MATHEMATICS MAGAZINE

CONTENTS

VOLUME 42 • MAY 1969 • NUMBER 3

MM

MATHEMATICS MAGAZINE

STEPHEN A. JENNINGS, *EDITOR*

EDITORIAL CORRESPONDENCE should be sent to the EDITOR, S. A. JENNINGS, Department of Mathematics, University of Victoria, Victoria, British Columbia, Canada. Articles should be typewritten and double-spaced on $8\frac{1}{2}$ by 11 paper. The greatest possible care should be taken in preparing the manuscript, and authors should keep a complete copy. Figures should be drawn on separate sheets in India ink and of a suitable size for photographing.

NOTICE OF CHANGE OF ADDRESS and other subscription correspondence should be sent to the Executive Director, A. B. WILLCOX, Mathematical Association of America, Suite 310, 1225 Connecticut Avenue, N. W., Washington, D. C. 20036.

ADVERTISING CORRESPONDENCE should be addressed to RAOUL HAILPERN, Mathematical Association of America, SUNY at Buffalo (University of Buffalo), Buffalo, New York 14214.

The MATHEMATICS MAGAZINE is published by the Mathematical Association of America at Washington, D. C., bi-monthly except July–August. Ordinary subscriptions are: 1 year $4.00 Members of the Mathematical Association of America and of Mu Alpha Theta may subscribe at the special rate of 2 years for $6.00. Single copies are 80¢.

Second class postage paid at Washington, D. C. and additional mailing offices.

PROBABILITY THEORY AND THE LEBESGUE INTEGRAL

TRUMAN BOTTS, Conference Board of the Mathematical Sciences

1. Random phenomena. Probability theory is the study of mathematical models for random phenomena. A random phenomenon is an empirical phenomenon whose observation under given circumstances leads to various different outcomes. When a coin is tossed, either heads or tails comes up; but on a given toss we can't predict which. When a die is tossed, one of the six numbered faces comes up; but again we can't predict which. In such simple random phenomena the various possible outcomes appear to occur with what is called "statistical regularity". This means that the relative frequencies of occurrence of the various possible outcomes appear to approach definite limiting values as the number of independent trials of the phenomenon increases indefinitely.

If we are trying to set up an abstract mathematical model for a random phenomenon, one of the features of the model should surely be a set E whose elements correspond to the various possible outcomes of this random phenomenon. For the case of tossing a coin this basic set might be the two-element set

$$E = \{H, T\}.$$

For the toss of a die it might be the six-element set

$$E = \{1, 2, 3, 4, 5, 6\}. \tag{1.1}$$

In the case of tossing a die we might also be interested in other "events", for instance, the event that an odd number comes up, or the event that the number which comes up is greater than 2, etc. We see that such events correspond, in our mathematical model, to *subsets* of the basic set E. In tossing a die, the event that an odd number comes up corresponds to the subset

$$\{1, 3, 5\}$$

of the set (1.1). The event that the number which comes up is greater than 2 corresponds to the subset

$$\{3, 4, 5, 6\},$$

and so forth.

The basic set E is not always finite. For instance, consider the random phenomenon of repeatedly tossing a coin until the first time heads comes up. Here the basic set E might be taken to be

$$E = \{H, TH, TTH, TTTH, \cdots\},$$

or we might simply take E to be the set

$$E = \{1, 2, 3, \cdots\}$$

of natural numbers, each natural number n corresponding to the outcome that n tosses are required.

Sometimes the basic set is not even countable. For example, consider the random phenomenon of spinning a pointer on a dial and, when it comes to rest, measuring—in radians, say—the angle θ it makes with some reference direction. Here it would be natural to take the basic set in our mathematical model to be

$$E = \{\theta\colon 0 \leqq \theta < 2\pi\} = [0, 2\pi).$$

This is well known to be an *uncountably* infinite set.

2. Probability. Let us return to the simple example of tossing a coin. We said that in repeated tosses of a coin the relative frequency of heads (i.e., the number of times heads comes up divided by the number of tosses) appears to approach some definite limit p as the number of tosses increases indefinitely. We assign this number to the element H of the basic set $E=\{H, T\}$ and call it the *probability* of the outcome heads. When we choose $p=(\frac{1}{2})$, we say our mathematical model is for the random phenomenon of tossing a *fair* coin. When we choose $p\neq(\frac{1}{2})$, we say our model corresponds to tossing a *biased* coin. In any case, though, we choose $0 \leqq p \leqq 1$ (for otherwise p could not be a limit of relative frequencies). Since the relative frequencies of heads and tails always have sum 1, we see that we would then wish to assign to T, representing the outcome tails, a probability q such that $p+q=1$.

In general, for a random phenomenon with n outcomes we would use a basic set

$$E = \{x_1, \cdots, x_n\}$$

of n elements, assigning to each element x_i a probability p_i such that $0 \leqq p_i \leqq 1$ and

$$p_1 + \cdots + p_n = 1.$$

And when the basic set E has a countable infinity of elements $x_1, x_2, \cdots, x_n, \cdots$, we assign to each x_i a probability p_i such that $0 \leqq p_i \leqq 1$ and

$$p_1 + p_2 + \cdots + p_n + \cdots = 1$$

in the sense of the sum of an infinite series.

Whenever E has a countable (i.e., finite or countably infinite) number of elements x_i ,with respective probabilities p_i, we can assign to every *event*, i.e., to every subset A of E, a probability

$$P(A) = \sum_{x_i \in A} p_i.$$

That is, to get the probability of event A, we just add up the probabilities assigned to the various points of A. It is not hard to show that the resulting function P, defined on the class of all events (i.e., all subsets of E), has the following properties.

(2.1)
(1) For every event A, $0 \leqq P(A)$ (i.e., P is *nonnegative*).
(2) $P(E)=1$.
(3) If $A_1, A_2, \cdots$ is a sequence, finite or infinite, of mutually exclusive events, then $P(A_1 \cup A_2 \cup \cdots) = P(A_1) + P(A_2) + \cdots$ (i.e., P is *countably additive*).

The development of probability theory has shown that properties (2.1) are just the ones we need for a probability function in general.

3. The uncountably infinite case. Now how do we assign probabilities to events when the basic set E is uncountably infinite? Let us return to the example of spinning a pointer on a dial, where $E=[0, 2\pi)$. Here, thinking of the case of a "fair" pointer, it is natural to begin by assigning to each interval I in this set a probability proportional to its length:

$$P(I) = \frac{\text{length of } I}{2\pi}. \tag{3.1}$$

Then

$$P(E) = \frac{2\pi}{2\pi} = 1.$$

But this only takes care of the *intervals* in E. What about *any* given subset A of E? It is natural to wish to consider the probability that the angle at which the pointer comes to rest will lie in such a set A. So the question now is: can we extend the domain of P to the class of *all* subsets of $E=[0, 2\pi)$, and in such a way that the essential requirements (2.1) for a probability function are satisfied? This is a very hard question, and unpleasantly enough, the answer turns out to be "No!" At least this is what can be proved if we permit the use of certain rather fancy tools of mathematical proof, called the axiom of choice and the continuum hypothesis. (If we *don't* permit use of the continuum hypothesis, the answer is as yet unknown!)

Our question becomes less difficult if we require in addition that the function P be "translation-invariant". This means that we require $P(A)=P(B)$ whenever the subsets A and B of $E=[0, 2\pi)$ are "rotations of each other", thought of as sets on the unit circle. This simpler question brings us to our first contact with the theory of measure and integration devised by the French mathematician Henri Lebesgue in the first years of this century. In effect, Lebesgue was able to answer this simpler question "No" without using the continuum hypothesis (though he still had to use the axiom of choice!).

