There Are Only Nine Finite Groups of Fractional Linear Transformations with Integer Coefficients

GREGORY P. DRESDEN
Washington & Lee University
Lexington, VA 24450
dresdeng@wlu.edu

An introduction to fractional linear transformations A *fractional linear transformation* (also called a *Möbius transformation*) over **C** is a function of the form

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

with $ad - bc \neq 0$. Most of us first encountered these in our complex analysis class, where we learned that such analytic functions map lines and circles to lines and circles on the complex plane (see, for example, books by Fisher [**3**, p. 187] or Rudin [**6**, p. 280]). In this note, we consider finite groups of fractional linear transformations (where the group operation is composition). We will arrive at the interesting conclusion that, provided we limit ourselves to integer coefficients, there are only nine such groups up to isomorphism. (For real or complex coefficients, there are infinitely many such groups, but we will get into that a little bit later.)

All of this material should be accessible to undergraduates; indeed, I've even had my beginning calculus students play with these functions when learning about compositions and inverses. Students in abstract algebra might appreciate these groups of functions as nice examples of cyclic and dihedral groups, and those interested in finding appropriate research topics will find plenty of material here to explore.

Let's examine our terms and definitions in a little more detail. By *integer coefficients*, of course, we mean that a, b, c, and d are all integers. Thus, we're considering functions of the form

$$m(x) = \frac{2x + 3}{4x + 5} \quad \text{or even} \quad p(x) = \frac{5}{6}x + 7,$$

since this can be written as

$$p(x) = \frac{5x + 42}{0x + 6},$$

but we are not considering functions like $q(x) = \frac{5}{6}$ (as here, $ad - bc = 0$). Let's also observe that the two fractional linear transformations

$$\frac{ax + b}{cx + d} \quad \text{and} \quad \frac{arx + br}{crx + dr} \quad (r \neq 0)$$

are identical. With this in mind, we see that there is no need to concern ourselves with fractional linear transformations with *rational* coefficients, as multiplying top and bottom by a common denominator would give us an identical function with integer coefficients (indeed, relatively-prime integer coefficients, if desired).

As mentioned above, our proposed group operation is function composition, so that, for

$$m(x) = \frac{2x+3}{4x+5}, \quad \text{say, and} \quad p(x) = \frac{6x+7}{8x+9},$$

we will have occasion to form $m \circ p(x) = m(p(x))$. It should be clear that these fractional linear transformations really do form a group under composition; the identity is $e(x) = x$ and the inverse of

$$\frac{ax+b}{cx+d} \quad \text{is} \quad \frac{dx-b}{-cx+a},$$

for which the condition $ad - bc \neq 0$ is required.

The composition of two fractional linear transformations is somewhat tedious to compute. A nice short-cut is provided by the map

$$\phi : \frac{ax+b}{cx+d} \longmapsto \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

It is surprising, but not to hard to check, that composition of functions corresponds exactly to matrix multiplication. In fact, ϕ is an isomorphism from the group of fractional linear transformations with integer coefficients to a group called $PGL(2, \mathbf{Q})$, the projective group of 2×2 matrices with rational entries. The word *projective* simply means that the matrices

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} ar & br \\ cr & dr \end{bmatrix}$$

are considered identical. (This condition is needed if the inverse of

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \text{is to be} \quad \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.)$$

Thus, as with the fractional linear transformations, we need only consider matrices with integer coefficients if we so desire.

The isomorphism ϕ makes it easy to compose functions; it's much simpler to multiply the matrix $\left[\begin{smallmatrix} 2 & 3 \\ 4 & 5 \end{smallmatrix}\right]$ by $\left[\begin{smallmatrix} 6 & 7 \\ 8 & 9 \end{smallmatrix}\right]$ than to attempt to simplify

$$\frac{2\left(\frac{6x+7}{8x+9}\right)+3}{4\left(\frac{6x+7}{8x+9}\right)+5}.$$

The isomorphism also gives us a shorthand for referring to our group of fractional linear transformations with integer coefficients (which we will henceforth denote as $PGL(2, \mathbf{Q})$.)

