APPLICATIONS OF GROUPS AND ISOMORPHIC GROUPS TO TOPICS IN THE STANDARD CURRICULUM, GRADES 9–11: PART II

Many relationships between groups and topics of secondary school mathematics are shown by the author, who proposes that the study of groups be included as standard fare in the mathematics curriculum of the average college-bound student.

By **ZALMAN USISKIN**

The University of Chicago
Chicago, Illinois

IT IS possible to form a set in an infinite additive group by beginning with any nonzero real a and adding it to itself over and over again, then including zero and the opposites of all numbers in the set. We call such a set the set of integral multiples of a. If $a = 3$, then here is such a set.

$$\{0, 3, -3, 6, -6, 9, -9, \cdots\}$$

With addition, this set forms a group, the group of *integral multiples* of 3.

In Part I of this article, the set of integral powers of 2 was seen to form a group with multiplication. This set can be thought of as beginning with 2, multiplying 2 by itself over and over again, then including 1 and the reciprocals of the numbers in the set. Thus the sets of integral powers and integral multiples are formed by analogous means, with the only differences being the number begun with (the *generator*) and the operation used. This hints at the existence of isomorphic groups. Listing a possible correspondence between the sets shows that this is the case.

⟨set of integral multiples of 3, +⟩	⟨set of integral powers of 2, ·⟩
0	1
3	2
−3	.5
6	4
−6	.25
9	8
−9	.125
⋮	⋮

Part I of this article, which appeared in the February issue of the MATHEMATICS TEACHER, contains applications of groups to sentence solving, systems, and real- and complex-number operations. Definitions and examples of groups and isomorphic groups are given there.

The reader is requested to add any two numbers in the left column, multiply the corresponding numbers in the right column, and check that the answers correspond, thus verifying the isomorphism. The reader should also *subtract* one number from another in the left column, *divide* the corresponding numbers in the right column, and again check that the answers correspond.

This particular example of isomorphic groups involving multiples and powers is very good for giving the idea of what is meant by an isomorphism, but the specific numbers can disguise the applications. It is easier to work in general terms.

Application 8: Isomorphic groups of multiples and powers can be used to help students understand fundamental properties of powers.

We begin by examining the additive group of multiples. Let us suppose that the group is generated by the number a. Then an element of the set of multiples will be of the form ma, where m is an integer. Then:

1. Closure of multiples is indicated by the distributive property, $ma + na = (m + n)a$.
2. The identity multiple occurs when m is 0, $0a = 0$.
3. Inverse multiples are of the form ma and $(-m)a$.

Most students are familiar with these three properties (even if not the present context) before they have worked much with powers. But now let us consider the corresponding properties for the multiplicative group of powers. If the group is generated by x, where $x \neq 1$ and $x \neq 0$, then an element of the set of powers will be of the form x^m, where m is an integer. Since the two groups are isomorphic, for each property of multiples there will be a corresponding property of powers.

1. Closure of powers is indicated by the power property: $x^m \cdot x^n = x^{m+n}$.
2. The identity power occurs when m is 0: $x^0 = 1$.
3. Inverse powers are of the form x^m and x^{-m}.

For most students, properties of powers seem unrelated to properties of multiples. But, in fact, *every* property of multiples has a corresponding property of powers.

4. The multiple of a multiple is a multiple:

$$n(ma) = (nm)a$$

5. The multiple of a sum is the sum of the multiples:

$$m(a + b) = ma + mb$$

4. The power of a power is a power:

$$(x^m)^n = x^{mn}$$

5. The power of a product is the product of the powers:

$$(xy)^m = x^m y^m$$

This approach to properties of powers can help the student realize that properties of powers are naturally connected with multiplication and that any connections of powers and addition are tenuous. (Thus $(x + y)^2 = x^2 + y^2$ is unreasonable.) If a student thinks that zero or negative powers are unnatural, he should be reminded that they are no more unnatural than zero or negative multiples. Advanced students can be shown that property 2 can be proved from property 1 using corresponding proofs.