We shall have to accept, then, that we *can't* assign probabilities to *all* the subsets of $E=[0, 2\pi)$, if we require properties (2.1) and (3.1) to hold. Well, what more modest class $\mathcal{S}$ of subsets of E, containing all the intervals of E, could we make do with? It would seem reasonable to require of any such class $\mathcal{S}$ that

(3.2) Whenever A belongs to $\mathcal{S}$, then so does $E-A$.

For our pointer-spinning example this just says that if we can consider the event that the pointer-angle *does* land in set A, then we certainly ought to be able to consider the event that it *doesn't*! Thinking of the countable additivity requirement in (2.1), it also seems reasonable to demand that

(3.3) Whenever $A_1, A_2, \cdots$ is a (finite or infinite) sequence of sets belonging to $\mathcal{S}$, then also $A_1 \cup A_2 \cup \cdots$ belongs to $\mathcal{S}$.

Mathematicians have a name (in fact, several names!) for any nonempty class $\mathcal{S}$ of subsets of a set E satisfying conditions (3.2) and (3.3). We call such a class a *σ-field* (or *Borel field* or *σ-algebra*) of subsets of E.

It was Lebesgue's theory of measure and integration that showed that P *could* be extended, so as to satisfy the requirements (2.1) and (3.1) and translation-invariance, from the class of intervals in $E=[0, 2\pi)$ to a σ-field of subsets of E, called the *Lebesgue measurable sets* of E. In the succeeding years this has led to a concept which lies at the foundation of modern probability theory, the concept of a *probability space.* A probability space is a triple $(E, \mathcal{S}, P)$ consisting of a set E (of "outcomes"), a σ-field $\mathcal{S}$ of subsets of E (the "events"), and a function P defined on $\mathcal{S}$ and having properties (2.1) (a "probability function"). We shall return to this concept after we have discussed certain ideas of integration, to which we now turn.

4. The Riemann integral. The integral of elementary calculus is sometimes called the *Riemann integral,* after the 19th century German mathematician who gave this integral a careful formulation. In order to compare it with the Lebesgue integral, let us recall briefly how it is defined.

If f is a bounded real-valued function on some interval $[a, b]$, then f is of course bounded, above and below, on every subset E of $[a, b]$. It follows from a basic property of the real numbers that f then has a *least upper bound*

$$\operatorname*{lub}_{x\in E} f(x)$$

on E and a *greatest lower bound*

$$\operatorname*{glb}_{x\in E} f(x)$$

on E. Corresponding to any partition λ of $[a, b]$ into pairwise-disjoint intervals $I_1, \cdots, I_n$, we may form—denoting the length of an interval I by $L(I)$—an "upper sum"

$$S(f;\lambda) = \sum_{k=1}^{n} (\operatorname*{lub}_{x\in I_k} f(x))\cdot L(I_k)$$

and a "lower sum"

$$s(f;\lambda) = \sum_{k=1}^{n} (\operatorname*{glb}_{x\in I_k} f(x))\cdot L(I_k).$$

It is easy to argue that as λ ranges over all such partitions of $[a, b]$ these upper sums form a collection of numbers having a lower bound and hence a greatest lower bound, which we define to be the *upper Riemann integral*

$$\operatorname*{glb}_{\lambda} S(f;\lambda) = \mathcal{R}\overline{\int_a^b} f(x)dx$$

of f over $[a, b]$. Similarly the lower sums form a collection having an upper bound and hence a least upper bound, which we define to be the *lower Riemann integral*

$$\operatorname*{lub}_{\lambda} s(f;\lambda) = \mathcal{R}\underline{\int_a^b} f(x)dx$$

of f over $[a, b]$. It is not hard to show that

$$\mathcal{R}\underline{\int_a^b} f(x)dx \leqq \mathcal{R}\overline{\int_a^b} f(x)dx.$$

When equality holds, we say that f is *Riemann-integrable* over $[a, b]$ and call this common value the *Riemann integral*

$$\mathcal{R}\int_a^b f(x)dx$$

of f over $[a, b]$. (Here the "R" for Riemann is just part of the integration sign.)

5. The Lebesgue integral. The Lebesgue integral of a bounded function f over $[a, b]$ may be defined in precisely the same manner as the Riemann integral, the only difference being that partitions of $[a, b]$ into intervals are replaced by partitions of $[a, b]$ into Lebesgue measurable sets.

Just as in the case of the particular interval $[0, 2\pi)$ already discussed earlier, Lebesgue's theory yields a σ-field of subsets of $[a, b]$ containing all subintervals of $[a, b]$ and called the *Lebesgue measurable sets* of $[a, b]$. This theory also yields a function L on this σ-field called *Lebesgue measure.* Like the probability function P already discussed, L is nonnegative and countably additive (and translation-invariant); and where P reduces to *relative length* for subintervals, L reduces to *actual length*; that is, for each subinterval I of $[a, b]$, $L(I) =$ length of I.

Now, corresponding to any partition μ of $[a, b]$ into pairwise-disjoint Lebesgue measurable sets $E_1, \cdots, E_n$, we form an upper sum

$$S(f;\mu) = \sum_{k=1}^{n} (\operatorname*{lub}_{x\in E_k} f(x))\cdot L(E_k)$$

and a lower sum

$$s(f;\mu) = \sum_{k=1}^{n} (\operatorname*{glb}_{x\in E_k} f(x))\cdot L(E_k).$$

As before, it is easy to argue that as μ ranges over all such partitions of $[a, b]$, these upper sums form a collection of numbers having a greatest lower bound, which we define to be the *upper Lebesgue integral* of f over $[a, b]$:

$$\operatorname*{glb}_{\mu} S(f;\mu) = \mathcal{L}\overline{\int_a^b} f(x)dx.$$

Analogously we define the *lower Lebesgue integral* of f over $[a, b]$ to be

$$\operatorname*{lub}_{\mu} s(f;\mu) = \mathcal{L}\underline{\int_a^b} f(x)dx.$$

As in the case of the Riemann integral, we have $\mathcal{L}\underline{\int_a^b} f(x)dx \leqq \mathcal{L}\overline{\int_a^b} f(x)dx$. When equality holds we say that f is *Lebesgue integrable* over $[a, b]$ and that this common value is the *Lebesgue integral*

$$\mathcal{L}\int_a^b f(x)dx$$

of f over $[a, b]$.

One thing we can notice at once. Since every partition of $[a, b]$ into intervals is also a partition of $[a, b]$ into Lebesgue measurable sets, we see that

$$\mathcal{R}\underline{\int_a^b} f(x)dx \leqq \mathcal{L}\underline{\int_a^b} f(x)dx \leqq \mathcal{L}\overline{\int_a^b} f(x)dx \leqq \mathcal{R}\overline{\int_a^b} f(x)dx.$$

It follows that whenever f is Riemann integrable over $[a, b]$, then f is also Lebesgue integrable over $[a, b]$, and $\mathcal{R}\int_a^b f(x)\,dx = \mathcal{L}\int_a^b f(x)\,dx$. Very simple examples show, though, that there are bounded functions f which are Lebesgue integrable over $[a, b]$ but not Riemann integrable over $[a, b]$. Thus the first advantage of the Lebesgue integral over the Riemann one is that it integrates more functions.

6. The Lebesgue integral in probability theory. The Lebesgue integral can be extended in a natural way to unbounded functions on unbounded domains. We shall indicate briefly how this extension of the Lebesgue integral is accomplished for the case of *nonnegative* functions only. These are of especial interest in probability theory.

First, there are Lebesgue measurable sets for the entire real line. These form a σ-field containing all the finite intervals. On this σ-field there is defined a Lebesgue measure. It has the properties that might be expected: that is, it is nonnegative, it is countably additive, it reduces to length for finite intervals, and it is translation-invariant. In fact, for every finite interval $[a, b]$ it reduces to the Lebesgue measure on the Lebesgue measurable subsets of $[a, b]$ already discussed above. (But of course it is no longer everywhere finite: it is easily seen that it *couldn't* be, since it reduces to length for intervals and is countably additive!) A not-necessarily-bounded function f on the real line is called *measurable* if for every real number c the set $\{x:f(x)\leqq c\}$ is a Lebesgue measurable set.

