

3-2002

Associativity of the Secant Method

Sam Northshield
SUNY Plattsburgh

Follow this and additional works at: http://digitalcommons.plattsburgh.edu/mathematics_facpubs

Recommended Citation

Northshield, S. (2002). Associativity of the Secant Method. *American Mathematical Monthly*, 109, 245-257.

This Article is brought to you for free and open access by the Mathematics at Digital Commons @ SUNY Plattsburgh. It has been accepted for inclusion in Mathematics Faculty Publications by an authorized administrator of Digital Commons @ SUNY Plattsburgh.

Associativity of the Secant Method

Sam Northshield

1. INTRODUCTION. This paper has its genesis in a problem the author first came upon while in college. Although the areas covered here are well travelled and nothing here is guaranteed original, it covers a pleasant nexus of many mathematical strands. Furthermore, we show the value of good notation and of reading an old master for solving a problem.

Consider iterates of the function $m(x) = 1 + 1/x$. Starting at 1, we get the sequence

$$1, 1 + \frac{1}{1}, 1 + \frac{1}{1 + \frac{1}{1}}, 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}}, \dots$$

As simple fractions, we have

$$\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \dots \tag{1}$$

which are the ratios of consecutive Fibonacci numbers. An induction argument shows

Proposition. *Let $F_1 = F_2 = 1$ and, for $n \geq 1$, $F_{n+1} = F_n + F_{n-1}$. Let $x_1 = 1$ and, for $n \geq 1$, $x_{n+1} = 1 + 1/x_n$. Then*

$$x_n = \frac{F_{n+1}}{F_n}.$$

The sequence x_n converges but we save a proof of this fact for later. Assuming convergence, we can identify the limit, say \hat{x} , as follows: since x_n is positive and satisfies $x_{n+1} = 1 + 1/x_n$, \hat{x} must be positive and satisfy $x = 1 + 1/x$, or, equivalently, \hat{x} is the unique positive solution of $x^2 - x - 1 = 0$. Hence $\hat{x} = \phi \equiv (1 + \sqrt{5})/2$, the Golden Mean. The sequence x_n in decimal form is illustrated by Table 1,

TABLE 1.

n	x_n	n	x_n
1	1	13	1.618025751
2	2	14	1.618037135
3	1.5	15	1.618032787
4	1.666666667	16	1.618034448
5	1.6	17	1.618033813
6	1.625	18	1.618034056
7	1.615384615	19	1.618033963
8	1.619047619	20	1.618033999
9	1.617647059	21	1.618033985
10	1.618181818	22	1.61803399
11	1.617977528	23	1.618033988
12	1.618055556	24	1.618033988

so it takes 23 iterations for the first 10 digits to stabilize.

Although it is known that continued fraction convergents provide the ‘best’ rational approximations to the Golden Mean, there are faster methods to approximate ϕ . A faster method, often seen in the calculus, is the Newton-Raphson method; see Figure 1. Given a starting “guess” T_0 , compute T_1, T_2, \dots using the formula

$$T_{n+1} = T_n - \frac{f(T_n)}{f'(T_n)} = \frac{T_n^2 + 1}{2T_n - 1}.$$

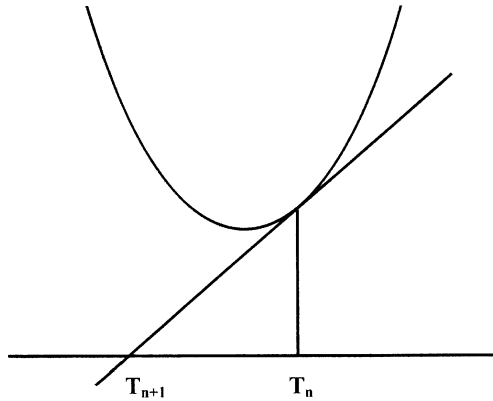


Figure 1.

Starting at $T_0 = 1$, we get the sequence in Table 2,

TABLE 2.

n	T_n
0	1
1	2
2	1.666666667
3	1.619047619
4	1.618034448
5	1.618033989
...	...

so it takes only 5 iterations for the first 10 digits to stabilize.