Given: $ma + na = (m + n)a$ $\qquad x^m \cdot x^n = x^{m+n}$.

Let $m = 0$, $n = 1$. Then:

$$0a + 1a = (0 + 1)a \qquad x^0 \cdot x^1 = x^{0+1}$$
$$0a + 1a = 1a \qquad x^0 \cdot x^1 = x^1$$

Since in a group the identity is unique, $0a$ must be the additive identity and x^0 the multiplicative identity.

The correspondences can be used to generate new properties of powers. Let us consider our next property.

6. The multiple of a difference is the difference of the multiples.

What property of powers would correspond? *Answer:* The power of a quotient is the quotient of the powers. That is, $m(a - b) = ma - mb$ corresponds to

$$\left(\frac{x}{y}\right)^m = \frac{x^m}{y^m}.$$

A student can use this idea to check properties of powers by examining what would be the corresponding property of multiples. Also, the correspondences give meaning to zero and negative integral exponents. Even more is possible.

Application 9: Isomorphic groups of multiples and powers can be used to help students understand fractional powers.

Students should be taught that fractional powers are no more unnatural than fractional multiples. For instance, $\frac{1}{2}a$ results from solving an equation involving multiples ($2b = a$) in the same manner that $x^{1/2}$ results from solving an equation involving powers ($y^2 = x$). But in order to maintain the one-to-one correspondence necessary in an isomorphism, we must require that the group of rational powers have a positive generator and only positive elements. Thus, we now restrict x to be positive, and $x^{1/2}$ stands only for the positive square root of x.

Here are some corresponding properties of rational multiples and rational powers:

1. $\frac{1}{2}a$ is the number that, when added to itself, gives a.

1. $x^{1/2}$ is the number that, when multiplied by itself, gives x.

2. Half of a sum is the sum of the halves:

$$\frac{1}{2}(a + b) = \frac{1}{2}a + \frac{1}{2}b.$$

(Each is the arithmetic mean of a and b.)

2. The square root of a product is the product of the square roots:

$$(xy)^{1/2} = x^{1/2}y^{1/2},$$

or $\sqrt{xy} = \sqrt{x} \cdot \sqrt{y}$.

(Each is the geometric mean of x and y.)

3. $$\underbrace{\frac{1}{n}a + \cdots + \frac{1}{n}a}_{n \text{ terms}} = \frac{n}{n}a = a.$$

3. $$\underbrace{x^{1/n} \cdot \cdots \cdot x^{1/n}}_{n \text{ factors}} = x^{n/n} = x.$$

4. $$\frac{m}{n}a = m\left(\frac{1}{n}a\right) = \frac{1}{n}(ma).$$

4. $$x^{m/n} = (x^{1/n})^m = (x^m)^{1/n},$$

or $x^{m/n} = (\sqrt[n]{x})^m = \sqrt[n]{x^m}$.

The properties given in (4) demonstrate how notations can disguise relationships between properties.

There are more than seventy such corresponding properties. Many of these are given in a different paper devoted to this idea (Usiskin, 1974). Here we give only one further pair of properties.

5. If p is between m and n, then pa is between ma and na.	5. If p is between m and n, then x^p is between x^m and x^n.

We might find a decimal approximation to $3\sqrt{2}$ by noting that this number is between 3(1.41) and 3(1.42). Similarly, $5^{\sqrt{2}}$ lies between $5^{1.41}$ and $5^{1.42}$. Thus the above properties allow irrational multiples and powers to be interpreted. These are necessary for the next application.

Application 10: Logarithms can be developed through a consideration of isomorphic groups of real numbers.

