analog of Lemma 4:

LEMMA 13. *Let P and Q be polynomials on C, each of degree $\geqslant 2$. If P and Q are linearly conjugate, then P and Q have the same degree and $\Delta(P) = \Delta(Q)$.*

Theorem 4 was announced in **[8]** and proved in **[9]**. In some cases the upper bound $d(d-1)$ for the order of an iterative root of a dth degree polynomial in Theorem 4 can be considerably lowered. For example, G. Zimmermann has shown (cf. **[16**, § 3]) that $d[d/2]$ is an upper bound for polynomials linearly conjugate to the Čebyšev polynomial of degree d, where $[d/2]$ is the greatest integer $\leqslant d/2$. Also, Theorems 1 and 3 extend to certain nonquadratic Čebyšev polynomials: see **[10]** and **[16**, § 3].

References

1. N. H. Abel, Détermination d'une fonction au moyen d'une équation qui ne contient qu'une seule variable. Manuscript 1824; Oeuvres Complètes, t. II, Christiana, 1881, pp. 36–39.
2. C. Babbage, An essay towards the Calculus of Functions, Part I, Philos. Trans. Royal Society, 105 (1815) 389–423.
3. I. N. Baker, Fixpoints of polynomials and rational functions, J. London Math. Soc., 39 (1964) 615–622.
4. R. A. Dean, Elements of Abstract Algebra, Wiley, New York, 1966.
5. J. M. Dubbey, The Mathematical Work of Charles Babbage, Cambridge University Press, 1978.
6. R. Isaacs, Iterates of fractional order, Canad. J. Math., 2 (1950) 409–416.
7. M. Kuczma, Functional Equations in a Single Variable, Monografie Matematyczne, Tom 46, Warszawa, 1968.
8. R. E. Rice, An upper bound for the order of an iterative root of a function, Notices Amer. Math. Soc., 23 (Oct. 1976) A-609, Abstract 738-B10.
9. ______, Fractional Iterates, Ph.D. Dissertation, University of Massachusetts, Amherst, Mass., 1977.
10. ______, Iterative square roots of Čebyšev polynomials, Stochastica, 3, no. 2 (1979) 1–14.
11. G. Riggert, *n*-te iterative Wurzeln von beliebigen Abbildungen (abstract), Aequationes Math., 14 (1976) 208.
12. R. Tambs Lyche, Sur l'équation fonctionnelle d'Abel, Fund. Math., 5 (1924) 331–333.
13. S. M. Ulam, A Collection of Mathematical Problems, Interscience, New York, 1960.
14. G. T. Whyburn, Orbit decompositions, Bull. Amer. Math. Soc. 47 (1941) 401, Abstract 291.
15. ______, Analytic Topology, Amer. Math. Soc. Colloquium Publications, vol. 28, Providence, 1942.
16. G. Zimmermann, Über die Existenz iterativer Wurzeln von Abbildungen, Inaugural-Dissertation, Phillipps-Universität Marburg/Lahn, 1978.

DEPARTMENT OF MATHEMATICS, UNION COLLEGE, SCHENECTADY, NY 12308. Present address: 5229 19TH ST., N.E., SEATTLE, WA 98105.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MASSACHUSETTS, AMHERST, MA 01003.

DEPARTMENT OF MATHEMATICS, ILLINOIS INSTITUTE OF TECHNOLOGY, CHICAGO, IL 60616.

MISCELLANEA

33. In the beginning, let me as distinctly as possible announce—not the theorem which I hope to demonstrate—for, whatever the mathematicians may assert, there is, in this world at least, *no such thing* as demonstration—but the ruling idea . . . which I shall be continually endeavoring to suggest.

—Edgar Allan Poe, *Eureka*, p. 1 (vol. 16, p. 185 of the Harrison edition of Poe's Works, New York, 1902).