The Finite Lamplighter Groups: A Guided Tour

Jacob A. Siehler

Jacob Siehler (siehlerj@wlu.edu) earned a Ph.D. at Virginia Tech and now teaches at Washington & Lee University. His research interests include finite groups, monoidal categories, and low-dimensional topology—as well as sneaking away, whenever possible, to study games, puzzles, and recreational mathematics of all sorts.

The appeal of dirty hands

What I'm about to disclose might be considered a dirty secret for a pure mathematician: in my first abstract algebra course, I obligingly proved all the propositions that were asked of me as neatly as I could, but what I really wanted to do was to go out to the mathematical garage and get my hands greasy. I always had an urge to break particular groups apart, make charts and tables, count subgroups, tally elements according to various properties I dreamt up, and find out just exactly what conjugates and centers and commutators and "all that stuff" *looked like*, until I felt like I could legitimately say I really *knew* the group. Forgive my italics, but this still gets me a little worked up. It was a particular joy when I met a new group, or a new family of groups, that I hadn't seen before.

To share the joy, here is a family of groups I met recently, which are easy to understand—no harder than the ubiquitous dihedral groups, say—and give rewarding answers to many of the questions an intrepid explorer might pose after seeing some of the fundamental concepts in group theory. Anyone familiar with the group theory terms I've used up to this point (and a little linear algebra) will feel at home here. We answer a few questions about these groups together, concentrating on the three C's (conjugates, centers, and commutators), and send you on your way with a few problems for further investigation.

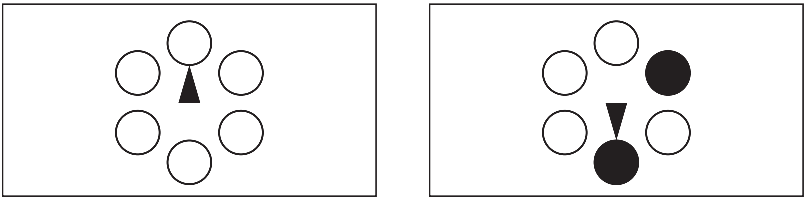
Turning and toggling

To business. We define a group L_n ('L' for 'lamplighter') for each integer $n \geq 1$. In the same way that the dihedral group D_{2n} can be defined in terms of operations ("rotate and reflect") on a regular n-sided polygon, L_n is defined in terms of operations ("turn and toggle") on a machine, M_n, consisting of n lamps arranged in a circle and a lighter which can be turned toward any of the lamps. Imagine a lovely contraption with lots of glass, gears, and polished metal, as in Figure 1. It won't affect the mathematics, but it is more exciting than a pedestrian diagram such as Figure 2(a), which shows the

http://dx.doi.org/10.4169/college.math.j.43.3.203
MSC: 20-01

Figure 1. A fancy model of the 6-lamp machine M_6 (illustration by Ruben de Vela).

6-lamp machine M_6 in its *initial state:* all the lamps off (empty circles) and the lighter pointed at the topmost lamp. Figure 2(b) shows a less pristine state of M_6. Every state of the machine can be encoded by an n-bit string to indicate the state of the lamps (clockwise *starting from the lighter*, with 1's for lit lamps), together with an integer in $\{0, \ldots, n-1\}$ indicating the position of the lighter. There are $n \cdot 2^n$ possible states for a machine with n lamps.



(a) Initial state: (000000, 0).

(b) (100010, 3), the result of applying $\alpha\rho^2\alpha\rho$ to (a).

Figure 2. Two states of the 6-lamp machine.

The group L_n consists of *actions* on M_n. It is generated by ρ, the action of moving the lighter to the next lamp clockwise, and α, the action of *toggling* whichever lamp the lighter is pointing to: turning it on if it's off, or vice versa. Both operations are invertible, as α is its own inverse, and $\rho^{-1} = \rho^{n-1}$ in L_n. Order matters, since $\rho\alpha$ ("toggle the current lamp, then move the lighter clockwise") has a different effect than $\alpha\rho$ ("move the lighter clockwise, then toggle that lamp"). I use the usual order for composition of functions: the rightmost action occurs first. For example, Figure 2(b) can be achieved by $\alpha\rho^2\alpha\rho$, or just as well by $\rho^2\alpha\rho^4\alpha\rho^3$.