When a measurable function f on the real line is nonnegative, we define its *Lebesgue integral*

$$\mathcal{L}\int_{-\infty}^{\infty} f(x)dx \tag{6.1}$$

(finite or infinite) over the whole real line to be the least upper bound of integrals $\mathcal{L}\int_a^b h(x)\,dx$ as $[a, b]$ ranges over all finite intervals and h ranges over all bounded Lebesgue integrable functions on $[a, b]$ for which $h(x)\leqq f(x)$ on $[a, b]$. When the integral (6.1) is finite, we say f is *Lebesgue integrable* over the real line.

We are now in position to indicate briefly a place in probability theory where the Lebesgue integral is a natural tool, but where the Riemann integral is inadequate. There are numerical-valued random phenomena for which it is natural to take the set of outcomes to be the real line, and the events to be the sets of a

σ-field $\mathcal{S}$ containing all the intervals and consisting entirely of Lebesgue measurable sets. To assign a probability to each of these events we can sometimes use a so-called *probability density function* f, that is, a nonnegative function whose integral over the whole real line exists and is 1: $\int_{-\infty}^{\infty} f(x)\,dx = 1$. (One very important such function is the so-called *normal* density function $f(x) = (1/\sqrt{2\pi})e^{-x^2/2}$.)

Using such a density function f we may try to define the probability $P(E)$ for each set E in the σ-field $\mathcal{S}$ by setting

$$P(E) = \int_{-\infty}^{\infty} f(x)K_E(x)dx \equiv \int_E f(x)dx, \tag{6.2}$$

where

$$K_E(x) = \begin{cases} 1 & \text{if } x \in E \\ 0 & \text{if } x \notin E, \end{cases}$$

termed the *characteristic function* (or *indicator function*) of E. It turns out that the sets E for which (6.2) exists as a Lebesgue integral always include all Lebesgue measurable sets and hence all sets of the σ-field $\mathcal{S}$ and that the resulting function P has the desired properties (2.1). But in general the sets E for which (6.2) exists as an (improper) Riemann integral don't form a σ-field or contain an adequate σ-field, at all.

As an indispensable setting and tool for probability, modern ideas of measure and integration really come into their own in the use of *multi-dimensional* measures and integrals to treat many related or independent random phenomena together. But this is a more complicated story and one we cannot go into here.

Suggestions for Further Reading

On probability as measure theory:

P. R. Halmos, The foundations of probability, Amer. Math. Monthly, 51 (1944) 493–510.

———, Measure Theory, Van Nostrand, Princeton, 1950, especially the "Heuristic Introduction" to Chapter IX.

On elementary modern accounts of the Lebesgue integral:

R. R. Goldberg, Methods of Real Analysis, Blaisdell, New York, 1964.

Edgar Asplund and Lutz Bungart, A first course in integration, Holt, Rinehart and Winston, New York, 1966.

PERFECT SQUARES OF THE FORM $(m^2-1)a_n^2+t$

MURRAY S. KLAMKIN, Scientific Laboratory, Ford Motor Company, Dearborn, Michigan

In Mathematical Note 3165, [1] Hale has shown that the sequence $\{a_n\}$, $n=0, 1, 2, \cdots$, where

$$a_{n+1} = 7a_n + \sqrt{48a_n^2+1}, \qquad a_0 = 0 \tag{1}$$

has the property that $48a_n^2+1$ is always a perfect square. In this note, we generalize the result as well as give an explicit solution for the difference equation (1).

Proceeding in a way essentially similar to Hale, we look for sequences of the type

$$a_{n+1} = ra_n + \sqrt{sa_n^2 + t} \tag{2}$$

such that

$$sa_{n+1}^2 + t \equiv \left\{m(ra_n + \sqrt{sa_n^2 + t}) + \lambda a_n\right\}^2 \tag{3}$$

for all a_n. On substituting (2) into (3), expanding out, and equating like functions of a_n, we obtain the following equations for the constants, r, s, m, and λ:

$$(s - m^2)(r^2 + s) = 2m\lambda r + \lambda^2,\ 2r(s - m^2) = 2m\lambda, \quad \text{and} \quad m^2 - s = 1.$$

The solution to this set of three equations is given by

$$r = \pm m, \quad \lambda = \mp 1, \quad s = m^2 - 1.$$

All we need now is to insure that sa_0^2+t is a perfect square. This is achieved by setting $t=p^2-sa_0^2$. It now follows that the sequence $\{a_n\}$ where

$$a_{n+1} = ma_n + \sqrt{(m^2 - 1)(a_n^2 - a_0^2) + p^2} \tag{4}$$

($n=0, 1, 2, \cdots$, m, p, a_0 arbitrary integers) has the property that $(m^2-1)(a_n^2-a_0^2)+p^2$ is a perfect square for all n. Hale's example corresponds to the special case $m=7$, $p=1$, $a_0=0$.

To obtain an explicit solution of (1), we relate it to Pell's equation. First note that by rationalizing (1), we obtain the symmetric equation $a_{n+1}^2-14a_{n+1}a_n+a_n^2=1$ which can be rewritten as $\sqrt{48a_{n+1}^2+1}=7a_{n+1}-a_n$. Thus (1) can now be expressed as the following equivalent 2nd order linear difference equation:

$$a_{n+1} = 7a_n + (7a_n - a_{n-1}) = 14a_n - a_{n-1}. \tag{5}$$

We now employ the following theorem relating to Pell's equation (see [2], pp. 195–212):

If D is a natural number which is not a perfect square, then the Diophantine equation $x^2=Dy^2+1$ has infinitely many solutions (x_n, y_n). All the solutions with positive x_n, y_n, are obtained from the formula

$$x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n \tag{6}$$

where (x_1, y_1) denotes the fundamental solution and which is $(m, 1)$ for $D=m^2-1$.

From (6), we have for $m=7$

$$x_{n+1} + y_{n+1}\sqrt{48} = (x_n + y_n\sqrt{48})(7 + \sqrt{48})$$

or

$$x_{n+1} = 7x_n + 48y_n, \tag{7}$$

$$y_{n+1} = x_n + 7y_n. \tag{8}$$

Substituting for x_n as given in (8) into (7), we obtain the same difference equation as (5). Consequently, $a_n = y_n$. Expanding out (6), we finally obtain

$$a_n = \sum_{k=1}^{n} \binom{n}{2k-1} 7^{n-2k+1} \cdot 48^{k-1}. \tag{9}$$

Another way of obtaining (9) and which also leads to the solution of (1) and (4) for arbitrary a_0 is to note that (2) and (3) imply (as in the derivation of (5)) that

$$a_{n+1} = 2ma_n - a_{n-1} \tag{10}$$

where $a_1 = ma_0 + p$. Equation (10) is now solved in the standard way. (See [3], Chapter 3.) Since the roots of $x^2 = 2mx - 1$ are $m \pm \sqrt{m^2-1}$, we obtain $a_n = A(m+\sqrt{m^2-1})^n + B(m-\sqrt{m^2-1})^n$. The constants A and B are determined from

$$a_0 = A + B \quad \text{and} \quad ma_0 + p = A(m + \sqrt{m^2 - 1}) + B(m - \sqrt{m^2 - 1}).$$

Finally,

$$a_n = \frac{a_0}{2} \{(m + \sqrt{m^2 - 1})^n + (m - \sqrt{m^2 - 1})^n\}$$
$$+ \frac{p}{2\sqrt{m^2 - 1}} \{(m + \sqrt{m^2 - 1})^n - (m - \sqrt{m^2 - 1})^n\}.$$

Added in proof. An easier way would be to require that equation (2) after being rationalized is symmetric in a_n and a_{n+1}.