As is common in complex analysis, we will occasionally have these fractional linear transformations operate on numbers in the extended complex plane $\widehat{\mathbf{C}} = \mathbf{C} \bigcup \{\infty\}$ (also called the *Riemann sphere*). This is easy to do if we agree that $1/0 = \infty$, that $1/\infty = 0$, and that other standard rules of arithmetic with ∞ apply (see Beardon [**1**, p. 4] or Rudin [**6**, p. 279] for more). In particular, if

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

let us agree that $m(\infty) = a/c$ and $m(-d/c) = \infty$ (but note that if $c = 0$ then both these equations read as $m(\infty) = \infty$).

A few special groups Let us define two types of (multiplicative) groups that will prove to be quite important to us. The *cyclic group* C_n of size n can be thought of as the set $C_n = \{e, a, a^2, a^3, \cdots a^{n-1}\}$ such that $a^i \cdot a^j = a^{i+j \bmod n}$ and $a^n = a^0 = e$. The *dihedral group* D_n is a bit more complicated; we write $D_n = \{e, a, a^2, \cdots a^{n-1}, b, ab, a^2b, \cdots a^{n-1}b\}$. The as behave as before, but we now have $b^2 = e$ and $ba = a^{n-1}b$ (equivalently, $b = b^{-1}$ and $b^{-1}ab = a^{-1}$). See Gallian's book [**4**, p. 442] for further discussion. Note that D_1 is simply $\{e, b\}$ and thus is isomorphic to C_2. The group $D_2 = \{e, a, b, ab\}$ is the smallest noncyclic group, and is often referred to as the *Klein four-group*. (The terms D_1 and D_2 are not standard nomenclature for these small groups, but they do help to simplify our notation.)

C_n and D_n can also be thought of as *symmetry groups* for certain geometric objects; indeed, for $n \geq 3$, C_n and D_n are isomorphic to the group of symmetries in $\mathbf{R}^3$ of a regular pyramid and regular prism, respectively, with regular n-gons for bases. Since these pyramids and prisms can each be inscribed within a sphere, we see that C_n and D_n can be thought of as a symmetry group for a sphere as well. A classical result [**8**, p. 40] states that the only finite symmetry groups of the sphere are C_n, D_n, A_4, S_4, and A_5 (where A_n and S_n represent the alternating and the symmetric groups on n letters). See also Toth's book [**10**, chapter 17] for a discussion of A_4, S_4, and A_5 as symmetry groups for the five platonic solids.

The cyclic groups C_n and the dihedral groups D_n also have a natural interpretation as symmetries of regular n-gons in the plane. Here, C_n is the group of pure rotations of an n-gon about its center, and D_n is the group of such rotations, along with the reflections about axes of symmetries (*dihedral* groups refer to the "two sides" of the polygon). Although these interpretations are well known and of interest in their own right, we are mostly concerned here with regarding these groups as symmetries of appropriate polyhedra in three dimensions.

Groups of fractional linear transformations under composition Let us consider examples to see how certain sets of these fractional linear transformations can form groups under composition. First, for $p(x) = 1/(x+1)$, then we have $p(p(x))$ (also written $p \circ p(x)$ or $p^{(2)}(x)$) equals $(x+1)/(x+2)$, and $p^{(3)}$, $p^{(4)}$, and $p^{(5)}$ are

$$\frac{x+2}{2x+3}, \frac{2x+3}{3x+5}, \quad \text{and} \quad \frac{3x+5}{5x+8},$$

respectively. Are you surprised to see the Fibonacci numbers appearing as coefficients? Note that $p(x)$ corresponds to the matrix

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} f_0 & f_1 \\ f_1 & f_2 \end{bmatrix}$$

in $PGL(2, \mathbf{Q})$, where f_i is the ith Fibonacci number. It is well known that this matrix generates the Fibonacci sequence: Its nth power is