It is usually easier to work in a group of multiples than in a group of powers because addition is easier than multiplication. The largest possible isomorphic groups of real multiples and powers are these:

the additive group of real multiples of a, $a \neq 0$	the multiplicative group of real powers of x, $x > 0$, $x \neq 1$

Subgroups of these have been studied in this article: The additive group of *integral* multiples of a and the multiplicative group of *integral* powers of x in application 8, and the corresponding groups involving *rational* multiples and powers in application 9. Actually, the names for these largest groups can be misleading. Since any real number is a real multiple of any other nonzero real and any positive real is a real power of any non-"one" positive real, the groups may be renamed as the following:

the additive group of reals	the multiplicative group of positive reals

What does isomorphism between these two groups mean? It means that if a and b from the additive group correspond to x and y from the multiplicative group, then the following correspond:

	Add reals	*Multiply positive reals*
1.	$a + b$	xy
2.	$-b$	$\frac{1}{y}$
3.	$a + -b = a - b$	$x \cdot \frac{1}{y} = \frac{x}{y}$
4.	na	x^n

In words, addition corresponds to multiplication, opposites to reciprocals, subtraction to division, and multiples to powers. Furthermore, the identities correspond.

5.	0	1

This is the only correspondence involving two known numbers that always holds. If one knew how to make the other elements in the groups correspond, then any multiplication could be converted to an addition problem, any calculation of reciprocals to a calculation of opposites, and so on. This is the fundamental idea behind logarithms. The numbers at the left will be the logarithms of the corresponding numbers at the right. Correspondences involving other numbers are determined by what corresponds to 1. Here we let B correspond to 1 and call B the *base* of the correspondence:

Logarithm	*Number*
1	B

Notice that B can be any positive number but 1. (If $B = 1$, the correspondence is not one to one.) Because multiples correspond to powers, we obtain the following:

	$1 + 1 = 2$	$B \cdot B = B^2$
6.	n	B^n
	$.5$	$\sqrt{B}$
	$.1$	$\sqrt[10]{B}$

This correspondence $n \rightarrow B^n$ (domain at left) is the exponential function with base B. The inverse correspondence (domain at right) is the logarithm function with base B. We commonly choose $B = 10$ in first meetings with logarithms, although for applications $B = e$ is most natural. When $B = 10$,

m	is the logarithm of	10^m
1		10
2		100
-1		.1
-2		.01
.		.
.		.
.		.

The advantage of 10 is well known. If the logarithm of a number in decimal notation is known, then others can be derived from it. Suppose

.3010	is the logarithm of	2.

Then multiplication at right corresponds to addition at left, and any number with scientific notation involving 2 has a logarithm whose decimal part is .3010. For example:

$.3010 + m$	is the logarithm of	$2 \cdot 10^m$
$.3010 - 4$	is the logarithm of	.0002

The approach using groups has the advantage that all properties of logarithms are known before one begins. In particular, properties 1 through 6 can be rewritten in the symbolism of the log function. That is, if $\log x = a$ and $\log y = b$, then (1) $\log xy = a + b = \log x + \log y$, (2) $\log 1/y = -b = -\log y$, (3) $\log x/y = a - b = \log x - \log y$, (4) $\log x^n = na = n \log x$, (5) $\log 1 = 0$ regardless of which base is used, and (6) $\log_B B^n = n$.

In short, a logarithm function is an isomorphism mapping the multiplicative group of positive reals onto the additive group of reals.

Groups and the Fundamental Concepts of Elementary Euclidean Geometry

Since the famous speech of Felix Klein in 1872 known as the *Erlanger Programm,* it has been known that some geometries—including projective, hyperbolic, elliptic, Euclidean, and others—can be associated with, and classified by, the groups of transformations that preserve properties studied in the particular geometry. Here we concentrate on Euclidean geometry and the content normally found in schools.

There are three fundamental concepts in elementary geometry that are important to mathematicians and that are easily related to the study of groups. They are distance, which is intimately associated with congruence; ratios of distances, likewise associated with similarity; and symmetry.

Application 11: The congruence group clarifies the nature of the equivalence relation properties of congruence.