There's an important principle here: group elements in L_n (actions) can be identified, bijectively, with states of M_n by identifying each group element with the result of its action on the initial state. This reveals any lamps toggled by the action (they end up lit) and how far the lighter ultimately moves, relative to its initial position. In this way, every ordered pair has a useful double meaning. For one thing, it tells us immediately that L_n is a group of $n \cdot 2^n$ elements. This double meaning is potentially confusing, however, so let's examine the example of Figure 2 carefully. As a *state*, (100010, 3) represents the static picture of Figure 2(b). As a *group element*, (100010, 3) denotes that action which changes Figure 2(a) to Figure 2(b). This action could be repeated, followed by other actions, applied to any other state of the machine, and so on. The action of group element $\beta = (100010, 3)$ is summed up as "The pointer advances three steps clockwise. The first and fifth lamps, as read clockwise from the new pointer position, are toggled." Mechanically, β might be achieved by various combinations of turns and toggles (e.g., $\rho^2\alpha\rho^4\alpha\rho^3$). The ordered pair puts that aside and represents the net result of the action in a uniform way. This abstraction suppresses any literal mechanical details, making calculations easier.

To get a feel for this, take another element in L_6. Figure 3 shows the result of applying $(100011, 5)$ ("5 steps clockwise; then toggle the 1st, 5th and 6th lamps from the pointer") after applying $(100010, 3)$ to the initial state. This is written $(100011, 5)(100010, 3)$, opposite the order of the pictures. The result, $(110010, 2)$, is the action that changes the initial state to the final state in Figure 3. Notice that the same ordered pair, interepreted as a *state*, is the result of performing the action $(100011, 5)$ on the state $(100010, 3)$. If this makes sense, you're well on top of things.

Try this: What is the order of $(100011, 5)$? You may use diagrams like Figure 3 but be alert for shortcuts.

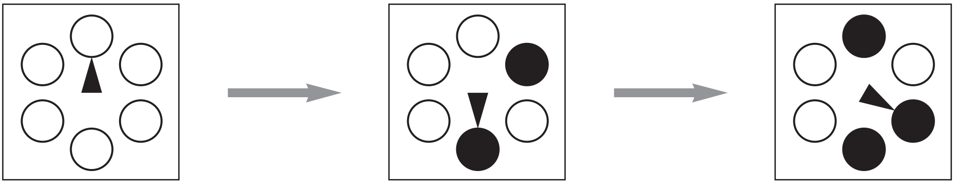


Figure 3. $(100011, 5)(100010, 3) = (110010, 2)$.

The twisty arithmetic of ordered pairs

It is not easy to tell, just by looking at it, what the order of an element like $(100011, 5)$ is. (The answer is twelve, incidentally.) You can see that it would be inconvenient to resort to diagrams each time the issue came up. I won't give a formula for the order of an arbitrary element here, but by the end of the article you should be able to work it out yourself, using the tools we now develop.

To begin, let $\text{Rot}(\vec{u}, k)$ denote the binary string $\vec{u}$ with its bits rotated k positions to the left. For example, $\text{Rot}(101001101, 1) = 010011011$ and $\text{Rot}(101001101, 2) = 100110110$ and so on. Negative values of k indicate rotation to the right. I have written $\vec{u}$ as if it were a vector, and we will treat an n-bit binary string as an n-dimensional vector—specifically, a vector whose components belong to $\mathbb{F}_2$, the field of integers mod 2. Using mod 2 arithmetic lets the 1's in the vector model the on-and-off toggling behavior. With this in mind, you just have to think through the steps to see that

$$(\vec{v}, k)(\vec{u}, j) = (\vec{v} + \text{Rot}(\vec{u}, k), k + j \pmod n) \tag{1}$$

describes the group multiplication in L_n. Check this for Figure 3. This gives a complete, if abstract, description of L_n, and we summarize the essential facts:

1. L_n is a nonabelian group of order $n \cdot 2^n$, generated by the turn and toggle operations, ρ and α.
2. Elements of L_n can be represented by ordered pairs $(\vec{v}, k)$, where $\vec{v} \in \mathbb{F}_2^n$ and $k \in \mathbb{Z}/n\mathbb{Z}$, the additive group of integers mod n. As ordered pairs, the generators are $\rho = (\vec{0}, 1)$ and $\alpha = (10\cdots0, 0)$.
3. Composition of elements in L_n is described by equation (1).

4. The identity element in L_n is $(\vec{0}, 0)$.
5. The inverse of $(\vec{v}, k)$ in L_n is $(\mathrm{Rot}(\vec{v}, -k), -k)$.