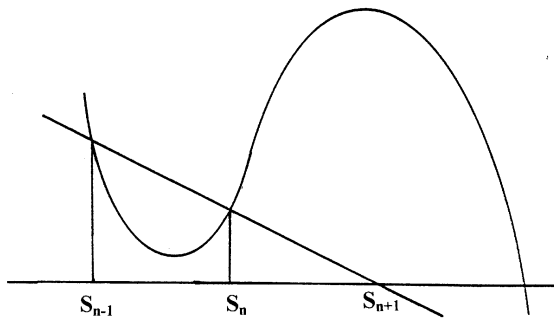


Figure 2.

The Secant Method (Figure 2) is similar to Newton’s method. Starting with two distinct “guesses” S_1, S_2 , and again for $f(t) = t^2 - t - 1$, compute

$$S_{n+1} = \frac{S_{n-1}f(S_n) - S_n f(S_{n-1})}{f(S_n) - f(S_{n-1})} = \frac{S_n S_{n-1} + 1}{S_n + S_{n-1} - 1}.$$

For $S_1 = 1$ and $S_2 = 2$, the sequence S_n is that shown by Table 3,

TABLE 3.

n	S_n
1	1
2	2
3	1.5
4	1.6
5	1.619047619
6	1.618025751
7	1.618033985
8	1.618033989
...	...

so it takes 6 iterations for the first 10 digits to stabilize.

The phenomenon of interest to us is that the numbers T_n and S_n are all continued fraction convergents to ϕ —that is, all are on the list of iterates of $1 + 1/x$ in (1). In Table 4, we compare the iterates of $1 + 1/x$ in Table 1 with the Newton-Raphson approximants in Table 2 and the Secant Method approximants in Table 3.

TABLE 4.

x_n	T_n	S_n
1	1	1
2	2	2
1.5		1.5
1.666666667	1.666666667	
1.6		1.6
1.625		
1.615384615		
1.619047619	1.619047619	1.619047619
1.617647059		
1.618181818		
1.617977528		
1.618055556		
1.618025751		1.618025751
1.618037135		
1.618032787		
1.618034448	1.618034448	

The apparent pattern is real:

Theorem 1. *Let x_n be the n th iterate of $m(x) = 1 + 1/x$ starting at 1, let $f(x) = x^2 - x - 1$, let T_n be the sequence from the Newton-Raphson method applied to f with $T_1 = 1$, and let S_n be the sequence from the Secant Method applied to f with $S_1 = 1$ and $S_2 = 2$. Then $T_n = x_{2^n}$ and $S_n = x_{F_n}$.*

This was first proved by Gill and Miller in 1981 [5]. An analysis of the Newton-Raphson method for a wider class of quadratic irrationalities was done by M. Filaseta [4]. Our goal is to explain this phenomenon in a new way and to investigate the most general situation in which it occurs.

2. OUR APPROACH TO THE PROBLEM. Our solution of this problem is largely a result of good notation. Consider the following binary operation:

$$x \oplus y = \frac{xy + 1}{x + y - 1}. \quad (2)$$

This operation is well defined on the extended real numbers $\overline{\mathbb{R}}$ (i.e., the reals with ∞ appended) and is in fact commutative on $\overline{\mathbb{R}}$ except in the $0/0$ case; i.e., when $xy = -1$ and $x + y = 1$ or, equivalently, when x and y are the distinct zeros of $x^2 - x - 1$. One can see this geometrically as well; $x \oplus y$ is the result of applying the secant method to the function $x^2 - x - 1$ with initial guesses x and y . The $0/0$ case occurs when the secant line coincides with the x -axis or, equivalently, when the distinct numbers x and y are both zeros of the function $x^2 - x - 1$.

The “number” ∞ plays a special role here. Geometrically, $x \oplus \infty$ is the limit of $x \oplus z$ as z approaches ∞ , which is where the *vertical* line through x intersects the x -axis—just x itself. That is, ∞ acts as an identity for \oplus and any line through the point at infinity is vertical.

