Constructing a Minimal Counterexample in Group Theory

ARNOLD D. FELDMAN
Franklin and Marshall College
Lancaster, PA 17604

Desmond MacHale's intriguing article [**2**] neatly illustrates one mode of interplay between proof and example in group theory by describing the commonly used inductive technique of minimal counterexamples. In this Note, we use some ideas from group theory and linear algebra to lead the reader through a geometric and algebraic construction of one of the minimal counterexamples sought by MacHale.

Recall that a group is called **nilpotent** if each of its Sylow subgroups is normal. One of MacHale's list of known-to-be-false conjectures is this: if G is a finite group having a fixed-point-free automorphism ϕ, then G is nilpotent. The true theorem on which the conjecture is based assumes that ϕ is of prime order; it was established by Thompson in his dissertation in 1959 [**4**]. His proof so excited the mathematical community that even the New York Times reported his result and the reaction to it [**3**]. MacHale indicates that [**1**, p. 336] contains details of a counterexample to the conjecture with $|G| = 147 = 7^2 \cdot 3$ and $|\phi| = 4$. In our minimal counterexample to be constructed, $|\phi| = 6$ and $|G| = 48 = 2^4 \cdot 3$.

In what follows, we use some standard conventions of notation in group theory. In particular, we write operators on the right and denote both the action of a group homomorphism and conjugation using superscripts.

Recall that if H and K are subgroups of a group G such that $G = HK$, $H \cap K = 1$, and H is normal in G, then G is called the **semidirect product** of H by K. In this situation, since H is normal in G, each element of K acts via conjugation as an automorphism of H. Of particular interest here is the situation in which each nontrivial element of K acts as a nontrivial (i.e., nonidentity) automorphism on H. In this case K is isomorphic to a subgroup of Aut H, the group of all automorphisms of H.

A well-known geometric example leads directly to an important link between group theory and geometry. If A is the group of rotations of a regular tetrahedron, then A contains eight elements of order 3, three of order 2, and an identity element. Each element of order 3 is a 120°rotation of the tetrahedron about an axis passing through one of the 4 vertices and perpendicular to the opposite face. Each element of order 2 is a rotation of 180° about one of three axes joining the midpoints of two nonadjacent edges of the tetrahedron. (See FIGURE 1.) If the vertices are labeled, and each rotation is identified with the permutation of the labels it produces, this identification provides a natural isomorphism between A and A_4, the group of even permutations on 4 letters. Thus it is possible to use the algebra of permutations or geometry to analyze A.

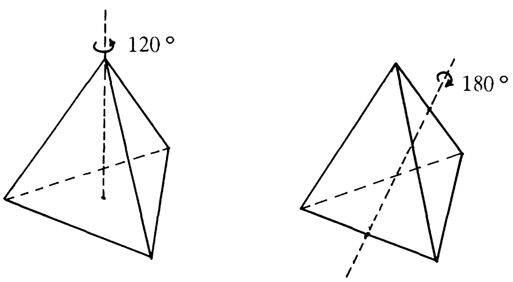

FIGURE 1

It is easy to see that A has a unique subgroup V of order 4, consisting of the identity element and the three elements of order 2. Thus if $x \neq 1$ is an element of V and σ is an element of order 3 in A, $x^\sigma = \sigma^{-1}x\sigma = y$ is in V and it is simple to check, using geometry or algebra, that $x \neq y$. Hence $V = \{1, x, y, xy\}$. Since conjugation by σ fixes only the identity element of V, we say that σ is a **fixed-point-free** automorphism of V. Using $\langle \sigma \rangle$ to denote the cyclic group of order 3 generated by σ, we have $A = V\langle \sigma \rangle$, the semidirect product of V by $\langle \sigma \rangle$.

We can learn more about the automorphism σ by rewriting V as an additive group and considering the 2×2 matrix M_σ associated with σ. This we do as follows:

Identify V with $(Z_2)^2$, the direct product of two additive groups of order 2. Identify x with $(1,0)$ and y with $(0,1)$, so that xy corresponds to $(1,1)$ and 1 corresponds to $(0,0)$. Thus in the semidirect product A, $(1,0)^\sigma = (0,1)$, $(0,1)^\sigma = (1,1)$, and $(1,1)^\sigma = (1,0)$. Of course, $(0,0)^\sigma = (0,0)$. We obtain the matrix M_σ associated with σ by using for its rows the images under σ of the "standard" basis elements $(1,0)$ and $(0,1)$ under conjugation by σ. Thus

$$M_\sigma = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Since $v^\sigma = vM_\sigma$, $v^\sigma = v$ if and only if $v = vM_\sigma$. Thus the fact that σ is fixed-point-free is equivalent to the fact that there exists no element v of V other than $(0,0)$ such that $vM_\sigma = v$.