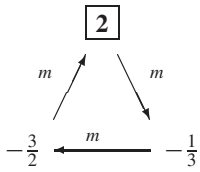
$$\begin{bmatrix} f_{n-1} & f_n \\ f_n & f_{n+1} \end{bmatrix}.$$

Let us define $p^{(0)}$ to be the the identity map $p^{(0)}(x) = x$, and note that the inverse of $p(x)$ is clearly $p^{(-1)}(x) = (-x+1)/x$. Thus, the set $\{p^{(i)}(x) : i \in \mathbf{Z}\}$ under composition forms an (infinite) group, isomorphic to $\mathbf{Z}$. A nice way to visualize the behavior of this group is to observe the orbit of a particular number (say, 1) under repeated iterations of p (and p^{-1}):

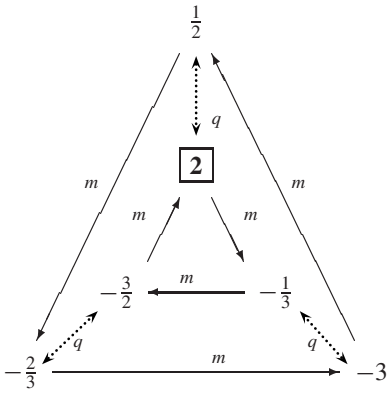
$$\cdots \underset{p^{-1}}{\leftarrow} -\tfrac{3}{2} \underset{p^{-1}}{\leftarrow} -2 \underset{p^{-1}}{\leftarrow} -1 \underset{p^{-1}}{\leftarrow} \infty \underset{p^{-1}}{\leftarrow} 0 \underset{p^{-1}}{\leftarrow} \boxed{1} \xrightarrow{p} \tfrac{1}{2} \xrightarrow{p} \tfrac{2}{3} \xrightarrow{p} \tfrac{3}{5} \xrightarrow{p} \tfrac{5}{8} \xrightarrow{p} \cdots$$

Again, we notice the appearance of the Fibonacci numbers, this time in the numerators and denominators of the terms in the orbit (the set of images of 1).

Next, for the similar function $m(x) = -1/(x+1)$, we find that $m^{(2)}(x)$ equals $(-x-1)/x$ and $m^{(3)}(x) = x$, the identity function. We say that m has order three under composition, and so $m(x)$ generates a finite group (isomorphic to C_3, the cyclic group of three elements). The following diagram shows the orbit of 2 under iteration by m:



Finally, consider $q(x) = 1/x$. Since $q^{(2)}(x)$ is the identity, q generates a group of order two. Of greater interest is the group generated by q and m together; these satisfy the relation $q \circ m = m^2 \circ q$, and so they generate a group of size six, isomorphic to the dihedral group D_3. The following picture illustrates a typical orbit under the group generated by $q(x)$:



This is the structure we are interested in: a set of fractional linear transformations, with integer coefficients, that forms a finite group under composition.

The nine finite groups Recall from our earlier discussion that $PGL(2, \mathbf{Q})$ represents the group of fractional linear transformations $(ax+b)/(cx+d)$ with integer coefficients such that $ad - bc \neq 0$. The following theorem gives our main result:

THEOREM 1. *All finite subgroups of $PGL(2, \mathbf{Q})$ are isomorphic to C_n or D_n for $n = 1, 2, 3, 4,$ or 6.*

Since $D_1 = C_2$, we see that there are actually just nine groups, as mentioned in the title. However, if we allow real coefficients in our fractional linear transformations (equivalently, real entries in our projective matrices), we can extend the list of possible finite groups:

THEOREM 2. *Every finite subgroup of $PGL(2, \mathbf{R})$ is either cyclic or dihedral, and there exist such subgroups of arbitrary order.*

Our proofs are constructive; see Corollary 1 for an explicit example of an element of $PGL(2, \mathbf{R})$ of arbitrary finite order under composition.