Assuming for the moment that \oplus is associative, one may define $1^{\oplus n}$ to be the n -fold “sum” of 1. Since $x \oplus 1 = 1 + 1/x$, the n th iterate of $1 + 1/x$ is the n -fold sum of 1. That is,

$$x_n = 1^{\oplus n}.$$

Since $x \oplus x = (x^2 + 1)/(2x - 1)$, which is just the Newton-Raphson method applied to $x^2 - x - 1$ with initial guess x , then the Newton-Raphson method starting at 1 gives:

$$1, 1 \oplus 1, (1 \oplus 1) \oplus (1 \oplus 1), ((1 \oplus 1) \oplus (1 \oplus 1)) \oplus ((1 \oplus 1) \oplus (1 \oplus 1)), \dots,$$

which by associativity and induction yields

$$T_n = 1^{\oplus 2^n} = x_{2^n}.$$

Similarly, the secant method applied to $x^2 - x - 1$ starting at 1 and $2 = 1 \oplus 1$ satisfies $S_{n+1} = S_n \oplus S_{n-1}$ and gives:

$$1, 1 \oplus 1, (1 \oplus 1) \oplus 1, ((1 \oplus 1) \oplus 1) \oplus (1 \oplus 1), \dots,$$

which by associativity and induction yields

$$S_n = 1^{\oplus F_n} = x_{F_n}.$$

It remains to show only that \oplus is associative. If one works out the algebra, one finds

$$(x \oplus y) \oplus z = \frac{xyz + x + y + z - 1}{xy + xz + yz - x - y - z + 1}.$$

Switching x and z , the right side remains unchanged but the left side becomes $(z \oplus y) \oplus x$, which is, by commutativity, $x \oplus (y \oplus z)$.

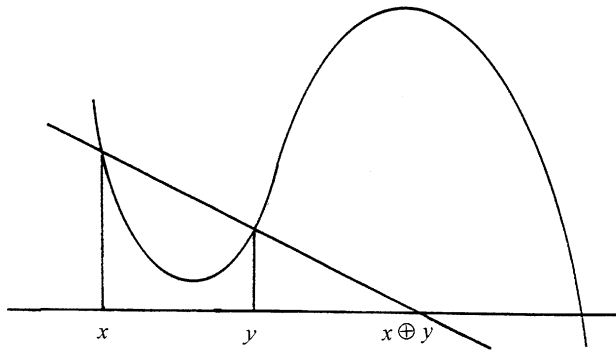


Figure 3.

3. TRYING TO GENERALIZE. At this point we wish to generalize. There is nothing special about the function $x^2 - x - 1$ or the number 1 in the argument in Section 2. That is, if we replace $x^2 - x - 1$ by any differentiable function f from \overline{R} to \overline{R} , define addition by the secant method (see Figure 3)

$$x \oplus y = \frac{xf(y) - yf(x)}{f(y) - f(x)}, \quad (3)$$

and replace $1 + 1/x$ by any function of the form $m(x) = x \oplus k$, then Theorem 1 is valid if \oplus is associative.

We assume that f is differentiable since the proof of Theorem 1 hinges on $k^{\oplus n}$ being well defined, which requires $x \oplus x$ to be well defined. When f is differentiable, then taking $x \oplus x = \lim_{y \rightarrow x} x \oplus y$, we find

$$x \oplus x = x - \frac{f(x)}{f'(x)},$$

which is the Newton-Raphson method applied to the function f with guess x . Actually, it is sufficient to assume only that f is continuous, since differentiability then follows from the associativity of \oplus !

The question we now ask is: "For which functions f is the relation \oplus associative?" Trial and error does not shed much light. Algebraic proofs of associativity are essentially *ad hoc* and it is difficult to see a definite strategy for proving or disproving associativity of \oplus for large classes of f . For example, if $f(x) = x^3$, then

$$x \oplus y = \frac{xy^2 + x^2y}{x^2 + xy + y^2},$$

which turns out not to be associative ($1 \oplus (1 \oplus -1) = 0$ but $(1 \oplus 1) \oplus -1 = 2/7$).

However, since the secant method is geometric, perhaps we can find a geometric proof of associativity and perhaps it would shed some light on the problem.

4. A GEOMETRIC VIEW. Our investigation is based on Pascal's "Mysterium Hexagrammicum" Theorem of 1640 (when Pascal was 16 years old): for any conic and any six points P_1, P_2, \dots, P_6 on it, the opposite sides of the resulting hexagram, extended if necessary, intersect at points lying on some straight line. More specifically, let $L(P, Q)$ denote the line through the points P and Q . Then the points $L(P_1, P_2) \cap L(P_4, P_5)$, $L(P_2, P_3) \cap L(P_5, P_6)$, and $L(P_3, P_4) \cap L(P_6, P_1)$ lie on a straight line (Figure 4).