References

1. D. S. Hale, Math Note 3165, Math. Gaz., October (1966) 307.
2. Trygve Nagell, Introduction to Number Theory, Almquist and Wiksell, Uppsala, Sweden, 1951.
3. Samuel Goldberg, Introduction to Difference Equations, Wiley, New York, 1961.

A DIFFERENT TECHNIQUE FOR THE EVALUATION OF $\int \sec \theta d\theta$

CLIFTON T. WHYBURN, Louisiana State University, now at Eastern Carolina University

Consider $\int \cos \theta d\theta/(1+\sin \theta) = \int \cos \theta(1-\sin \theta)\, d\theta/(1-\sin^2 \theta) = \int \sec \theta d\theta - \int \sin \theta d\theta/\cos \theta = \int \sec \theta d\theta + \ln \cos \theta + C_1$. But, of course, $\int \cos \theta d\theta/(1+\sin \theta) = \ln(1+\sin \theta) + C_2$, so, equating, we have:

$$\int \sec \theta d\theta = \ln(\sec \theta + \tan \theta) + C_3.$$

A similar technique works for $\int \csc \theta d\theta$.

SOLUTION OF AN EQUATION IN A LINEAR ALGEBRA BY MEANS OF THE MINIMAL POLYNOMIAL

JOHN C. KIEFFER, University of Illinois and F. MAX STEIN, Colorado State University

1. Introduction. If $q(x)$ is a polynomial with complex coefficients, we attempt to determine polynomials $p(x)$ such that

$$q(p(A)) = A, \tag{1}$$

where A is an element (e.g., a matrix) which generates a finite dimensional linear algebra $C[A]$ over the complex number field C. To do this we shall need certain ideas and results from linear algebra; these are presented in Section 2. In succeeding sections the main results of the paper are derived which lead to the principal theorem of the paper. In the final section a corollary is presented which answers the question that originally prompted this study: How can all kth roots of a matrix which are expressible as polynomials in the matrix be determined?

2. Results from linear algebra. Let $C[A]$ denote an algebra generated by an element A over the complex number field C; designate the additive identity and multiplicative identity of $C[A]$ by O and I respectively. Then it is easy to see that

$$C[A] = \{c_0I + c_1A + \cdots + c_nA^n;\ c_i \in C,\ (i = 0, 1, \cdots, n),\ n = 1, 2, \cdots\}.$$

If the dimension of the linear algebra is m, every element $p(A)$ of $C[A]$ is a polynomial in A and can be represented uniquely as a linear combination of the basis elements $\{I, A, A^2, \cdots, A^{m-1}\}$. Namely, since the dimension of the linear algebra is finite, it follows that there is a *unique monic polynomial* $m(x)$ of lowest degree such that $m(A) = 0$. This polynomial of degree m in x,

$$m(x) = x^m + c_{m-1}x^{m-1} + \cdots + c_1x + c_0, \tag{2}$$

is called the *minimal polynomial* of A; it is such that

$$m(A) = A^m + c_{m-1}A^{m-1} + \cdots + c_1A + c_0I = 0. \tag{3}$$

Thus A^m and all higher powers of A are linear combinations of $A^{m-1}, A^{m-2}, \cdots, A, I$. It follows that every element of $C[A]$ is a polynomial in A of degree less than m.

We shall need the following lemmas in our later work.

LEMMA 1. *If $p(x)$ and $r(x)$ are polynomials in x, then*

$$p(A) = r(A) \tag{4}$$

if and only if

$$p(x) \equiv r(x) \bmod m(x), \tag{5}$$

where $m(x)$ is the minimal polynomial of A.

The proof of this lemma is straightforward and is omitted.

Since $m(x)$ is a monic polynomial it can be factored as

$$m(x) = \prod_{i=1}^{s} (x - x_i)^{m_i}, \tag{6}$$

where the x_i are the zeros of $m(x)$ and m_i is the multiplicity of the factor $x-x_i$. Note that $\sum_{i=1}^{s} m_i = m$.

If $D^n\phi(x)$ denotes the nth derivative of the polynomial $\phi(x)$ with respect to the variable x, and if $D^0\phi(x) = \phi(x)$, then the following lemma holds; the proof is not difficult and is therefore omitted.

LEMMA 2. *If $p(x)$ and $q(x)$ are polynomials in x, then*

$$p(x) \equiv q(x) \bmod m(x) \tag{7a}$$

if and only if

$$D^n p(x_i) = D^n q(x_i) \tag{7b}$$

for $n = 0, 1, \cdots, m_i - 1$ and $i = 1, 2, \cdots, s$, where $m(x)$ is the monic polynomial given in (6).

We observe that our problem as stated in the introduction: to find all elements $p(A)$ in $C[A]$ such that

$$q(p(A)) = A, \tag{8}$$

is equivalent to finding all polynomials $p(x)$ of degree less than m such that

$$q(p(x)) \equiv x \bmod m(x). \tag{9}$$

We note that we need be concerned only with solutions of (9) of degree less than m since any solution $p^*(x)$ of (9) of degree greater than or equal to m is congruent modulo $m(x)$ to another solution $p(x)$ of degree less than m, and

$$p^*(x) \equiv p(x) \bmod m(x) \text{ implies that } p^*(A) = p(A) \tag{10}$$

by Lemma 1.

3. Derivation of the principal result. We now consider two sets S and G. Let S be the set of all polynomials $p(A)$ that satisfy (8), and let G be the set of all polynomials in x of the form

$$\prod_{i=1}^{s} (x - w_i)^{m_i}, \tag{11}$$

where

(11a) w_i is any zero of $q(x) - x_i$ if x_i is a simple zero of $m(x)$, and
(11b) w_i is any simple zero of $q(x) - x_i$ if x_i is a multiple zero of $m(x)$.

To arrive at our principal result we shall show that there is a one-to-one correspondence between the elements of the sets S and G. Explicitly, any $p(A)$ in S has a minimal polynomial $g(x)$ in G, and for any $g(x)$ in G there is a unique polynomial $p(A)$ in S whose minimal polynomial is $g(x)$.

If $p(A)$ is an element of S, we shall show that the minimal polynomial $g(x)$ of $p(A)$ is in G; i.e., the minimal polynomial of $p(A)$ is of the form (11) with (11a) and (11b) holding. Since $x-x_i$ divides $p(x)-p(x_i)$, then $m(x)$, the minimal polynomial of A, divides

$$\prod_{i=1}^{s} [p(x) - p(x_i)]^{m_i}, \tag{12}$$

that is,

$$\prod_{i=1}^{s} [p(x) - p(x_i)]^{m_i} \equiv 0 \bmod m(x). \tag{13}$$

But by Lemma 1 we see that (13) implies that

$$\prod_{i=1}^{s} [p(A) - p(x_i)I]^{m_i} = 0. \tag{14}$$

Since $g(x)$ is the minimal polynomial of $p(A)$, then from (14) we have that

$$\prod_{i=1}^{s} [x - p(x_i)]^{m_i} \equiv 0 \bmod g(x), \tag{15}$$

or, equivalently, that $g(x)$ divides $\prod_{i=1}^{s}[x-p(x_i)]^{m_i}$. From (15) we can conclude that

$$\text{degree } g(x) \leqq m. \tag{16}$$

Now A is an element of $C[p(A)]$ since $A=q(p(A))$. Therefore $C[A]$ is a subset of $C[p(A)]$ and hence

$$\text{dimension } C[A] = m \leqq \text{dimension } C[p(A)] = \text{degree } g(x). \tag{17}$$

From (16) and (17) we conclude that

$$\text{degree } g(x) = m; \tag{18}$$

therefore

$$g(x) = \prod_{i=1}^{s} [x - p(x_i)]^{m_i}. \tag{19}$$

By the assumption that $p(A)$ is in S, i.e., that $q(p(A))=A$, we conclude from (9) and the case $n=0$ in Lemma 2 that

$$q(p(x_i)) = x_i, \tag{20}$$

if x_i is any zero of $m(x)$, that is, $p(x_i)=w_i$, where w_i is some zero of $q(x)-x_i$. Therefore, in the particular case when x_i is a simple zero of $m(x)$, we see that (11a) holds.