The Counterexample

We use more geometry to construct our minimal counterexample of a nonnilpotent group G having a fixed-point-free automorphism. First, let T_1 and T_2 be congruent regular tetrahedra, with the vertices of T_1 labeled 1, 2, 3, 4, and the vertices of T_2 labeled 5, 6, 7, 8. (See FIGURE 2a.) Also, consider the set S of 8 labeled points in 3-space depicted in FIGURE 2b; S consists of two subsets S_1 and S_2, each of which contains the vertices of a tetrahedron the same size as each of T_1 and T_2. For $i = 1$ or 2, if we place T_i on S_i in such a way that the vertices and labels match, we say T_i is in "home position". In FIGURE 2c, both T_1 and T_2 are in home position. In FIGURE 2d, only T_2 is in the home position.

There are 12 ways to place T_1 on S_1 with vertices on vertices, corresponding to the 12 elements of the group of rotations of a tetrahedron. Similarly, there are 12 ways to place T_2 on S_2. Thus there are $12 \cdot 12 = 144$ ways of placing T_1 on S_1 and T_2 on S_2. Similarly, there are 144 ways of placing T_2 on S_1 and T_1 on S_2. Thus there are 288 ways of placing the pair of tetrahedra T_1 and T_2 onto the framework formed by the subsets S_1 and S_2 of S. Each of these 288 positions for T_1 and T_2 corresponds to a permutation of the 8 elements of S, with the home position for both T_1 and T_2, depicted in FIGURE 2c, corresponding to the identity permutation. Any other position for T_1 and T_2 corresponds to the unique permutation of S required to take the vertices of T_1 and T_2 to this position from the home position. For example, the position of T_1 and T_2 in FIGURE 2d corresponds to the permutation (2 3 4).

The set U of permutations of S that corresponds to this set of 288 positions for T_1 and T_2 on S is clearly a subgroup of the group of permutations of S. We will show that U has a nonnilpotent subgroup G of order 48 and an element ϕ of order 6 which is a fixed-point-free automorphism of G via conjugation as an element of U. This G and ϕ provide the minimal counterexample described in the introduction. To construct that counterexample we need to introduce several subgroups of U.

Denote by A_1 the subgroup of elements of U that do not affect S_2. Thus if we start with T_1 and T_2 in home position as in FIGURE 2c and apply an element of A_1, we obtain a result in which T_1 is still on S_1 in one of 12 positions, and T_2 is still on S_2 in home position. Thus the elements of A_1 correspond to the rotations of the tetrahedron T_1, so A_1 is isomorphic to the group $A = V\langle \sigma \rangle$ described above. Similarly, denote by A_2 the subgroup of elements of U not affecting S_1. Thus the elements of A_2 correspond to the rotations of the tetrahedron T_2, and A_2 is also isomorphic to A. It is easy to see that A_1 and A_2 have trivial intersection and that the elements of A_1 commute with the elements of A_2, so U has a subgroup $A_1 \times A_2$. Since the index of $A_1 \times A_2$ in

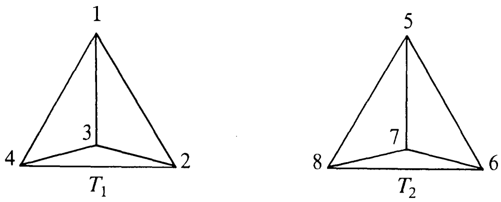

FIGURE 2a

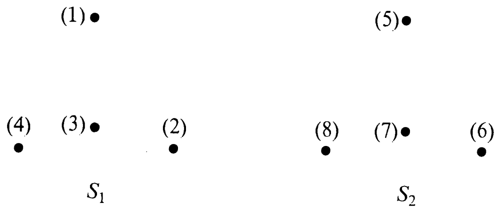

FIGURE 2b

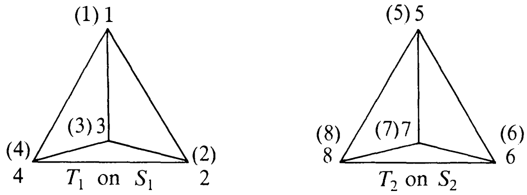

FIGURE 2c

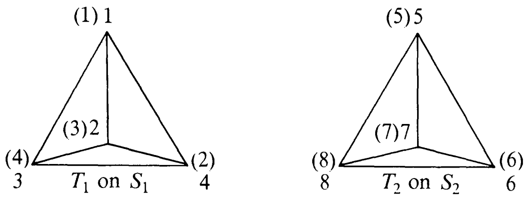

FIGURE 2d

U is 2, $A_1 \times A_2$ is a normal subgroup of U.