We've generalized from rational to real coefficients; what happens if we allow complex coefficients? Here we refer to a well-known result: any finite group of fractional linear transformations with complex coefficients (that is, a finite subgroup of

$PGL(2, \mathbf{C})$) is isomorphic to a finite group of symmetries of the sphere [**5**], and hence (as mentioned earlier) is isomorphic to a cyclic group C_n, a dihedral group D_n, or one of the symmetry groups A_4, S_4, and A_5 of the tetrahedron, cube, and icosahedron, respectively [**8**]. However, our Theorem 2 indicates that it is impossible to represent A_4, S_4, and A_5 using projective matrices $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ with real coefficients, since these groups are neither cyclic nor dihedral.

Constructing fractional linear transformations of finite order For the moment, let us allow complex coefficients, and let us consider how to construct fractional linear transformations of small order. Clearly, $e(x) = x$ has order 1 and $m(x) = -x$ has order 2 (under composition). It's interesting to note, however, that $-x + b$ also has order 2, for b any complex number. For order 4, we might guess at ix or even $ix + b$, and a moment's work shows that these both work.

The coefficients 1, -1, and i are all *primitive nth roots of unity* for $n = 1$, 2, and 4 respectively. Recall that for n a positive integer, we call ζ a primitive nth root of unity if $\zeta^n = 1$ and $\zeta^k \neq 1$ for every $0 < k < n$. Thus, ζ is a root of $x^n - 1$, and for $n > 1$ it is also a root of the polynomial $(x^n - 1)/(x - 1) = x^{n-1} + \cdots + x^2 + x + 1$. The only rational roots of unity are ± 1; the only quadratic roots are $\pm i$ and $\pm 1/2 \pm i\sqrt{3}/2$ (of orders 3, 4, and 6). All other roots of unity are cubic, quartic, or of even higher degree over the rationals [**4**, chapter 33]. For more information on field extensions and on degrees of algebraic numbers over $\mathbf{Q}$, see Gallian [**4**, chapters 20–21]. We note that one must be careful not to confuse the *order* of a primitive root of unity with its *degree* as an algebraic number over $\mathbf{Q}$, nor should we confuse it with the *order* of a fractional linear transformation under composition. These are all distinct concepts.

Based on our earlier work, we might suspect that the linear transformation $m(x) = \zeta x + b$ (with ζ, b complex) will have order n under composition if and only if ζ is a primitive nth root of unity. This is in fact the case, as can be seen by noticing that $m^{(n)}(x) = \zeta^n x + b(\zeta^{n-1} + \cdots + \zeta^2 + \zeta + 1)$. Thus, if ζ is a primitive nth root of unity, then $m(x)$ has order n, and vice versa.

How do we now proceed to find arbitrary fractional linear transformations of finite order? As it turns out, we can show that any fractional linear transformation $(ax + b)/(cx + d)$ is conjugate to some linear map $Ax + B$, and we now know exactly what is necessary for these linear maps to have finite order. (Recall that one defines two elements α, β of a group G to be *conjugate in G* if there is some $t \in G$ such that $\beta = t^{-1}\alpha t$. It is easy to show that conjugate elements have the same order.) Our first lemma is as follows:

LEMMA 1. *Suppose*

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

with rational coefficients, $ad - bc \neq 0$, has finite order under composition. Then, $m(x)$ has order 1, 2, 3, 4, or 6, and in the last three cases, $m(x)$ is conjugate (in $PGL(2, \mathbf{Q})$) to

$$\frac{-1}{x+1}, \frac{x-1}{x+1}, \quad \text{or} \quad \frac{2x-1}{x+1},$$

respectively.

REMARK. The order-2 maps are not all conjugate in $PGL(2, \mathbf{Q})$. In particular, for $p(x) = -4/x$, then $p(x)$ is not conjugate to $q(x) = 1/x$ using only transformations with rational coefficients. This can be seen by trying to find $s(x)$ such that $q = s^{-1} \circ p \circ s$; after much calculation, we find that $s(x)$ can only be $\pm 2ix$.