If x_i is a multiple zero of $m(x)$, then by applying Lemma 2 for the case $n=1$ we conclude that

$$D(q(p(x))) = 1 \quad \text{at} \quad x = x_i. \tag{21}$$

Upon expanding the left side of (21) we get $q'(p(x))p'(x) = 1$ at $x = x_i$, or

$$q'(w_i)p'(x_i) = 1. \tag{22}$$

Now w_i cannot be a multiple zero of $q(x) - x_i$, otherwise the derivative of $q(x) - x_i$, which is $q'(x)$, would be zero at $x = w_i$. Thus in (22) we would have $0 = 1$, an obvious contradiction. Hence w_i is a simple zero of $q(x) - x_i$ when x_i is a multiple zero of $m(x)$, (11b). Therefore, from (19), (20), and (22) and the definition of the set G, $g(x)$ is an element of G.

From the assumption that $p(A)$ is in S, we have that $q(p(A)) = A$, and therefore that

$$p(q(p(A))) = p(A). \tag{23}$$

Then from (23) and Lemma 1 we conclude that

$$p(q(x)) \equiv x \bmod g(x), \tag{24}$$

where $g(x)$ is the minimal polynomial of $p(A)$.

We next wish to show that for any $g(x)$ in G there is a unique polynomial $p(A)$ in S whose minimal polynomial is $g(x)$. To outline our steps we observe first that if $p(A)$ in S has $g(x)$ as its minimal polynomial, then (24) holds. Thus for an arbitrary element $g(x)$ of G we determine that there is a unique polynomial $p(x)$ of degree less than m that satisfies (24). We then show that the corresponding polynomial in A, $p(A)$, is in S and has $g(x)$ as a minimal polynomial. Thus $p(A)$ is the unique element in S whose minimal polynomial is $g(x)$.

We proceed to show that for each polynomial $g(x)$ in G (of the form (11)) there is exactly one polynomial $p(x)$ of degree less than m which is a solution to (24). Applying Lemma 2 to (24) we can get the m equations

$$D^n p(q(x)) = D^n x \quad \text{at} \quad x = w_i, \tag{25}$$

for $n = 0, 1, \cdots, m_i - 1$ and $i = 1, 2, \cdots, s$. Since the polynomial $p(x)$ is supposed to be of degree less than m, it can be considered to have exactly m undetermined coefficients. From (25) we obtain m linear equations in the m unknown coefficients of $p(x)$ from which we obtain a *unique* solution if the determinant of the matrix of coefficients of the unknowns is not zero. From these equations we thus obtain the desired unique polynomial $p(x)$, provided we show that this determinant is not zero.

If the determinant of the matrix of coefficients of the system of equations in (25) were zero, there would be a nontrivial solution to the system of homogeneous equations obtained by replacing the constants on the right side of each equation in (25) by zero. That is, in this case there would be a nonzero polynomial, say $h(x)$, of degree less than m such that

$$D^n h(q(x)) = 0 \quad \text{at} \quad x = w_i, \tag{26}$$

for $n = 0, 1, \cdots, m_i - 1$ and $i = 1, 2, \cdots, s$. For the case $n = 0$ we observe that

$$h(x_i) = 0, \qquad i = 1, 2, \cdots, s, \tag{27}$$

using the fact that $q(w_i)=x_i$ from (11a) and (11b).

For multiple zeros of $m(x)$ (i.e., when $m_i>1$ in (26)) the polynomial $h(q(x))$ must be differentiated m_i-1 times. By repeated application of the chain rule for differentiation we get, after letting $y=q(x)$ for simplicity in notation,

$$(28) \qquad D^n h(y) = h^{(n)}(y)f_n + h^{(n-1)}(y)f_{n-1} + \cdots + h'(y)f_1,$$

where $f_n=(q'(x))^n$. According to (26) the right member of (28) equals zero if we let $x=w_i$, and when $n=1$ we get

$$(29) \qquad h'(x_i)q'(w_i) = 0,$$

since $q(w_i)=x_i$. Also, since $q'(w_i)\neq 0$ for any w_i such that $m_i>1$ from (11b), then $h'(x_i)=0$ in (29). Proceeding then by induction we obtain

$$(30) \qquad h^{(n)}(x_i) = 0, \qquad n = 1, 2, \cdots, m_i - 1,$$

for all i for which $m_i>1$. Thus, from (27) and (30), we can write

$$(31) \qquad h^{(n)}(x_i) = 0, n = 0, 1, \cdots, m_i - 1 \quad \text{and} \quad i = 1, 2, \cdots, s;$$

that is, $m(x)=\prod_{i=1}^{s}(x-x_i)^{m_i}$ divides $h(x)$. But this contradicts the fact that $h(x)$ is a nonzero polynomial of degree less than m, since $m(x)$ is of degree m. Hence the determinant of the matrix of coefficients obtained from the equations in (25) is nonzero; this in turn implies that there is a unique solution $p(x)$ of degree less than m to (25) for any $g(x)$ in G.

Next we shall show that $p(A)$ satisfies $q(p(A))=A$, and hence that $p(A)$ is an element of S.

Starting with $p(q(x))\equiv x \bmod g(x)$ from (24) we can write

$$(32) \qquad q(p(q(x))) \equiv q(x) \bmod g(x).$$

Thus $g(x)$ divides $q(p(q(x)))-q(x)$. Hence, $q(p(x))-x$ is a polynomial such that when x is replaced by $q(x)$, the result is divisible by $g(x)$.

Also from (6), (11a), and (11b) we can obtain

$$(33) \qquad m(q(x)) = \prod_{i=1}^{s} (q(x) - x_i))^{m_i} = \prod_{i=1}^{s} (q(x) - q(w_i))^{m_i}.$$

Therefore, since $x-w_i$ divides $q(x)-q(w_i)$, we have that $g(x)=\prod_{i=1}^{s}(x-w_i)^{m_i}$ divides $m(q(x))$. Hence $m(x)$ also has this substitution property.

It is easily verified that the set of all polynomials with this substitution property forms an ideal and so must consist of precisely all of the multiples of the smallest degree polynomial in the set. Thus if it can be shown that no nonzero polynomial of degree less than m has this substitution property, then $m(x)$ must be the smallest degree polynomial in the set. Thus $m(x)$ would divide $q(p(x))-x$, and this would imply that $q(p(A))=A$, as desired.

Now the set of all polynomials modulo $g(x)$ is a linear algebra of dimension m over C. So if there is a nonzero polynomial of degree less than m in this set which has the above substitution property, then the maximum number of independent powers of $q(x)$ modulo $g(x)$ is less than m. The powers of $p(q(x))$ are in the subspace generated by the powers of $q(x)$, and so the maximum number of independent powers of $p(q(x))$ is not greater than the maximum number of independent powers of $q(x)$, and hence is less than m. But each power of $p(q(x))$ is congruent modulo $g(x)$ to the corresponding power of x from (24). Therefore the maximum number of independent powers of x is less than m. But $1, x, \cdots, x^{m-1}$ are m independent powers of x modulo $g(x)$. Therefore we have a contradiction and we conclude that (8) holds, and hence that $p(A)$ is in S.