There is an element τ of U which corresponds to translating T_1 to the right and T_2 to the left from their respective home positions, so that T_1 is on S_2 and T_2 is on S_1. Thus, after application of τ, the vertex of T_1 labeled j will be at the point of S_2 labeled $(j+4)$, and the vertex of T_2 labeled k will be at the point of S_1 labeled $(k-4)$. Since $\tau^2 = 1$, $\langle \tau \rangle$ is a cyclic group of order 2. The elements of $A_1 \times A_2$ leave T_1 on S_1 and T_2 on S_2, so $A_1 \times A_2$ and $\langle \tau \rangle$ intersect trivially. Thus the semidirect product $(A_1 \times A_2)\langle \tau \rangle$ has order $144 \cdot 2 = 288$, so $(A_1 \times A_2)\langle \tau \rangle = U$.

Just as A has a unique subgroup V of order 4, each A_i has a unique subgroup V_i of order 4. Then $V_1 \times V_2$ is the unique subgroup of order 16 in $A_1 \times A_2$. This uniqueness implies $V_1 \times V_2$ is normal in U, since $A_1 \times A_2$ is normal in U. Therefore, each element of U acts on $V_1 \times V_2$ as an automorphism via conjugation.

Now consider V_1, V_2, and $V_1 \times V_2$ as additive groups, writing $V_1 \times V_2 = \{(x_1, x_2, x_3, x_4) | x_1, x_2, x_3, x_4 \in Z_2\}$, where $\{(1,0,0,0),(0,1,0,0)\}$ generates V_1 as a subgroup of $V_1 \times V_2$ and $\{(0,0,1,0),(0,0,0,1)\}$ generates V_2. Then we can represent automorphisms of $V_1 \times V_2$ by 4×4 matrices with entries in Z_2.

For example, let σ_1 be the element of A_1 analogous to the element σ of A described earlier; the position of T_1 and T_2 corresponding to σ_1 is depicted in FIGURE 2d. The analogy to $A = V\langle \sigma \rangle$ yields $(1,0,0,0)^{\sigma_1} = (0,1,0,0)$ and $(0,1,0,0)^{\sigma_1} = (1,1,0,0)$. Also, as an element of A_1, σ_1 commutes with each element of A_2, including the generators $(0,0,1,0)$ and $(0,0,0,1)$ of V_2. Thus $(0,0,1,0)^{\sigma_1} = (0,0,1,0)$ and $(0,0,0,1)^{\sigma_1} = (0,0,0,1)$. We use these images of $\{(1,0,0,0),(0,1,0,0),(0,0,1,0),(0,0,0,1)\}$ under σ_1 as the rows of the matrix M_{σ_1} for σ_1. Therefore,

$$M_{\sigma_1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Similarly, we let σ_2 be the element of A_2 analogous to σ in A, and obtain the matrix M_{σ_2} for σ_2:

$$M_{\sigma_2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Also $(x_1, x_2, x_3, x_4)^{\tau} = (x_3, x_4, x_1, x_2)$; this fact follows from the way in which τ interchanges the positions of the tetrahedra T_1 and T_2. Thus the matrix M_{τ} for the action of τ is