Proof. It's easy to verify that the three examples given in the lemma have order 3, 4, and 6. Note also that $q(x) = 1/x$ has order 2, and of course the identity map $e(x) = x$ has order 1.

We now show that 1, 2, 3, 4, and 6 are the only orders possible. Suppose that $m(x)$ is as above, with order $n < \infty$. If $c = 0$, then we can write $m(x) = (a/d)x + b/d$, a linear map, and so by our earlier discussion, $a/d = \pm 1$ (the only rational roots of unity) and $m(x)$ has order $n = 1$ or $n = 2$. If $c \neq 0$, we can solve the equation

$$\frac{ax + b}{cx + d} = x$$

to get at least one finite fixed point α for $m(x)$, of degree ≤ 2 over $\mathbf{Q}$. We conjugate $m(x)$ with $s(x) = \alpha + 1/x$ to get $\widehat{m}(x) = s^{-1} \circ m \circ s(x)$, a fractional linear transformation with coefficients in the (possibly quadratic) field $\mathbf{Q}(\alpha)$. Since s takes ∞ to α and m fixes α, then $\widehat{m}(\infty) = \infty$, which implies $\widehat{m}(x)$ is actually strictly linear, of the form $Ax + B$. Thus, since $\widehat{m}$ has the same (finite) order as m, then A is a primitive nth root of unity. Since $A \in \mathbf{Q}(\alpha)$ and since $\mathbf{Q}(\alpha)$ is at worst quadratic over $\mathbf{Q}$, then $A = \pm 1, \pm i$, or $\pm 1/2 \pm i\sqrt{3}/2$. Thus, $n = 1, 2, 3, 4$, or 6.

We finish by showing that, when $n = 3$, 4, or 6, $m(x)$ is conjugate to one of the transformations from our list in the above lemma. For $m(x)$ of order ≥ 3, choose three rational numbers A, B, and C such that $m(x) : A \mapsto B \mapsto C$. Let $s(x)$ be the fractional linear transformation that takes $0 \mapsto A$, $-1 \mapsto B$, and $\infty \mapsto C$ (note that this $s(x)$ will have rational coefficients). Then, for $\widehat{m}(x) = s^{-1} \circ m \circ s(x)$, we have that $\widehat{m}(x) : 0 \mapsto -1 \mapsto \infty$. This implies $\widehat{m}(x)$ has the form $(\widehat{a}x - 1)/(x + 1)$ for some $\widehat{a} = \widehat{m}(\infty)$, and it's now easy to show that the order of $\widehat{m}(x)$ being 3, 4, or 6 forces $\widehat{a}$ to equal 0, 1, or 2, respectively. ∎

In Lemma 1, we can't help but notice the suggestive pattern exhibited by the fractional linear transformations of orders 3, 4, and 6. Each has the form $(ax - 1)/(x + 1)$, with a from 0 to 2, and so we might think that $(3x - 1)/(x + 1)$ would also have finite order. Sadly, that isn't so; the sequence that describes the as is actually $a_n = 1 + 2\cos(2\pi/n)$, as we will see later.

The following lemma states that if we use only *real* coefficients, then we cannot represent A_4, S_4, or A_5 using fractional linear transformations. This is the last step; after this lemma, we can proceed directly to the proof of our two theorems.

LEMMA 2. *If K is a subfield of $\mathbf{R}$, then all finite subgroups of the set of fractional linear transformations with coefficients in K (equivalently, all finite subgroups of $PGL(2, K)$) are either cyclic or dihedral.*

Proof. By results of Lyndon and Ullman [**5**], we need only show that A_4, S_4, and A_5 cannot be realized in $PGL(2, K)$. We will show the impossibility of A_4; since $A_4 \subset S_4$ and $A_4 \subset A_5$, then this implies that S_4 and A_5 cannot be realized either.