Finally we show that the minimal polynomial of $p(A)$ is $g(x)$. We know that $p(A)$ has a minimal polynomial, say $g^*(x)$, and we assume that $g^*(x) \neq g(x)$. Now $g^*(x)$ is in G since $p(A)$ is in S, so $g^*(x)$ has the form given by (11). That is

$$g^*(x) = \prod_{i=1}^{s} (x - \overset{*}{w}_i)^{m_i}, \tag{34}$$

where the w_i^* satisfy (11a) and (11b). Also since $g(x)$ is in G, then $g(x)$ has the form

$$g(x) = \prod_{i=1}^{s} (x - w_i)^{m_i}. \tag{35}$$

Since $g^*(x) \neq g(x)$, it must be true that for some i, say $i=k$, $w_k^* \neq w_k$.

Now $p(A)$ is in S, so $p(A)$ satisfies (8). That is,

$$q(p(A)) = A. \tag{36}$$

Then, as in (23),

$$p(q(p(A))) = p(A), \tag{37}$$

and therefore, as in (24),

$$p(q(x)) \equiv x \bmod g^*(x). \tag{38}$$

But we obtained $p(A)$ by solving (24) so that

$$p(q(x)) \equiv x \bmod g(x). \tag{39}$$

Applying Lemma 2 for $n=0$ and $i=k$ we obtain from (38)

$$p(q(\overset{*}{w}_k)) = \overset{*}{w}_k, \tag{40}$$

and from (39)

$$p(q(w_k)) = w_k. \tag{41}$$

But since $g^*(x)$ and $g(x)$ are both in G, we obtain, from (11a) and (11b), that

$$q(\overset{*}{w}_k) = q(w_k) = x_k. \tag{42}$$

Substituting this result into (40) and (41) we obtain a contradiction, namely that $w_k^* = w_k$. Hence, $g^*(x) = g(x)$, and the minimal polynomial of $p(A)$ is $g(x)$.

We now summarize the results of the preceding discussion in the following theorem.

THEOREM. *If*

(a) *$C[A]$ is a linear algebra over the complex number field C generated by A,*

(b) *the linear algebra in* (a) *is of dimension m,*

(c) *the minimal polynomial of A is designated by $m(x)$,*

(d) *$q(x)$ is a fixed polynomial over C,*

(e) *S is the set of all polynomials $p(A)$ that satisfy $q(p(A))=A$, and*

(f) *G is the set of all polynomials in x of the form* (11) *with* (11a) *and* (11b) *holding, then any polynomial $p(A)$ in S has a minimal polynomial $g(x)$ in G, and for any $g(x)$ in G there is a unique polynomial $p(A)$ in S whose minimal polynomial is $g(x)$.*

From the theorem we observe that the two sets S and G are of the same size. Therefore, since G has at most a finite number of elements, there are at most a finite number of solutions of (8).

We should also observe that the set G may be empty. Then there are no solutions to (8).

4. An application to matrices. If the element A is a square matrix of order n, we consider the case for which the polynomial $q(x)=x^k$, k a positive integer greater than one. Then (8) reduces to

$$q(p(A)) = (p(A))^k = A. \tag{43}$$

If (43) has solutions $p(A)$, these solutions will be the kth roots of A that are in $C[A]$. That is, from (43) we will have the kth roots of A expressible as polynomials in A.

For the minimal polynomial of A,

$$m(x) = \prod_{i=1}^{s} (x - x_i)^{m_i}, \tag{44}$$

we form the set G, the set of all polynomials of the form

$$\prod_{i=1}^{s} (x - w_i)^{m_i}, \tag{45}$$

where, from (11a) and (11b) w_i is any zero of $q(x)-x_i=x^k-x_i$, except that w_i cannot be a multiple zero of x^k-x_i when m_i is greater than one.

Now x^k-x_i has k distinct zeros, unless $x_i=0$; in this case there is only one zero (namely zero itself), and that zero is of multiplicity $k\geqq 2$. So if $x_i=0$ is a multiple zero of $m(x)$, there can be no possible w_i, and so G is empty.

On the other hand, if zero is not a multiple zero of $m(x)$, G is not empty; in fact G has k^t members, where t is the number of nonzero distinct zeros of $m(x)$. Thus from $m(x)$ we find k^t members of S, the totality of solutions of (43), by solving

$$p(x^k) \equiv x \bmod g(x) \tag{46}$$

for each $g(x)$ in G. This leads us to the following corollary.

COROLLARY. *If A is a square matrix of order n, and k is an integer such that*

$k\geqq 2$, then the equation $(p(A))^k=A$ has a solution $p(A)$ if and only if the number zero is not a multiple zero of $m(x)$, the minimal polynomial of A.

Prepared in a National Science Foundation Undergraduate Science Education Program in Mathematics at Colorado State University by Mr. Kieffer under the direction of Professor Stein.

REMARKS ON THE FUNCTIONAL EQUATION $f(x+y) = f(x)+f(y)$

EDWIN HEWITT and HERBERT S. ZUCKERMAN, University of Washington

1. Let f be a real-valued function defined on the real line R and satisfying the functional equation

$$f(x + y) = f(x) + f(y). \tag{1}$$

It has been known since Cauchy's time that a continuous solution of (1) has the form $f(x)=Kx$ for a constant K. G. Hamel [**1**] constructed the discontinuous solutions of (1) using (as seems to be necessary) the axiom of choice. He also proved the following

THEOREM. *If f is a solution of* (1) *not of the form $f(x)=Kx$, then the graph of $y=f(x)$ has a point in every neighborhood of every point in the plane $R\times R$.*

It is an obvious consequence of this theorem that if f satisfies (1) and is continuous at some point, or is bounded above or below on some interval, then $f(x)$ has the form Kx.

Hamel's proof of the theorem uses the axiom of choice and also a sophisticated approximation theorem. The use of the axiom of choice can be avoided but the approximation theorem is essential to his argument. We give here a very elementary proof of the theorem.

First let g be any solution of

$$g(x + y) = g(x) + g(y). \tag{2}$$

Since $g(0)=g(0+0)=g(0)+g(0)$, we see that $g(0)=0$. For all positive integers n, we have

$$g(nx) = g(x) + \cdots + g(x) = ng(x).$$

For all positive integers m and nonnegative integers n, we have

$$g\left(\frac{n}{m}x\right) = ng\left(\frac{1}{m}x\right) = \frac{n}{m}\, mg\left(\frac{1}{m}x\right) = \frac{n}{m}g(x).$$

For all $x\in R$, we have $0=g(0)=g(x-x)=g(x)+g(-x)$, so that $g(-x)=-g(x)$. It follows that

$$g(rx) = rg(x) \tag{3}$$

for all $x\in R$ and all rational numbers r.

Now let f be as described in the theorem. It suffices to find, for arbitrary real numbers a, b and positive real ϵ, a real number x_1 such that

$$|x_1 - a| < \epsilon \tag{4}$$

and

$$|f(x_1) - b| < \epsilon. \tag{5}$$

Let g be the function $g(x) = f(x) - f(1)x$. It is plain that g satisfies (2) and that $g(1) = 0$. From (3) we see that

$$g(r) = rg(1) = 0 \tag{6}$$

for all rational r. Since $f(x)$ is not of the form Kx, there is an x_0 such that $f(x_0) \neq f(1)x_0$, and hence $g(x_0) \neq 0$. Therefore we can find a rational number s such that

$$\left| s - \frac{b - af(1)}{g(x_0)} \right| < \frac{\epsilon}{2\,|g(x_0)|}, \tag{7}$$

and then we can find a rational number t such that

$$|t - a + sx_0| < \frac{\epsilon}{1 + 2\,|f(1)|}\,. \tag{8}$$

From (7) we see immediately that

$$|sg(x_0) - b + af(1)| < \frac{\epsilon}{2}, \tag{9}$$

and from (8) that

$$|sx_0 + t - a| < \epsilon \quad \text{and} \quad |sx_0 + t - a| \cdot |f(1)| < \frac{\epsilon}{2}\,. \tag{10}$$

Let $x_1 = sx_0 + t$. Inequality (4) is just part of (10). Applying (2), (3), and (6), we have $g(x_1) = g(sx_0 + t) = sg(x_0) + g(t) = sg(x_0)$; thus (9) can be rewritten as

$$|g(x_1) - b + af(1)| = |sg(x_0) - b + af(1)| < \frac{\epsilon}{2}\,. \tag{11}$$

By our definitions we have

$$g(x_1) = f(x_1) - x_1 f(1) = f(x_1) - (sx_0 + t)f(1),$$

so that (11) can be rewritten as

$$|f(x_1) - b - (sx_0 + t - a)f(1)| < \frac{\epsilon}{2}\,.$$

This inequality, with (10), implies that

$$|f(x_1) - b| < |sx_0 + t - a| \cdot |f(1)| + \frac{\epsilon}{2} < \epsilon,$$

and this is exactly (5).