By the way, the righthand side of (1) has a useful interpretation as a state. It's the result of applying action $(\vec{v}, k)$ to a machine in an arbitrary state $(\vec{u}, j)$.

Are you two related?

Which, if any, of the three elements

$$a = (101110001010, 8), \quad b = (101100110010, 8), \quad c = (000101101011, 8), \quad (2)$$

are conjugate to one another in L_{12}? Go ahead. I'll wait while you figure it out.

To approach this systematically, let's see what an arbitrary conjugate of an element $(\vec{v}, k)$ in L_n looks like. Using (1) and simplifying, we get

$$(\vec{u}, j)(\vec{v}, k)(\vec{u}, j)^{-1} = (\mathrm{Rot}(\vec{v}, j) + \vec{u} + \mathrm{Rot}(\vec{u}, k), k)\,,$$

which tells us immediately that *conjugate elements have the same rotation number*. We could say that $(\vec{w}, k)$ is conjugate to $(\vec{v}, k)$ if $\vec{w} = \mathrm{Rot}(\vec{v}, j) + \vec{u} + \mathrm{Rot}(\vec{u}, k)$ for some $\vec{u} \in \mathbb{F}_2^n$ and some integer j, but this is not a practical criterion to check directly! On the other hand, the function $f_k : \mathbb{F}_2^n \to \mathbb{F}_2^n$ defined by $f_k(\vec{u}) = \vec{u} + \mathrm{Rot}(\vec{u}, k)$ is a linear transformation, and this gives us a foothold.

Since we compute mod 2, the kernel of f_k is easy to characterize: $\vec{u} \in \ker f_k$ if and only if $\vec{u} = \mathrm{Rot}(\vec{u}, k)$. It follows, inductively, that $\vec{u} = \mathrm{Rot}(\vec{u}, sk)$, for any integer s. Let $m = \gcd(n, k)$. By the Euclidean Algorithm, we can choose integers r and s so that $m = rn + sk$. Then

$$\mathrm{Rot}(\vec{u}, m) = \mathrm{Rot}(\vec{u}, rn + sk) = \mathrm{Rot}(\mathrm{Rot}(\vec{u}, sk), rn) = \mathrm{Rot}(\vec{u}, rn) = \vec{u}.$$

Since $\vec{u}$ is a vector of length n, rotating it by multiples of n has no effect. We have proved that if $\vec{u} \in \ker f_k$, then $\vec{u}$ is periodic with period m. Conversely, if $\vec{u}$ is periodic with period m, then $\mathrm{Rot}(\vec{u}, k) = \vec{u}$ (since $m|k$), which implies $\vec{u} \in \ker f_k$. Periodicity is more striking when vectors are represented circularly, as in Figure 4.

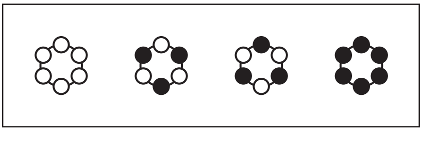


Figure 4. Graphic representation of the four vectors (000000, 010101, 101010, and 111111) in $\mathbb{F}_2^6$ which have period 2. These four comprise the kernel of both f_2 and $f_4 : \mathbb{F}_2^6 \to \mathbb{F}_2^6$.

So, $\ker f_k$ consists of precisely those vectors which are periodic with period $m = \gcd(n, k)$, and this is an m-dimensional subspace of $\mathbb{F}_2^n$. By the rank-nullity theorem, the image of f_k (let's call it X_k), has dimension $n - m$.

In order to obtain a nice criterion for recognizing conjugates of $(\vec{v}, k)$ in L_n, we introduce one more linear transformation, $p_k : \mathbb{F}_2^n \to \mathbb{F}_2^m$. To compute $p_k(\vec{u})$, partition $\vec{u}$ into vectors of length $\gcd(n, k)$ and add them together. For example,

$$p_8(101110001010) = 1011 + 1000 + 1010 = 1001,$$

which I like to write with the bits arranged in a circle:

$$p_8(101110001010) =$$ .