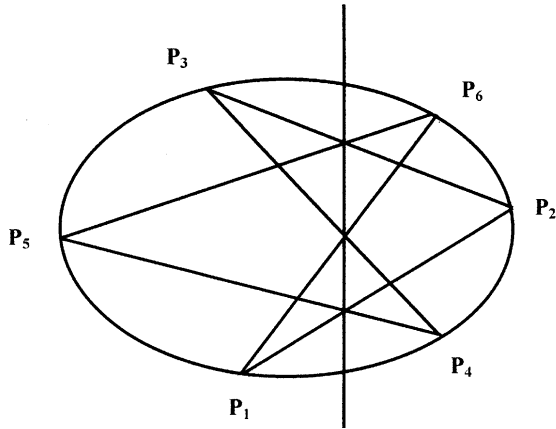


Figure 4.

We now show the associativity of the ‘addition’ (2) arising from $f(x) = x^2 - x - 1$ (see Figure 5). The slope of f is unbounded (at ∞) and it is through the ‘point at infinity’ that all secant lines are vertical (recall that ∞ acts as identity for \oplus).

For any real number x , let \bar{x} denote the point $(x, f(x))$. Given u , the points $\bar{u}, \bar{y} \oplus \bar{z}, \bar{x}, \bar{y}, \bar{z}$, and $\bar{x} \oplus \bar{y}$ are points on a conic and so, applying Pascal’s theorem, the points $L(\bar{x}, \bar{y}) \cap L(\bar{u}, \bar{x} \oplus \bar{y})$, $L(\bar{y}, \bar{z}) \cap L(\bar{u}, \bar{y} \oplus \bar{z})$, and $L(\bar{x} \oplus \bar{y}, \bar{z}) \cap L(\bar{x}, \bar{y} \oplus \bar{z})$ lie on some straight line. Letting u approach ∞ , the lines $L(\bar{u}, \bar{x} \oplus \bar{y})$ and $L(\bar{u}, \bar{y} \oplus \bar{z})$ become vertical and the first two points approach $(x \oplus y, 0)$ and $(y \oplus z, 0)$, respectively. Since these first two points lie on the x -axis, so does the third and thus $(x \oplus y) \oplus z = x \oplus (y \oplus z)$.

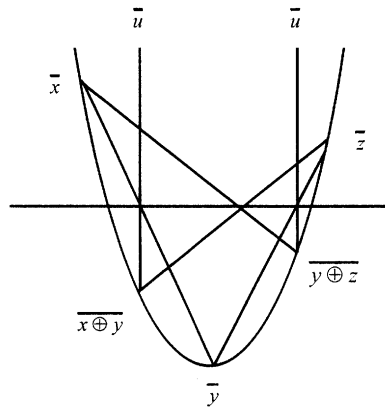


Figure 5.

Our argument is valid for any function f whose graph is a conic section with unbounded slope. The requirement that the slope be unbounded allows a “virtual” point at ∞ such that secant lines through it are all vertical. In particular, f must be of the form

$$f(x) = \frac{ax^2 + bx + c}{dx + e}$$

for some a, b, c, d, e with not both a and d being 0. We may thus conclude:

Theorem 2. If $f(x) = (ax^2 + bx + c)/(dx + e)$ and not both a and d are zero, then \oplus defined by (3) is associative. Given any k , let $m(x) = x \oplus k$, define x_n by $x_1 = k$ and $x_{n+1} = x_n \oplus k$, let T_n be the sequence from the Newton-Raphson method applied to f starting at k , and let S_n be the sequence from the secant method applied to f starting at k and $m(k)$. Then $T_n = k^{\oplus 2^n} = x_{2^n}$ and $S_n = k^{\oplus F_n} = x_{F_n}$.