Euclid's notion of congruence in the plane was very general in that it could be applied to any type of figure. As given in Heath's translation, "things which coincide with one another are equal to one another" (Heath 1956, pp. 224–28). In the language of congruence, "two figures are congruent if they can be made to coincide." In filling the mathematical gaps of Euclid, Hilbert chose to restrict congruence to segments, angles, and triangles, those figures most studied in elementary geometry (Heath 1956, pp. 228–30). In the United States (but not in many other countries), Hilbert's ideas on congruence were adopted by the School Mathematics Study Group (SMSG) and adapted in many other modernizations of geometry. The use of transformations to define congruence is gaining popularity because this use enables one to fill in Euclid's gaps and yet still keep a general definition of congruence. In transformation language, two figures α and β are congruent, $\alpha \cong \beta$, if and only if there is an isometry (distance-preserving transformation) T with $T(\alpha) = \beta$. This mathematizes Euclid's idea by using reflections, rotations, translations, and glide reflections (these being the only possible isometries) for the physical ideas of superposition and coinciding.

Almost immediately, in virtually every development of congruence, one has a need for the equivalence relation properties of congruence:

1. For each figure α, $\alpha \cong \alpha$.
2. If $\alpha \cong \beta$, then $\beta \cong \alpha$.
3. If $\alpha \cong \beta$ and $\beta \cong \gamma$, then $\alpha \cong \gamma$.

In terms of the general definition of congruence, these properties require the following:

1. There is an isometry I so that for each figure α, $I(\alpha) = \alpha$.
2. If there is an isometry T with $T(\alpha) = \beta$, then there is an isometry T' with $T'(\beta) = \alpha$.
3. If T_1 and T_2 are isometries with $T_1(\alpha) = \beta$ and $T_2(\beta) = \gamma$, then there is an isometry T_3 with $T_3(\alpha) = \gamma$.

Now we look at these properties from the point of view of group properties and composition of transformations. The properties are equivalent to the following:

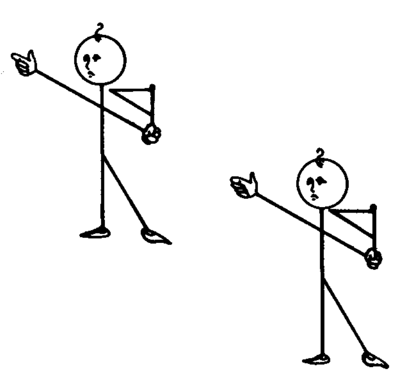
1. The set of isometries contains the identity under composition. (I is the identity.)
2. The set of isometries contains an inverse for each of its elements. (T' is the inverse of T.)
3. The set of isometries is closed under composition. ($T_3 = T_2 \circ T_1$.)

Since composition is always associative, we see that the equivalence relation properties of congruence are logically equivalent to the statement that the set of isometries with composition forms is a group. This group is naturally known as the *congruence group*.

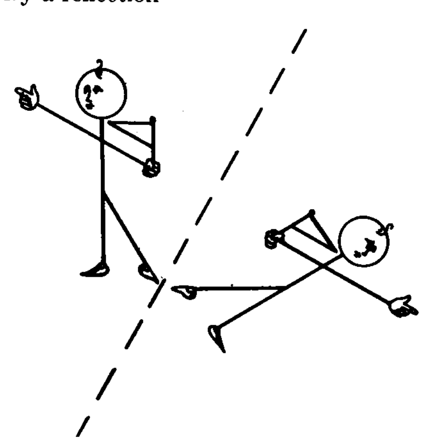
Application 12: The group of similarity transformations with composition clarifies the nature of the equivalence relation properties of similarity.