Quirky notation aside, p_k is easy to compute, and clearly a linear transformation. It also commutes with rotations, that is, $p_k(\text{Rot}(\vec{u}, j)) = \text{Rot}(p_k(\vec{u}), j)$. Now, I claim that X_k, as defined above, is contained in $\ker p_k$. Why? A typical element in X_k has the form $\vec{u} + \text{Rot}(\vec{u}, k)$, and

$$\begin{aligned} p_k\left(\vec{u} + \text{Rot}(\vec{u}, k)\right) &= p_k(\vec{u}) + p_k\left(\text{Rot}(\vec{u}, k)\right) \\ &= p_k(\vec{u}) + \text{Rot}(p_k(\vec{u}), k) \\ &= p_k(\vec{u}) + p_k(\vec{u}), \text{ since } p_k(\vec{u}) \in \mathbb{F}_2^m \text{ and } m|k \\ &= 0. \end{aligned}$$

Moreover, p_k is surjective. Pick any vector $\vec{x}$ in $\mathbb{F}_2^m$ and append $(n - m)$ zeros. You've just constructed a vector in the preimage of $\vec{x}$ under p_k. Thus $\dim\ker p_k = n - m = \dim X_k$, and this shows that $\ker p_k = X_k$.

Now, the element $(\vec{w}, k)$ is conjugate to $(\vec{v}, k)$ in L_n

$$\begin{aligned} &\iff \vec{w} = \text{Rot}(\vec{v}, j) + \vec{u} + \text{Rot}(\vec{u}, k) \text{ for some } (\vec{u}, j) \in L_n \\ &\iff \vec{w} \in \text{Rot}(\vec{v}, j) + X_k \\ &\iff p_k(\vec{w}) = p_k\left(\text{Rot}(\vec{v}, j)\right) \text{ since } X_k = \ker p_k \\ &\iff p_k(\vec{w}) = \text{Rot}(p_k(\vec{v}), j). \end{aligned}$$

Call $p_k(\vec{v})$ the *p-vector* associated to the element $(\vec{v}, k)$ in L_n. We have proved the

Conjugacy criterion. *Two elements are conjugate in L_n if and only if they have the same rotation number, and the same p-vector (up to rotation).*

Example. The three elements $a, b, c \in L_{12}$ in (2) have the same rotation number, but their p-vectors are:

$p(a) =$ , $p(b) =$ , and $p(c) =$ .

If those bits were black and white beads on a necklace, then $p(a)$ and $p(c)$ would be indistinguishable. Thus, a and c are conjugates, but $p(b)$ has a different pattern, even with rotations allowed, and b is not conjugate to the other two.

Notes on necklaces

To determine conjugacy in L_n, we end up considering two binary strings the same if they agree up to rotation. This equivalence relation separates binary strings of any given length—d, say—into equivalence classes known as *binary necklaces* of length d. There is a marvelous formula for counting the number of distinct necklaces of a given length:

$$(1/d) \sum_{s|d} 2^s \phi(d/s), \tag{3}$$

where $\phi(n)$ denotes the number of positive integers less than n and relatively prime to n. (For a proof of the formula, see [**2**]; see [**6**] for a wealth of additional comments and references.)

If you want to count the conjugacy classes in L_n, this formula is just the ticket. By the Conjugacy Criterion, L_n has one conjugacy class for each rotation number $k \in \{0, \dots, n-1\}$, and for each binary necklace of length $\gcd(n,k)$. Using (3), the total number of conjugacy classes in L_n is given by

$$\sum_{k=0}^{n-1} \left((1/\gcd(n,k)) \sum_{s \mid \gcd(n,k)} 2^s \Phi(\gcd(n,k)/s) \right), \tag{4}$$

which looks unwieldy, but is actually easy to compute. Results are tabulated in Table 1 for small values of n.

Table 1. Number of conjugacy classes in L_n, for small n.

n	1	2	3	4	5	6	7	8	9	10	11	12
	2	5	8	13	16	28	32	56	80	136	208	400

All 28 classes in L_6 are represented in Figure 5. As an exercise, think for a moment which classes contain more than one element, and which contain only a single element. Also, why would a similar table illustrating the 32 conjugacy classes in L_7 be comparatively boring?