2. If f is any solution of (1) and $f(a)=0$, it follows from (1) and (3) that $f(x+ra)=f(x)$ for all rational numbers r and real numbers x. That is, f is a periodic function with all numbers ra as periods. In particular, the function g defined by $g(x)=f(x)-f(1)x$ has every rational number as a period.

3. We now take up a functional equation which on the surface appears very different from (1). Let f, g, h be real-valued functions defined on R, and consider the functional equation

$$f(x+y) = g(x) + h(y) \tag{12}$$

We shall find all solutions of (12).

Suppose that f, g, h satisfy (12). Then we have

$$f(x) = f(x+0) = g(x) + h(0), \quad \text{and} \quad f(x) = f(0+x) = g(0) + h(x),$$

so that

$$g(x) = f(x) + a, \qquad h(x) = f(x) + b, \tag{13}$$

where a and b are constants. Substituting (13) in (12), we find $f(x+y)=f(x)+f(y)+a+b$, so that

$$f(x+y) + a + b = (f(x) + a + b) + (f(y) + a + b). \tag{14}$$

The identity (14) means that

$$f(x) = \phi(x) - a - b, \tag{15}$$

where

$$\phi(x+y) = \phi(x) + \phi(y). \tag{16}$$

From (15) and (13), we have

$$g(x) = \phi(x) - b, \qquad h(x) = \phi(x) - a. \tag{17}$$

Conversely, suppose that f, g, h are defined by (15) and (17), where ϕ is any solution of (16) and a and b are arbitrary numbers. Then we have

$$f(x+y) = \phi(x+y) - a - b = \phi(x) - b + \phi(y) - a = g(x) + h(y).$$

That is, f, g, and h satisfy (12).

4. It might appear that functions with the pathological property described in Section 1 cannot exist. They do exist in great profusion, but their construction depends upon the axiom of choice and is decidedly nonelementary. In addition to Hamel's original paper [1], the reader may consult any of a number of textbooks, *e.g.*, [2], p. 49.

References

1. Georg Hamel, Eine Basis aller Zahlen und die unstetigen Lösungen der Funktionalgleichung: $f(x+y)=f(x)+f(y)$, Math. Ann., 60 (1905) 459–462.

2. Edwin Hewitt and K. R. Stromberg, Real and Abstract Analysis, Springer-Verlag, New York and Heidelberg, 1965.

AN EXTENSION OF A MEAN VALUE THEOREM

A. M. RUSSELL, University of Melbourne, Victoria

In [1] Flett proves that if $f(x)$ is a function defined in an interval $[a, b]$, and differentiable in that interval with $f'(a)=f'(b)$, then there exists a point ξ in (a, b) such that

$$\frac{f(\xi)-f(a)}{\xi-a}=f'(\xi).$$

In [2] Lakshminarasimhan extends this result using the Dini-derivatives [3] of $f(x)$. In this note we obtain an extension of the result in [2]. More precisely, we prove the following

THEOREM. *Let $f(x)$, $g(x)$ be defined in $[a, b]$ and suppose that for each function the four Dini-derivatives exist, are finite, and that $f(x)-f(a)$ is of constant sign throughout $[a, b]$. Suppose further that $f(x)$, $g(x)$ have right-hand and left-hand derivatives at a and b respectively with $f'_+(a)\cdot g'_-(b)=f'_-(b)\cdot g'_+(a)$. Then if the Dini-derivatives of $g(x)$ are nonzero, and one is of constant sign throughout (a, b), then there exist $\xi_1, \xi_2, \xi_3, \xi_4, \eta_1, \eta_2, \eta_3, \eta_4$ between a and b such that one of the following cases occurs.*

A. *Either*

$$\frac{f_+(\xi_1)}{g^+(\xi_1)}\leqq\frac{f(\xi_1)-f(a)}{g(\xi_1)-g(a)}\leqq\frac{f^-(\xi_1)}{g_-(\xi_1)}\quad or \tag{1}$$

$$\frac{f_-(\eta_1)}{g^-(\eta_1)}\leqq\frac{f(\eta_1)-f(a)}{g(\eta_1)-g(a)}\leqq\frac{f^+(\eta_1)}{g_+(\eta_1)}. \tag{2}$$

B. *Either*

$$\frac{f_-(\xi_2)}{g_-(\xi_2)}\leqq\frac{f(\xi_2)-f(a)}{g(\xi_2)-g(a)}\leqq\frac{f^+(\xi_2)}{g^+(\xi_2)}\quad or$$

$$\frac{f_+(\eta_2)}{g_+(\eta_2)}\leqq\frac{f(\eta_2)-f(a)}{g(\eta_2)-g(a)}\leqq\frac{f^-(\eta_2)}{g^-(\eta_2)}.$$

C. *Either*

$$\frac{f^-(\xi_3)}{g^-(\xi_3)}\leqq\frac{f(\xi_3)-f(a)}{g(\xi_3)-g(a)}\leqq\frac{f_+(\xi_3)}{g_+(\xi_3)}\quad or$$

$$\frac{f^+(\eta_3)}{g^+(\eta_3)}\leqq\frac{f(\eta_3)-f(a)}{g(\eta_3)-g(a)}\leqq\frac{f_-(\eta_3)}{g_-(\eta_3)}.$$

D. *Either*

$$\frac{f^+(\xi_4)}{g_+(\xi_4)}\leqq\frac{f(\xi_4)-f(a)}{g(\xi_4)-g(a)}\leqq\frac{f_-(\xi_4)}{g^-(\xi_4)}\quad or$$

$$\frac{f^-(\eta_4)}{g_-(\eta_4)}\leqq\frac{f(\eta_4)-f(a)}{g(\eta_4)-g(a)}\leqq\frac{f_+(\eta_4)}{g^+(\eta_4)}.$$

Proof. We first note that $f(x)$, $g(x)$ are continuous functions in $[a, b]$. Since one of the Dini-derivatives of $g(x)$ is nonzero and of constant sign in (a, b), we can assume that $g(x)$ is strictly monotonic. We shall establish Case A in which $f(x)-f(a)$ is nonnegative and $g(x)$ is strictly increasing on $[a, b]$.

We consider the function $p(x)$ defined by

$$p(x) = \frac{f(x) - f(a)}{g(x) - g(a)}, \qquad a < x \leqq b; \qquad p(a) = \frac{f'_+(a)}{g'_+(a)} \cdot$$

The function $p(x)$ so defined is continuous in $[a, b]$.