Among the nice features of transformation definitions for congruence and similarity are the analogies that arise in the treatment of the two concepts. This is seen first in a general definition of similarity using transformations. (Such a general definition is not found in Euclid.) Two figures α and β are similar, $\alpha \sim \beta$, if and only if there is a similarity transformation T (composite of size transformations and isometries) with $T(\alpha) = \beta$. From the definition, one can deduce (a formal treatment may be found in Dodge [1972, pp. 104–13]) that if figures are similar, then they are positionally related to each other in such a way that one can be mapped onto the other in exactly one of four ways:

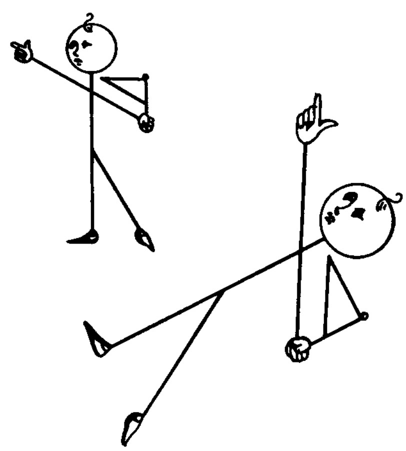
1. By a translation



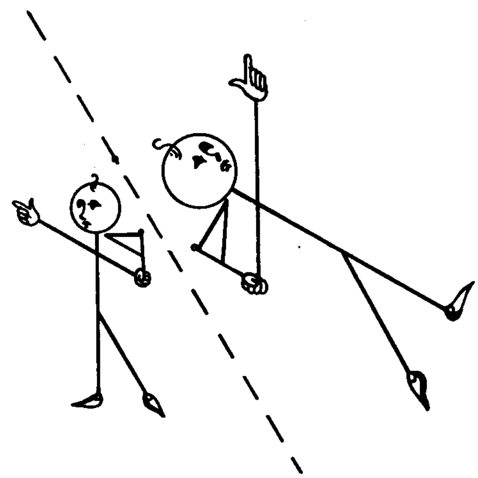
2. By a reflection



3. By a spiral similarity



4. By a **reflective similarity** (a composite of a size transformation and a reflection over a line that contains the center of the size transformation)



The first two of these ways always yield congruent figures. Ways 3 or 4 are needed when the figures are similar and sometimes when the given figures are congruent.

The set of similarity transformations consists of all the transformations of these four types. That this set forms a group with composition is logically equivalent to the statement that similarity is an equivalence relation. The equivalence relation properties imply that one will always obtain similar figures by successive applications of these transformations—never can a figure obtained by this method not be similar to all others so obtained. Thus we can talk about classes of similar figures without worrying about exceptional cases.

Application 13: Symmetry groups of figures can be used to deduce information about the figures.

Associated with every figure is the set of all isometries (reflections, rotations, translations, or glide reflections that map that figure onto itself). This set is the *symmetry set* of the figure. With composition, this symmetry set always forms a group, the *symmetry group* of that figure. Figure 1 shows that most rectangles, rhombuses, and ellipses have the same or isomorphic symmetry groups, each with symmetry sets containing four elements. (Squares and circles have larger symmetry sets.) The reader should draw in the appropriate rhombus.

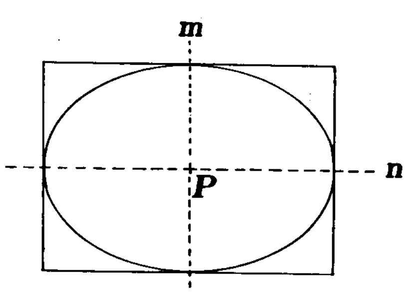


Fig. 1. Isometries in symmetry set: reflection over line *m*, reflection over line *n*, rotation of 180° about *P*, and identity.

The more symmetry a figure has, the more one should expect to find segments of equal length and angles of equal measure. In fact, this is the way students may look at figures before they prove segments and angles equal. For example, if a student does not see that the base angles of an isosceles triangle are congruent *because of the symmetry of the figure,* then any proof would be a waste of time. A student ought to see that in a circle, arcs with the same measure have chords of the same length because of the symmetry of the figure—one chord could be rotated into the other. By the same reasoning, any two diagonals of a regular pentagon are congruent (Fig. 2).