In our original example, we looked at iterates of $m(x) = 1 + 1/x$, starting at 1, and saw that they were of the form $1^{\oplus n}$. Now, let m be a general Möbius transformation:

$$m(x) = \frac{ax + b}{cx + d}.$$

This is a generalization of the original example, where $m(x) = (1x + 1)/(1x + 0)$. We show that the iterates, starting at k , of the general m are of the form $k^{\oplus n}$ for an appropriately defined \oplus . Given k , if the iterates $m_n(k)$ converge at all, they converge to a fixed point of m —that is, to a root of the characteristic polynomial $p(x) = cx^2 + (d - a)x - b$. Given a number e , possibly infinite, consider the function $f(x) = p(x)e/(x - e)$. The operation \oplus turns out to be associative and commutative and the functions $x \oplus k$ are Möbius transformations (we prove this in Section 7). Since the Möbius transformations $m(x)$ and $x \oplus m(e)$ have, up to constant multiple, the same characteristic polynomials [$m(e) \oplus x = x$ iff $f(x) = 0$ iff $p(x) = 0$] and agree at some value other than a fixed point [$m(e) = e \oplus m(e)$],

$$m(x) = x \oplus m(e).$$

Letting $e = m^{-1}(k)$, we find that if $f(x) = p(x)/(x - m^{-1}(k))$, then $m(x) = x \oplus k$ and we have

$$m_n(k) = k^{\oplus(n+1)}.$$

As an example, let $m(x) = (2x + 3)/(4x + 5)$ and $k = 7$. Then $m^{-1}(7) = -16/13$, and, defining $f(x) = (52x^2 + 39x - 39)/(13x + 16)$, we find that

$$x \oplus y = (25xy + 39(x + y) + 48)/(52xy + 64(x + y) + 87)$$

from which it follows that

$$x \oplus 7 = (2x + 3)/(4x + 5)$$

and

$$m_n(7) = 7^{\oplus(n+1)}.$$

5. GROUPS. For the functions of the form $(ax^2 + bx + c)/(dx + e)$, is there a group with group operation \oplus ? Yes! Geometrically, $\iota = -e/d$ ($\iota = \infty$ if $d = 0$) acts as the identity. Let $Z(f) = \{x : f(x) = 0\}$ denote the zero set of f and let $G = \overline{R} - Z(f)$. Then G is closed under \oplus . The existence of an inverse for any k is ensured by the fact that every $x \oplus k$ is a Möbius transformation: given k , let $m(x) = x \oplus k$ and define $k^{-1} = m^{-1}(\iota)$.

The base field R is arbitrary and, since Möbius transformations are most commonly thought of as defined over the complex numbers C , we may consider the group G to

be the set $G = \{z \in \overline{\mathbb{C}} : f(z) \neq 0\}$ with group operation \oplus and identity ι . Then G is a Lie group that is homeomorphic to the Riemann sphere with one or two punctures.

6. SOME EXAMPLES.

A. Consider $f(x) = (x^2 + 1)/x$. The corresponding “addition” is $x \oplus y = (x + y)/(1 - xy)$. The reader may recognize this addition and its relationship to π : The arctangent acts as a homomorphism

$$\tan^{-1}(x \oplus y) = \tan^{-1}(x) + \tan^{-1}(y)$$

and, for example, Machin’s formula

$$1 \oplus \frac{1}{239} = \frac{1}{5} \oplus \frac{1}{5} \oplus \frac{1}{5} \oplus \frac{1}{5}$$

holds, from which it follows, using the Maclaurin series for the arctangent, that

$$\pi = 4 \sum_{n=0}^{\infty} \frac{(-1)^n (4 \times 239^{2n+1} - 5^{2n+1})}{(2n + 1) 1195^{2n+1}}.$$

Furthermore, one can obtain a closed formula for iterates of Möbius transformations corresponding to f :

$$x \oplus c = \tan(\tan^{-1}(x) + \tan^{-1}(c))$$

and thus

$$m_n(c) = \tan(n \times \tan^{-1}(c)).$$

B. Consider $f(x) = (x^2 - c^2)/x$. Then $x \oplus y = (x + y)/(1 + xy/c^2)$, which is the velocity addition law of special relativity with light velocity c . If $c^2 = k$ is a non-square integer, does adding one to itself n times, $1 \leq n < \infty$, produce infinitely many convergents to the simple continued fraction of c ? The definitive answer was found by Douglas Hensley [6].