Suppose we have a subgroup G isomorphic to A_4. Since A_4 contains elements of order 3, we can assume by Lemma 1 that (after an appropriate conjugation) $-1/(x + 1) \in G$. We note that the product of an element of order 3 (in A_4) with something of order 2 gives us a new element of order 3 (as is easily seen by considering products such as (abc) with $(ab)(cd)$; see Gallian again [**4**, p. 104] for a complete multiplication table for A_4). However, every element of order 2 in $PGL(2, K)$ has either the form $-x + b$ (if it fixes ∞) or $(ax + b)/(x - a)$ (if it takes ∞ to some finite a). Now, $-1/(x + 1)$ composed with $-x + b$ is $1/(x - b - 1)$, which has order 3 only for $b = -1 \pm i$. And, $-1/(x + 1)$ composed with

$$\frac{ax + b}{x - a} \quad \text{is} \quad \frac{-x + a}{(a + 1)x + (b - a)},$$

and a few minutes of algebra will show that this has order 3 only for $b = \frac{1}{2}(1 + 2a \pm \sqrt{-4a^2 - 4a - 3})$, a complex number for all real values of a. Thus, A_4 cannot be realized using only real coefficients. ■

Proof of theorems We are now ready to prove our main theorems, which we restate for convenience:

THEOREM 1. *All finite subgroups of PGL*$(2, \mathbf{Q})$ *are isomorphic to* C_n *or* D_n *for* $n = 1, 2, 3, 4,$ *or* 6.

THEOREM 2. *Every finite subgroup of PGL*$(2, \mathbf{R})$ *is either cyclic or dihedral, and there exist such subgroups of arbitrary order.*

Proof. By Lemma 2, we only need concern ourselves with cyclic and dihedral subgroups. To show $G = PGL(2, \mathbf{R})$ contains all cyclic and dihedral groups, we will show that for every $n > 0$, there exists an element $m(x)$ of order n such that for $q(x) = 1/x$, then $m(x)$ and $q(x)$ generate the dihedral group D_n (with C_n as a cyclic subgroup).

For $n = 1$, let $m(x) = x$, and for $n = 2$, let $m(x) = -x$. These clearly give us C_1, C_2 and (with $q(x) = 1/x$) D_1 and D_2. Now assume $n \geq 3$. Let ζ_n be a primitive nth root of unity, in particular, $e^{2\pi i/n}$, let $a_n = 1 + 2\cos(2\pi/n) = 1 + \zeta_n + 1/\zeta_n$ (a real number), and define $m(x)$ as $(a_n x - 1)/(x + 1)$. It's not hard to show that

$$m^{-1}(x) = \frac{x + 1}{-x + a_n}$$

and that $q^{-1} \circ m \circ q = m^{-1}$. We need only show that $m(x)$ has order n to exhibit our dihedral group D_n. A clever way to do this is to define $\widehat{m} = s^{-1} \circ m \circ s$ with $s(x) = \zeta_n + 1/x$; since $s(\infty) = \zeta_n$ and $m(\zeta_n) = \zeta_n$, we have that $\widehat{m}(\infty) = \infty$, and so $\widehat{m}(x) = Ax + B$ for some $A, B \in \mathbf{C}$. By comparing $\widehat{m}(x)$ and $s^{-1} \circ m \circ s(x)$ for $x = 0$ and $x = -1/\zeta_n$, we find that $A = \zeta_n$ and $B = \zeta_n/(\zeta_n + 1)$. By a previous discussion, $\widehat{m}(x)$ (and hence $m(x)$ itself) has order n. This proves Theorem 2.