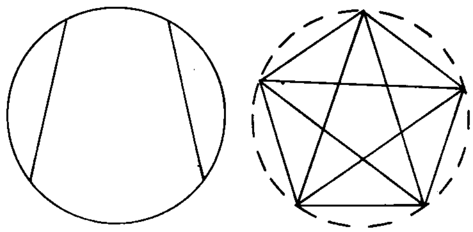


Fig. 2

It may be that symmetry is as aesthetically pleasing a topic as can be studied in mathematics. (See, for example, Weyl [1952] and Locher [1971].) But these are applications outside of geometry. Many statements about functions can be interpreted as indicating symmetry in their graphs. For instance:

$\sin(-x) = -\sin x$ $f(-x) = -f(x)$	indicates	rotation symmetry about the origin
$\cos(-x) = \cos x$ $f(-x) = f(x)$	indicates	reflection symmetry to the y-axis
$\tan(x + \pi) = \tan x$ periodicity in a function	indicates	translation symmetry

Conversely, if one has a graph that is known to possess symmetry, one can make statements about the corresponding function or relation.

Groups and Trigonometric Functions

The graphs of each of the common trigonometric functions possess much symmetry, and these symmetries can be used to deduce relationships about the functions, or conversely, as mentioned immediately above.

Here we give a totally different type of application of groups and isomorphism, an application that relates elementary geometry, transformations, matrices, and trigonometry.

Application 14: The formulas for $\cos(x + y)$ and $\sin(x + y)$ are consequences of the isomorphism between multiplication of certain matrices and composition of rotations.

Just as the standard definitions of congruence and similarity serve to disguise any connection with groups, so also do the standard definitions for the trigonometric functions, either in terms of triangles or in terms of a wrapping or winding function. A more useful and perhaps simpler definition follows: When the point (1, 0) is rotated a magnitude x about the origin, its image lies on the unit circle. Call the image ($\cos x$, $\sin x$).

From this definition, using only basic geometric properties of rotations, it is possible to show that the image of any point (a, b) under a rotation of magnitude x, center $(0, 0)$, is the point (a', b'), where

$$\begin{bmatrix} a' \\ b' \end{bmatrix} = \begin{bmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{bmatrix} \cdot \begin{bmatrix} a \\ b \end{bmatrix}.$$

That is, $\begin{bmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{bmatrix}$ is a matrix for this rotation.

When a matrix stands for a transformation in this way, multiplication of the matrices corresponds to composition of the transformations. If a set of transformations forms a group with composition, then the corresponding set of matrices will form a multiplicative group.

In this case, it is well known that the set of rotations with center (0, 0) with composition forms a group. Specifically, composition is always associative, the identity is the rotation of 0°, the inverse of a rotation of magnitude x is a rotation of magnitude $-x$, and the composite of two rotations with magnitudes x and y is a rotation of magnitude $x + y$.

It is the last of these group properties that is most important for the problem at hand. The composite of a rotation of 50° and a rotation of 75° is a rotation of 125°. (The rotations used here have center at (0, 0).) In general terms, if R_x stands for a rotation of magnitude x,

$$R_x \circ R_y = R_{x+y}.$$

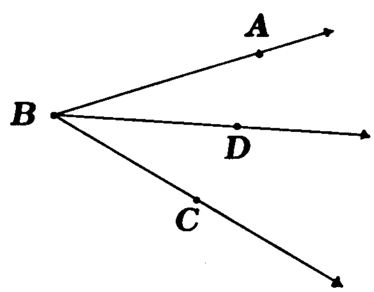
But a corresponding matrix identity is due to the isomorphism:

$$\begin{bmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{bmatrix} \cdot \begin{bmatrix} \cos y & -\sin y \\ \sin y & \cos y \end{bmatrix} = \begin{bmatrix} \cos (x+y) & -\sin (x+y) \\ \sin (x+y) & \cos (x+y) \end{bmatrix}$$

Multiplying the matrices at left yields the familiar formulas for $\cos(x + y)$ and $\sin(x + y)$, two times each.