C. If $f(x) = 1/x$, then $x \oplus y = x + y$ —normal addition. Does normal multiplication correspond to some f ? That is, does there exist an f such that $x \oplus y = xy$? If so, let $y = x$ and get $x \oplus x = x^2$. On the other hand, $x \oplus x$ is an iteration of the Newton-Raphson method and we have the differential equation

$$x^2 = x - f(x)/f'(x).$$

Solving, we find $f(x) = x/(1 - x)$. Finally, checking that \oplus given by f is indeed ordinary multiplication, we conclude that the answer is Yes!

D. If $f(x) = x^2$, we get $x \oplus y = 1/(1/x + 1/y)$; the electrically minded may recognize this as the addition of resistances arranged in parallel. The other extreme—resistors arranged in series—is covered by the case $f(x) = 1/x$. One wonders if *all* these different addition rules have some electrical interpretation.

E. If f is a Möbius transformation, then $x \oplus y$ is of the form $Axy + B(x + y) + C$.

In Example A, we saw that the arctangent acts as a homomorphism and that this leads to a closed formula for the iterates of m . This is true for all of the examples A–E, and more (Table 5):

TABLE 5.

$f(x)$	$x \oplus y$	$F(x)$
$\frac{x^2 + 1}{x}$	$\frac{x + y}{1 - xy}$	$\tan^{-1}(x)$
$\frac{x^2 - 1}{x}$	$\frac{x + y}{1 + xy}$	$\tanh^{-1}(x)$
$x^2 + 1$	$\frac{xy - 1}{x + y}$	$\cot^{-1}(x)$
$x^2 - x - 1$	$\frac{xy + 1}{x + y - 1}$	
$\frac{1}{x}$	$x + y$	x
x^2	$\frac{1}{1/x + 1/y}$	$\frac{1}{x}$
$\frac{x}{1 - x}$	xy	$\ln(x)$
$\frac{ax + b}{cx + d}$	$Axy + B(x + y) + C$	

The reader might enjoy pausing to try to find how to derive F from f before we do so in the next section. Rather mild hypotheses on an associative addition are known to imply the existence of a continuous such homomorphism. For a definitive treatment with extensive references to the literature, see [1, pp. 253–273].

7. A USEFUL LEMMA AND ITS CONSEQUENCES. A consequence of the associativity of \oplus follows. We otherwise make no assumptions about f except continuity and that the graph of f has unbounded slope. If e is a real number such that $f(e) = \infty$, then define $p(x) = f(x)(x - e)$ but otherwise define $p(x) = f(x)$. If f is a conic with unbounded slope, then p is just the numerator of f .

Lemma 1. *If f is such that \oplus is associative, then*

$$\frac{\partial}{\partial x}(x \oplus y) = \frac{p(x \oplus y)}{p(x)}.$$

Proof. Let $s(x, y) = f(x)/(x - x \oplus y) = (f(x) - f(y))/(x - y)$. Let ι be e if $f(e) = \infty$ (if $f(e) = \infty$ for several values of e , any one will do), otherwise let $\iota = \infty$. In either case, $\lim_{z \rightarrow \iota} x \oplus z = x$. Then associativity ensures that $x \oplus y \oplus z$ is well defined and

$$\begin{aligned} \frac{\partial}{\partial x}(x \oplus y) &= \lim_{z \rightarrow \iota} \frac{x \oplus y - x \oplus y \oplus z}{x - x \oplus z} = \lim_{z \rightarrow \iota} \frac{f(x \oplus y)}{s(x \oplus y, z)} \frac{s(x, z)}{f(x)} \\ &= \frac{f(x \oplus y)}{f(x)} \lim_{z \rightarrow \iota} \frac{s(x, z)}{s(x \oplus y, z)}. \end{aligned}$$

Note that

$$\lim_{z \rightarrow \iota} \frac{s(x, z)}{s(x \oplus y, z)} = \lim_{z \rightarrow \iota} \frac{f(x) - f(z)}{x - z} \frac{x \oplus y - z}{f(x \oplus y) - f(z)} = \lim_{z \rightarrow \iota} \frac{x \oplus y - z}{x - z},$$

which equals 1 if $\iota = \infty$ and equals $\frac{x \oplus y - e}{x - e}$ if $\iota = e$. ■

It immediately follows, by the definition of f , that $f(x) = \infty$ has at most one real solution. Another consequence, used in Sections 4 and 5, is that a function of the form $x \oplus k$ is a Möbius transformation.