$$M_{\tau} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

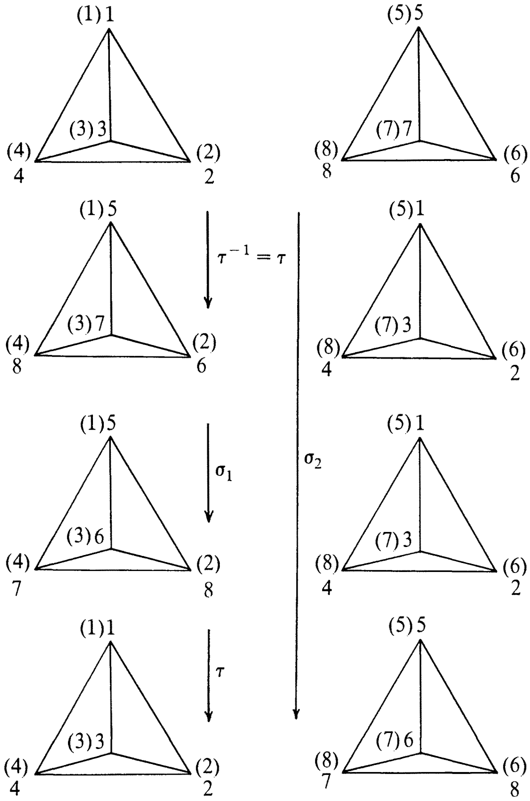

FIGURE 3

These matrices facilitate computation. For instance, the matrix for σ_1^{-1} equals $(M_{\sigma_1})^{-1}$, the inverse of the matrix for σ_1, and the matrix of a product is the product of the matrices: $M_{\sigma_1\sigma_2^{-1}} = (M_{\sigma_1})(M_{\sigma_2^{-1}}) = M_{\sigma_1}(M_{\sigma_2})^{-1}$. The facts we need about individual automorphisms could be verified geometrically, but instead we simply note that such use of matrices to study automorphisms of certain groups is a common technique of considerable power. See [**1**, 1.3.2, 2.6.1] for more detail.

Now we can define G and ϕ. First let $\alpha = \sigma_1\sigma_2^{-1}$ and let $\phi = \sigma_1\sigma_2\tau$. Define G as $(V_1 \times V_2)\langle\alpha\rangle$. G is a subgroup of U since $V_1 \times V_2$ is normal in U. Since G is of order $16 \cdot 3$, $V_1 \times V_2$ is a Sylow 2-subgroup of G and $\langle\alpha\rangle$ is a Sylow 3-subgroup of G. If G were nilpotent, then α would commute with each element v of $V_1 \times V_2$ for the following reason. The nilpotence of G would imply that $V_1 \times V_2$ and $\langle\alpha\rangle$ were normal in G. Thus for v in $V_1 \times V_2$, $(v^{-1}\alpha^{-1}v)\alpha = v^{-1}(\alpha^{-1}v\alpha)$ is in both $V_1 \times V_2$ and $\langle\alpha\rangle$. But the orders of these subgroups are relatively prime, so their intersection is the identity. Thus $v^{-1}\alpha^{-1}v\alpha$ is the identity, and $v\alpha = \alpha v$ as claimed.

If α did commute with each element of $V_1 \times V_2$, then conjugation by α would produce the trivial automorphism of $V_1 \times V_2$, so M_α would be the 4×4 identity matrix. But $\alpha = \sigma_1\sigma_2^{-1}$ implies $M_\alpha = M_{\sigma_1}(M_{\sigma_2})^{-1}$, which is

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

so G is not nilpotent.

Our first step in establishing that the automorphism $\phi = \sigma_1\sigma_2\tau$ fixes only the identity element of $G = (V_1 \times V_2)\langle\alpha\rangle$ is to show that if an element $v\alpha^i$ of G is fixed by ϕ, then α^i is trivial and therefore v in $V_1 \times V_2$ is fixed by ϕ. To do this, we note that $\sigma_1^\tau = \sigma_2$, for σ_2 does to the tetrahedron on S_2 just what σ_1 does to the tetrahedron on S_1. (See FIGURE 3.) Therefore, $\sigma_2^\tau = (\sigma_1^\tau)^\tau = \sigma_1$. Since σ_1 and σ_2 commute, $\alpha^\phi = (\sigma_1\sigma_2^{-1})^{\sigma_1\sigma_2\tau} = \sigma_1^\tau(\sigma_2^{-1})^\tau = \sigma_2\sigma_1^{-1} = \alpha^{-1}$. Thus if α^i is in $\langle\alpha\rangle$, $(\alpha^i)^\phi = \alpha^{-i}$.

Now suppose that g is an element of $G = (V_1 \times V_2)\langle\alpha\rangle$ fixed by ϕ, so $g = v\alpha^i$ and $g^\phi = g$. Then $v\alpha^i = (v\alpha^i)^\phi = v^\phi(\alpha^i)^\phi = v^\phi\alpha^{-i}$, so $v^{-1}v^\phi = \alpha^{2i}$. Since $V_1 \times V_2$ and $\langle\alpha\rangle$ have trivial intersection, $\alpha^{2i} = 1$ and $v^\phi = v$. Since α is of order 3, $\alpha^{2i} = 1$ implies $\alpha^i = \alpha^{4i} = 1$, so $g = v$, a fixed point for ϕ in $V_1 \times V_2$.