$$\begin{bmatrix} \cos x \cdot \cos y - \sin x \cdot \sin y & -\cos x \cdot \sin y - \sin x \cdot \cos y \\ \sin x \cdot \cos y + \cos x \cdot \sin y & -\sin x \cdot \sin y + \cos x \cdot \cos y \end{bmatrix}$$
$$= \begin{bmatrix} \cos (x+y) & -\sin (x+y) \\ \sin (x+y) & \cos (x+y) \end{bmatrix}$$

The significance of all this is that these long formulas for $\cos(x + y)$ and $\sin(x + y)$ result immediately from one of the group properties of rotations written in matrix language. This group property of rotations may either be assumed in elementary geometry or deduced from the familiar angle addition postulate (fig. 3).



$$m\angle ABC = m\angle ABD + m\angle DBC$$

Fig. 3

Thus the formulas for $\cos(x + y)$ and $\sin(x + y)$ can be interpreted as "angle-addition" written in matrix language.

A second group property can be applied to deduce formulas for $\cos(-x)$ and $\sin(-x)$. Because of the isomorphism between the composition of the rotations and the multiplication of their matrices, inverse rotations have inverse matrices. Thus R_x and R_{-x} have inverse matrices:

inverse of matrix for R_x = matrix for R_{-x}

$$\text{inverse of} \begin{bmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{bmatrix} = \begin{bmatrix} \cos(-x) & -\sin(-x) \\ \sin(-x) & \cos(-x) \end{bmatrix}$$

Specificially calculating the inverse again twice gives the desired identities. Thus:

$$\begin{bmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{bmatrix} = \begin{bmatrix} \cos(-x) & -\sin(-x) \\ \sin(-x) & \cos(-x) \end{bmatrix}$$

One may proceed from these basic identities to deduce many others.

Summary

There are a large number of applications of ideas about groups to standard topics in the high school mathematics curriculum. Some have been given in the two parts of this article. Applications to equation solving, systems, congruence, similarity, and symmetry make use of little more than the defining properties of groups. Applications to properties of powers and multiples, exponents and logarithms, real- and complex-number operations, and trigonometry make heavy use of isomorphic groups.

The applications using isomorphic groups repeatedly exhibit the truism that what looks hard in one language may be easy in another. The languages of transformations and matrices were occasionally used to provide the simpler alternate languages.

Finally, in choosing the content for this article, a distinction was made between *examples* of groups involving high school content and *applications* of groups to that content. It would not be sufficient to advocate groups for the curriculum merely because there are many instances of groups using objects and operations known to average high school students. Thus examples have not been given except in the context of an application. But the large number of applications of groups to aid understanding of standard topics—with respect both to concepts and to skills—seems to indicate that the study and uses of groups deserve a significant role in the average high school student's encounters with mathematics.

REFERENCES

Dodge, Clayton. *Euclidean Geometry and Transformations*. Reading, Mass.: Addison-Wesley Publishing Co., 1972.

Heath, T. L. *Euclid's Elements*. 2d ed. vol. 1. New York: Dover Publications, 1956.

Locher, J. L., ed. *The World of M. C. Escher*. New York: Harry N. Abrams, 1971.

Usiskin, Zalman. "Some Corresponding Properties of Real Numbers and Implications for Teaching." *Educational Studies in Mathematics*, 5 (1974): 279–90.

Weyl, Hermann. *Symmetry*. Princeton, N.J.: Princeton University Press, 1952.

RECREATION: EIGHT-MARKER PUZZLE

By RAYMOND E. SPAULDING

Radford College
Radford, Virginia

THE eight-marker puzzle is a variation of the ancient game of checkers, but it is played on just one row of squares. Playing the game helps students develop problem-solving ability and gaming strategy analysis.

Instructions

Draw a row of nine squares. Make eight markers, four of them red and four blue. Place the markers on the squares as shown in figure 1, leaving the middle square empty. (R indicates a red marker, B a blue one.)

R	R	R	R		B	B	B	B

Fig. 1

☞