Corollary 1. *Let p be a quadratic polynomial. Then for all k , $m(x) = x \oplus k$ is a Möbius transformation.*

Proof. The basic fact we use here is that the Schwarzian derivative

$$S(m) = (m''/m')' - \frac{1}{2}(m''/m')^2$$

is zero if and only if m is a Möbius transformation. Let $m(x) = x \oplus k$. By Lemma 1,

$$m' = \frac{p \circ m}{p}.$$

Using this to work out its Schwarzian derivative, $S(m) = (q \circ m - q)/p^2$, where $q = pp'' - \frac{1}{2}(p')^2$. Since p is a quadratic polynomial, q is constant and so $S(m) = 0$. ■

In Section 6, a homomorphism was found for Example A. We now find such a homomorphism in the general case.

Corollary 2. *If F satisfies $F' = 1/p$ and $F(\iota) = 0$, then*

$$F(x \oplus y) = F(x) + F(y).$$

Proof. Suppose $F' = 1/p$. By Lemma 1,

$$\frac{\partial}{\partial x} F(x \oplus y) = F'(x)$$

and thus $F(x \oplus y) = F(x) + G(y)$ for some function G . By commutativity, $F(x) + G(y) = F(y) + G(x)$ from which it follows that $F(x) - G(x) = F(y) - G(y)$, and so F and G differ by a constant (say c). Hence,

$$F(x \oplus y) = F(x) + F(y) + c.$$

The condition $F(\iota) = 0$ ensures that this constant is zero. ■

This gives us, as in Example A, a closed formula for $k^{\oplus n}$, namely

$$k^{\oplus n} = F^{-1}(nF(k)).$$

The functions F and p are, for the given function m , solutions to well-known functional equations. Namely, up to scaling, F is a solution to *Abel's functional equation*

$$F(m(x)) = F(x) + 1,$$

and p is a solution to *Julia's equation*

$$p(m(x)) = p(x)m'(x).$$

Returning to our original example, the homomorphism is then

$$5^{-1/2} \log |(x - \bar{\phi})/(x - \phi)|,$$

where ϕ and $\bar{\phi}$ are the two solutions of $x^2 - x - 1 = 0$. Thus, if k is closer to ϕ than to $\bar{\phi}$, then $F(k) > 0$ and $F(k^{\oplus n}) \rightarrow \infty$ as $n \rightarrow \infty$; it follows that

$$k^{\oplus n} \rightarrow \phi.$$

Thus, for example, $F_{n+1}/F_n = 1^{\oplus n} \rightarrow \phi$. Other consequences of associativity appear in [7].

8. ELLIPTIC CURVES. The reader familiar with elliptic curves no doubt recognizes a similarity between our secant addition and the “group law” for elliptic curves. An elliptic curve is a type of cubic curve, i.e., zero set of a two-variable polynomial of degree three. The union of the x -axis and the graph of $y = (ax^2 + bx + c)/(dx + e)$ is also a cubic curve—albeit a degenerate one—defined by

$$y^2(dx + e) = y(ax^2 + bx + c).$$

This equation gives the most general cubic curve whose graph is the union of the x -axis and the graph of a function.

There is a way to “add” nonsingular points on a cubic curve—the group law—and this method applied to our degenerate curves is exactly our secant addition. The usual proof that the group law is associative follows from the Cayley-Bacharach theorem, a celebrated generalization of Pascal’s theorem; see [9] for details. A recent definitive treatment of the role of Pascal’s theorem in the history of algebra, geometry, and algebraic geometry and a discussion of where these developments are leading is in [2], where early parts are accessible to nonspecialists.