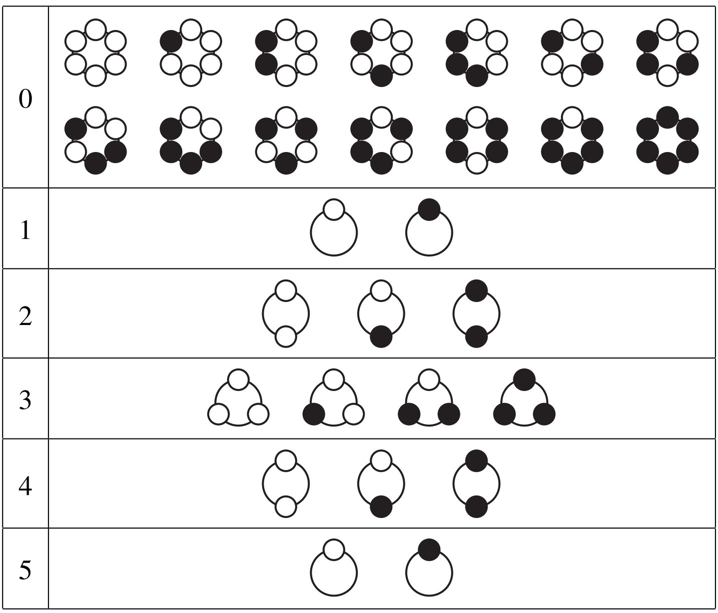


Figure 5. The 28 conjugacy classes in L_6.

The center is just a big flip

A good description of the center is another *sine qua non* for any claim to "really understand" a group. The center $Z(L_n)$ of L_n is small and you can find it without a single calculation by thinking of necklaces. Recall that $Z(L_n)$ consists of those elements which commute with *every* element in L_n. Equivalently, an element belongs to the center if it is the only element in its conjugacy class.

How can $(\vec{v}, k)$ be the only element in its conjugacy class? First of all, the map $p_k : \mathbb{F}_2^n \to \mathbb{F}_2^m$ (where $m = \gcd(n, k)$) must be injective, otherwise there are many elements with the same p-vector as $(\vec{v}, k)$, not even counting rotations. We computed $\dim \ker p_k = n - m$, so for p_k to be injective, $n = m = \gcd(n, k)$ and that means $k = 0$. Central elements in L_n have rotation number 0.

Not only that, for $(\vec{v}, 0)$ to be in $Z(L_n)$, it must satisfy $\vec{v} = \mathrm{Rot}(\vec{v}, 1)$. Otherwise, $(\mathrm{Rot}(\vec{v}, 1), 0)$, which has the same p-vector up to rotation, would be another element in the same conjugacy class! But that is a very strong requirement: it says that $\vec{v}$ is either all 0's or all 1's. Its conjugacy class is represented by a single-color necklace of size n. Voilà.

The center. *$Z(L_n)$ is a subgroup of order 2, for every $n \geq 1$. The nontrivial element is $(\vec{1}, 0)$, representing the operation, "toggle every lamp, and don't move the lighter".*

Note how the central element can be described in a coordinate-free way without referring to specific positions. Puzzle fans may be reminded of the Rubik's Cube group, in which the only nontrivial central element can be described similarly as "flip every edge piece" (see [**5**]).

We have ways of making you commute

The nonabelian nature of L_n (for $n > 1$) is shown by its tiny center, and also by the existence of nontrivial commutators in the group. Recall that the commutator of two elements x and y is defined by $[x, y] = xyx^{-1}y^{-1}$, which is the identity if and only if x and y commute. How do we recognize a commutator in L_n? Define the *parity* of a vector to be 0 (even parity) or 1 (odd parity) according as the vector contains an even or odd number of 1's. This is another linear transformation, $\mathrm{Par} : \mathbb{F}_2^n \to \mathbb{F}_2$ defined by

$$\mathrm{Par}(\vec{v}) = \sum_i \vec{v}_i .$$

The rank-nullity theorem tells us that the even-parity vectors are of dimension $(n - 1)$ in $\mathbb{F}_2^n$, so there are 2^{n-1} of them.

Now, an arbitrary commutator in L_n looks like this (after simplifying):

$$[(\vec{u}, j), (\vec{v}, k)] = (\vec{u} + \vec{v} + \mathrm{Rot}(\vec{u}, k) + \mathrm{Rot}(\vec{v}, j), 0) . \qquad (5)$$

The rotation number is necessarily zero. Also, any two rotations of the same vector, when added together, must give even parity (every 1 that occurs is counted twice). So every commutator belongs to the set

$$E_n = \left\{(\vec{v}, 0) \in L_n \,\middle|\, \mathrm{Par}(\vec{v}) = 0\right\},$$

which, incidentally, is a subgroup of L_n. And since all the rotation numbers are zero, the group operation inside E_n reduces to simply adding vectors, mod 2. On the other hand, consider the following special case of equation 5:

$$[(\vec{u}, 0), (\vec{0}, 1)] = (\vec{u} + \mathrm{Rot}(\vec{u}, 1), 0) = (f_1(\vec{u}), 0),$$

where f_1, as we have seen, is a linear map whose image has dimension $n-1$. Thus, every element of E_n can be expressed as a commutator of this form.