If we now restrict ourselves to rational coefficients, then our discussion above, combined with Lemma 1, proves Theorem 1. (Note that only for $n = 3$, 4, or 6 does the element

$$m(x) = \frac{a_n x - 1}{x + 1}$$

have rational coefficients; these are exactly the elements mentioned in Lemma 1.) ■

The existence of a real fractional linear transformation of any order, as demonstrated in this proof, deserves its own statement:

COROLLARY 1. *For* $n \geq 3$ *and* $a_n = 1 + 2\cos(2\pi/n)$, *then* $(a_n x - 1)/(x + 1)$ *has order n under composition.*

For further study This article just touches the surface of the many fascinating topics associated with groups of fractional linear transformations and groups of matrices with restricted entries. For example, a great deal of attention has been paid to the *modular group* (denoted $\Gamma(1)$), which is the set

$$\left\{ \frac{ax + b}{cx + d} : ad - bc = 1, \quad a, b, c, d \in \mathbf{Z} \right\}.$$

This infinite group is generated by two noncommuting elements: $p(x) = -1/x$ and our old friend $m(x) = -1/(x + 1)$ [**9**]. One could also venture into representation

theory, which (loosely stated) asks which groups can be represented by matrices in $GL(V)$ for V a complex vector space [**7**]. Then there is the fascinating theory of iterations of rational functions. Ours are the quotients of linear polynomials and thus rather simple, but if one considers quotients of polynomials of degree greater than or equal to 2, one begins to venture into the rich area of complex dynamics (see Beardon [**1**], and also Devaney [**2**] for general analytic functions). As a single example, one can show that any rational function of degree 5 in numerator and denominator (even with just integer coefficients!) has periodic points (under iteration) of all orders (see Beardon [**1**, Theorem 6.2.2]).

Finally, there are a few open questions suggested by this article, such as: for which algebraic number fields K will all isomorphic finite groups in $PGL(2, K)$ actually be conjugate in $PGL(2, K)$? This is certainly true for $K = \mathbf{C}$ (see Shurman [**8**], and also Theorem 2.6.1 in the paper by Lyndon and Ullman [**5**]), and certainly not true for $K = \mathbf{Q}$ (as seen in the remark following Lemma 1, above). Most likely, more can be said. One might also ask how many nonconjugate groups (isomorphic to D_3, say) are in $PGL(2, \mathbf{Q})$, and if there is a way to describe or index them all.

REFERENCES

1. Alan F. Beardon, *Iteration of Rational Functions*, vol. **132** of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 1991,
2. Robert L. Devaney, *An Introduction to Chaotic Dynamical Systems*, 2nd ed., Addison-Wesley Studies in Nonlinearity, Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989.
3. Stephen D. Fisher, *Complex Variables*, Brooks/Cole, Monterey, CA, 1986.
4. Joseph A. Gallian, *Contemporary Abstract Algebra*, 5th ed., Houghton Mifflin, Boston, MA, 2002.
5. R. C. Lyndon and J. L. Ullman, Groups of elliptic linear fractional transformations, *Proc. Amer. Math. Soc.* **18** (1967), 1119–1124.
6. Walter Rudin, *Real and Complex Analysis*, McGraw-Hill, New York, 1987.
7. Jean-Pierre Serre, *Linear Representations of Finite Groups*, vol. **42** of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 1977. Translated from the second French edition by Leonard L. Scott.
8. Jerry Shurman, *Geometry of the Quintic*, A Wiley-Interscience Publication, John Wiley & Sons Inc., New York, 1997.
9. Joseph H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, vol. **151** of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 1994.
10. Gabor Toth, *Glimpses of Algebra and Geometry*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1998.

Path Representation of One-Dimensional Random Walks

OSCAR BOLINA
Departamento de Física-Matemática
Universidade de São Paulo
Caixa Postal 66318
São Paulo 05315-970 BRASIL
bolina@if.usp.br*

Imagine a particle moving on the x axis, starting at some initial position $x = k, k > 0$, and moving back and forth on the line by random steps of unit length. Suppose that the particle moves right with probability p and left with probability $1 - p$, where, of course, $0 < p < 1$.

*Present address: Department of Mathematics, University of California, Davis, CA, 95616-8633.