9. FINAL WORDS. The theory of polynomial approximation on $[-1, 1]$ inevitably involves the weight function $\sqrt{1 - x^2}$. In this context, the addition law

$$a \oplus b = a\sqrt{1 - b^2} + b\sqrt{1 - a^2}$$

has been found of importance. Although not obviously a “secant” addition law, it is, nevertheless, associative on the interval $[-1, 1]$ (the arcsine acts as a homomorphism!). In [3], M. Felten develops an entire calculus based on this exotic addition. In general, the theory of addition rules of the form $a \oplus b = af(b) + bf(a)$ closely parallels that of secant addition. For example, if \oplus is associative and $h(x) = f(x)/x$, then for some k ,

$$h(x \oplus y) = \frac{h(x)h(y) + k}{h(x) + h(y)}.$$

That is, even though $x \oplus c$ is not a Möbius transformation, it is conjugate to one; see [8] for details. This implies Lemma 1 and Corollary 2 (for appropriate choice of p).

Does this “secant addition” theory extend beyond the “iterates of Möbius transformations” case (that is, the case $f(x) = (ax^2 + bx + c)/(dx + e)$)? The answer, at least for functions f that are continuous from \overline{R} to itself, is no; see [8] for a proof. A heuristic proof (with many gaps) is as follows. Assuming associativity, Lemma 1 implies that f is meromorphic and so is a ratio of two power series. The group G defined in Section 5 is homeomorphic to a punctured Riemann sphere—the punctures correspond to the zeros of f . There can be at most two punctures since, otherwise, the fundamental group of the manifold G would be nonabelian. Hence the numerator of f is a polynomial of degree 2 or less. Each zero of the denominator of f corresponds to an ‘identity’ for G and since there is only one such identity, the denominator of f is linear.

Finally, we note an interesting connection with matrices. Recall our initial example $m(x) = 1 + 1/x$, $f(x) = x^2 - x - 1$, and $x \oplus y = (xy + 1)/(x + y - 1)$. Let A be a 2×2 matrix with characteristic equation $x^2 - x - 1 = 0$. For example, let

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

—note the correspondence with $1 + 1/x = (1x + 1)/(1x + 0)$! Since A satisfies its characteristic equation, $A^2 = A + I$ and we have

$$(A - xI)(A - yI) = (1 - x - y)A + (xy + 1)I \doteq A - (x \oplus y)I \quad (4)$$

where “ \doteq ” denotes equality up to scalar multiplication.

More generally, let A be a matrix with quadratic characteristic polynomial p . If $f(x) = p(x)$, then (4) remains valid while, if $f(x) = p(x)/(x - e)$,

$$(A - xI)(A - yI) \doteq (A - (x \oplus y)I)(A - eI)$$

where, in either case, \oplus is defined by (3).

REFERENCES

1. J. Aczel, *Lectures on Functional Equations and Their Applications*, Academic Press, New York, 1966.
2. D. Eisenbud, M. Green, and J. Harris, Cayley-Bacharach theorems and conjectures, *Bull. Amer. Math. Soc.* **33** (1996) 295–324.
3. M. Felten, A modulus of smoothness based on an algebraic addition, *Aequationes Math.* **54** (1997) 56–73.
4. M. Filaseta, Newton’s method and simple continued fractions, *Fibonacci Quart.* **24** (1986) 41–46.
5. J. Gill and G. Miller, Newton’s method and ratios of Fibonacci numbers, *Fibonacci Quart.* **19** (1981) 1–4.
6. D. Northshield, Simple continued fractions and special relativity, *Proc. Amer. Math. Soc.* **67** (1997) 219–220.
7. S. Northshield, On iterates of Möbius transformations on fields, *Math. Comp.* **70** (235) (2000) 1305–1310.
8. S. Northshield, *Notes on some associative binary relations*, preprint.
9. J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, New York, 1992.

SAM NORTHSHIELD, a product of the free-school movement in the U.S., was groomed to be an astrologer/farmer. After a brief career as an artist and unable to find a real job, he enrolled at Marlboro College where he fell in love with mathematics (thanks to Joe Mazur.) He went on to get a Ph.D. at the University of Rochester (thanks to Carl Mueller) in 1989. His first, and possibly last, real job (interrupted by visiting positions at the University of Minnesota, Gustavus Adolphus College, and Carleton College) is at Plattsburgh SUNY, where he is now Professor of Mathematics. He is very happy to have a job so closely related to his favorite hobby. His preferred research areas are probability, discrete mathematics, and number theory.

State University of New York, Plattsburgh, NY 12901
samuel.northshield@plattsburgh.edu