Now we show that ϕ has order 6, and show that if ϕ fixes v in $V_1 \times V_2$ then $v = (0,0,0,0)$. Note that $\phi^2 = (\sigma_1\sigma_2\tau)^2 = \sigma_1\sigma_2\tau\sigma_1\sigma_2\tau = \sigma_1\sigma_2(\sigma_1\sigma_2)^\tau$; but $(\sigma_1\sigma_2)^\tau = \sigma_2\sigma_1$, and σ_1 commutes with σ_2, so $\phi^2 = \sigma_1^2\sigma_2^2$. Therefore, $\phi^3 = \sigma_1^2\sigma_2^2\sigma_1\sigma_2\tau = \tau$, which has order 2. Hence ϕ is of order 6.

If ϕ fixes v in $V_1 \times V_2$, then surely ϕ^4 also fixes v. From the previous calculations, we have $\phi^4 = (\sigma_1^2\sigma_2^2)^2 = \sigma_1^4\sigma_2^4 = \sigma_1\sigma_2$, so $M_{\phi^4} = M_{\sigma_1\sigma_2} = M_{\sigma_1}M_{\sigma_2}$, which is

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Let $v = (x_1, x_2, x_3, x_4)$, so $vM_{\phi^4} = v$ implies

$$(x_1, x_2, x_3, x_4)\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} = (x_1, x_2, x_3, x_4),$$

where all entries are elements of F_2, the field of 2 elements. Clearly the only solution to this equation is $(0,0,0,0)$. Hence ϕ^4, and also ϕ, is a fixed-point-free automorphism of $V_1 \times V_2$, so ϕ is a fixed-point-free automorphism of G as claimed.

The proof that our counterexample is minimal with respect to the order of G is, unfortunately, too technical to allow its presentation here. The central idea is to use induction to determine as much as possible the *form* of a minimal counterexample, then investigate small groups of the appropriate form to see which is the one sought. Specifically, a candidate G must be of the form $G = WS$, where W is a normal subgroup of G that is the direct product of k copies of Z_r (a cyclic group of prime order r), while S is a Sylow s-subgroup of G for some prime s other than r. Note that in the actual minimal counterexample, $W = V_1 \times V_2$, $r = 2$, $k = 4$, $S = \langle \sigma \rangle$, and $s = 3$.

This description of the form of a minimal counterexample reminds us that minimality can be defined in a variety of ways. For instance, we might try to determine the pair G_1, ϕ_1 such that the number n of prime factors of the order of G_1, counting multiplicities, is minimal. In the counterexample minimizing the order of G, $n = 5$, since $48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3$. However, the smallest possible value for n is actually 3; there exists a nonnilpotent group G_1 of order $75 = 5 \cdot 5 \cdot 3$ having a fixed-point-free automorphism ϕ_1 of order 4.

One of the main areas of interest in groups having fixed-point-free automorphisms is the analysis of the situation in which the group and the automorphism are of relatively prime order [**1**, Chapter 10]. Thus it is interesting to note that G_1 is also the nonnilpotent group of smallest order having a fixed-point-free automorphism of relatively prime order. Hence G_1, ϕ_1 provides a counterexample minimal with respect to two different criteria. An enterprising reader might wish to refer to MacHale's article [**2**] and examine more of his examples with respect to various definitions of minimality.

References

[1] D. Gorenstein, Finite Groups, Harper and Row, New York, 1968.

[2] D. MacHale, Minimum counterexamples in group theory, this MAGAZINE, 54 (1981) 23–28.

[3] New York Times, April 24, 1959, p. 29.

[4] J. Thompson, Finite groups with fixed-point-free automorphisms of prime order, Proc. Acad. Sci., 45 (1959) 578–581.

Design of an Oscillating Sprinkler

BART BRADEN
Northern Kentucky University
Highland Heights, KY 41076

The common oscillating lawn sprinkler has a hollow curved sprinkler arm, with a row of holes on top, which rocks slowly back and forth around a horizontal axis. Water issues from the holes in a family of streams, forming a curtain of water that sweeps back and forth to cover an approximately rectangular region of lawn. Can such a sprinkler be designed to spread water uniformly on a level lawn?

We break the analysis into three parts:

1. How should the sprinkler arm be curved so that streams issuing from evenly spaced holes along the curved arm will be evenly spaced when they strike the ground?
2. How should the rocking motion of the sprinkler arm be controlled so that each stream will deposit water uniformly along its path?
3. How can the power of the water passing through the sprinkler be used to drive the sprinkler arm in the desired motion?

The first two questions provide interesting applications of elementary differential equations. The third, an excursion into mechanical engineering, leads to an interesting family of plane curves which we've called curves of constant diameter. A serendipitous bonus is the surprisingly simple classification of these curves.