Commutator subgroup and abelianization. *The commutator subgroup $[L_n, L_n]$ consists precisely of the elements of even parity and zero rotation. It is an abelian group of order 2^{n-1}, in which every element has order 2. The quotient group $L_n/[L_n, L_n]$ is isomorphic to a direct product of cyclic groups, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$.*

To prove this, define $\pi : L_n \to (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ by $\pi(\vec{v}, k) = (\mathrm{Par}(\vec{v}), k)$. Check that π is a surjective homomorphism, whose kernel is precisely E_n. The Fundamental Homomorphism Theorem then gives the desired isomorphism. Perhaps more important than this quick proof (which doesn't reveal how the proposition was discovered in the first place) is to interpret the meaning of an element in this quotient group. What is forgotten in passing from L_n to L_n/E_n is the matter of precisely which lamps are toggled on or off. All that is remembered by the quotient map π is whether an even or odd number of lamps have been toggled (the $\mathbb{Z}/2\mathbb{Z}$ factor), and the rotation of the lighter (the $\mathbb{Z}/n\mathbb{Z}$ factor).

Question. Can you explain exactly what's "forgotten" in the quotient $L_n/Z(L_n)$?

Furthering your acquaintance

Outside this paper, *the* lamplighter group refers to an *infinite* group which uses an infinite strip of lamps ($\mathbb{Z}$ as opposed to $\mathbb{Z}/n\mathbb{Z}$). It appears in many articles on random walks (e.g., [**4**]). I do not know who first coined the lamplighter name; the group appears anonymously in 1983 [**3**], but surely it has been known for a very long time.

The finite versions presented here aren't new discoveries, but they make such a wonderful case study in basic concepts of finite groups that they should be widely known as a family with a name. Like the dihedral groups, they can be described compactly as semidirect products (see [**1**]), without reference to machines and operations.

There are many additional accessible, enjoyable questions to ask about these groups. Here are just a few, no more difficult than the questions we have already answered.

1. Find a formula for the size of the conjugacy class of a given element $(\vec{v}, k)$ in L_n. (Hint: Consider the period of the p-vector, if it is periodic.)
2. Find a formula for the order of an element $(\vec{v}, k)$ in L_n. (Hint: Elements behave differently in this respect, depending on whether their p-vector is zero or not). What's the maximum order of an element in L_n?
3. Characterize the elements $\beta \in L_n$ for which ρ and β generate all of L_n. If you would rather have a specific little puzzle, my birthday was in July, 1975. Can you express α in terms of ρ and $\beta = (011110110111, 7)$ in L_{12}?

For some small n, you can connect L_n to well-known groups.

4. Show that L_2 is isomorphic to the dihedral group of 8 elements, and L_3 is isomorphic to $A_4 \times Z_2$.

My last question is an open-ended one for which I do not have a satisfying answer, even for small n:

5. L_n is generated by two elements, ρ and α. Is there a presentation of L_n with two generators and a small number of relations?

Finally, if you like to generalize, consider replacing the on-off lamps in your machine with 3-way lamps. Or 4-way lamps, or two overlapping circles of lamps that can turn independently, or . . . well, have fun! Wherever you decide to explore, leave a light on for me before you move on.

Summary. In this article, we present a family of finite groups, which provide excellent examples of the basic concepts of group theory. To work out the center, conjuagacy classes, and commutators of these groups, all that's required is a bit of linear algebra.

References

1. D. Dummit and R. Foote, *Abstract Algebra*, John Wiley, New York NY, 2004.
2. R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics*, Addison-Wesley, Reading MA, 1994.
3. V. A. Kaimanovich and A. M. Vershik, Random walks on discrete groups: Boundary and entropy, *Ann. Prob.* **11** (1983) 457–490; available at http://dx.doi.org/10.1214/aop/1176993497.
4. R. Lyons, R. Pemantle, and Y. Peres, Random walks on the lamplighter group, *Ann. Prob.* **24** (1996) 1993–2006; available at http://dx.doi.org/10.1214/aop/1041903214.
5. D. Singmaster, *Notes on Rubik's Magic Cube*, Enslow Publishers, Hillside NJ, 1981.
6. N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*; available at http://www.research.att.com/~njas/sequences/A000031.

Null Law Suits

With regard to the proliferation of legal proceedings concerning U.S. President Barak Obama's birthplace:

> These cases are like trying to divide by zero. They're halfway between nonsense and zero.

—*The Rachel Maddow Show*, January 26, 2012
—suggested by Margaret Cibes