Furthermore, $p'_-(b) = [g'_-(b)/[g(b)-g(a)]]\ [p(a)-p(b)]$. Since $g(x)$ is strictly monotonic, $g'_-(b)/[g(b)-g(a)]>0$. Consequently if $p(a)<p(b)$, then $p'_-(b)<0$, so that $p(x)$ is a decreasing function of x at $x=b$. Since $p(x)$ is continuous in $[a, b]$ it must therefore attain its maximum at a point ξ_1 between a and b. Hence

$$0 \leqq p^-(\xi_1) \quad \text{and} \quad p_+(\xi_1) \leqq 0. \tag{3}$$

Further, using the nonnegativity of $f(x)-f(a)$ and the monotonicity of $g(x)$, we can show that

$$p^-(\xi_1) \leqq \frac{f^-(\xi_1)}{g(\xi_1) - g(a)} - \frac{f(\xi_1) - f(a)}{g(\xi_1) - g(a)} \cdot \frac{g_-(\xi_1)}{g(\xi_1) - g(a)} \tag{4}$$

and

$$p_+(\xi_1) \geqq \frac{f_+(\xi_1)}{g(\xi_1) - g(a)} - \frac{f(\xi_1) - f(a)}{g(\xi_1) - g(a)} \cdot \frac{g^+(\xi_1)}{g(\xi_1) - g(a)} \cdot \tag{5}$$

Combining (3) and (4) and dividing by $g_-(\xi_1)/[g(\xi_1)-g(a)]$ (which is greater than zero irrespective of whether $g(x)$ is increasing or decreasing) we obtain

$$\frac{f^-(\xi_1)}{g_-(\xi_1)} \geqq \frac{f(\xi_1) - f(a)}{g(\xi_1) - g(a)} \cdot \tag{6}$$

Similarly from (3) and (5) we obtain

$$\frac{f_+(\xi_1)}{g^+(\xi_1)} \leqq \frac{f(\xi_1) - f(a)}{g(\xi_1) - g(a)} \cdot \tag{7}$$

Combining inequalities (6) and (7) gives (1).

If, on the other hand, $p(a)>p(b)$, then $p'_-(b)>0$, so that $p(x)$ is an increasing function of x at $x=b$. Hence $p(x)$ will attain its minimum value at a point η_1 between a and b, in which case

$$p^+(\eta_1) \geqq 0, \qquad p_-(\eta_1) \leqq 0. \tag{8}$$

Furthermore,

$$p^+(\eta_1) \leqq \frac{f^+(\eta_1)}{g(\eta_1) - g(a)} - \frac{f(\eta_1) - f(a)}{g(\eta_1) - g(a)} \cdot \frac{g_+(\eta_1)}{g(\eta_1) - g(a)} \tag{9}$$

and

$$p_-(\eta_1) \geqq \frac{f_-(\eta_1)}{g(\eta_1) - g(a)} - \frac{f(\eta_1) - f(a)}{g(\eta_1) - g(a)} \cdot \frac{g^-(\eta_1)}{g(\eta_1) - g(a)} . \tag{10}$$

Inequalities (2) now follow from (8), (9), and (10).

Finally, when $p(a) = p(b)$, the required inequalities (1), and (2) follow readily by noting the continuity of $p(x)$ in $[a, b]$. This establishes Case A. Case B, which corresponds to $f(x) - f(a)$ being nonpositive and g increasing, can be deduced from Case A by replacing $f(x)$ by $-f(x)$. Similarly, Cases C and D can be deduced from Case A.

When $g(x)$ is differentiable in $[a, b]$, equality holds in (4) and (5), and we can replace $p^-(\xi_1)$ and $p_+(\xi_1)$ by $p_-(\xi_1)$ and $p^+(\xi_1)$, respectively, thus giving stronger inequalities than (1) and (2). In addition, the differentiability of $g(x)$ enables us to remove from $f(x) - f(a)$ the constant-sign restriction required in (4), (5), (9), and (10). Corresponding remarks hold for (9) and (10). Consequently, by putting $g(x) = x$ we then obtain the inequalities of [2].

In conclusion, for the special case when each of $f(x)$ and $g(x)$ is differentiable in $[a, b]$, we observe that an α exists between a and b such that

$$\frac{f(\alpha) - f(a)}{g(\alpha) - g(a)} = \frac{f'(\alpha)}{g'(\alpha)} .$$

References

1. T. M. Flett, A mean-value theorem, Math. Gaz., 42 (1958) 38–39.
2. T. V. Lakshminarasimhan, A mean value theorem—an extension, Amer. Math. Monthly, 73 (1966) 862–863.
3. R. P. Boas, A primer of real functions, Carus Monograph 13, MAA, New York, 1963.

ANOTHER THEOREM RELATING SYLVESTER'S MATRIX AND THE GREATEST COMMON DIVISOR

M. A. LAIDACKER, Lamar State College of Technology

As is well known, a necessary and sufficient condition for two nonconstant polynomials to have a nonconstant greatest common divisor is that the determinant of Sylvester's matrix be zero. However, a greatest common divisor (gcd) of two polynomials can also be derived from Sylvester's matrix as stated in Theorem 3.

It is to be assumed throughout that f and f_1 are polynomials of degrees m and m_1 respectively where $m \geqq m_1 > 0$, and the coefficients of the polynomials are definite constants. In addition, whenever a gcd is mentioned, it is with reference to f and f_1.

A gcd, f_r, can be found by Euclid's algorithm which yields the equations

$$\begin{aligned} f &= f_1 q_1 + f_2 \\ f_1 &= f_2 q_2 + f_3 \\ &\vdots \\ f_{r-2} &= f_{r-1} q_{r-1} + f_r \\ f_{r-1} &= f_r q_r \end{aligned}$$

where f_i is of degree m_i, q_1 is of degree $m-m_1$, q_i is of degree $m_{i-1}-m_i$, $m_{i-1} \geqq m_i+1$, and $i=2, 3, \cdots, r$.

THEOREM 1. *The polynomial f_i can be expressed in the form $g_i f + g_i' f_1$ where g_i and g_i' are polynomials of degrees $m_1 - m_{i-1}$ and $m - m_{i-1}$ respectively.*

Theorem 1 is easily proved using induction on i.

COROLLARY 1.1. *A* gcd *can be represented in the form $g_r f + g_r' f_1$ where g_r and g_r' are polynomials of degrees no greater than $m_1 - 1$ and $m-1$ respectively.*

The proof of Corollary 1.1 follows directly from Theorem 1 and the fact that $m_{i-1} \geqq m_i + 1$.

Recalling that Sylvester's matrix of $f = a_0 x^m + a_1 x^{m-1} + \cdots + a_m$ and $f_1 = b_0 x^{m_1} + b_1 x^{m_1 - 1} + \cdots + b_{m_1}$ is

$$\begin{bmatrix} a_0 & a_1 & \cdots & a_m & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_m & 0 \cdots & 0 \\ & & & \vdots & & & \\ 0 & 0 \cdots & 0 & a_0 & a_1 & \cdots & a_m \\ b_0 & b_1 & \cdots & b_{m_1} & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_{m_1} & 0 \cdots & 0 \\ & & & \vdots & & & \\ 0 & 0 \cdots & 0 & b_0 & b_1 & \cdots & b_{m_1} \end{bmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m_1 \text{ rows} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \text{ rows,} \end{matrix}$$

we prove the following theorem.

THEOREM 2. *If the elements of the ith row of Sylvester's matrix are the coefficients of polynomial p_i and the elements of the ith row of Sylvester's matrix in echelon form are the coefficients of polynomial e_i, then there are no nonzero polynomials of the form $\alpha_1 p_1 + \alpha_2 p_2 + \cdots + \alpha_{m+m_1} p_{m+m_1}$ of degree less than k where k is the degree of the last nonzero polynomial e_p, α_i is a constant for $i=1, 2, \cdots, m+m_1$, and Sylvester's matrix is put in echelon form by row transformation only.*

Proof. Let p_i and e_i be polynomials described by the respective matrices where the entries of the first column are the coefficients of the x^{m+m_1-1} term, the second column are the coefficients of the x^{m+m_1-2} term, etc.

It should be noted that the set of polynomials generated by p_i is the same as the set generated by the polynomials e_i, $i=1, 2, \cdots, m+m_1$.

Suppose the theorem is not true for k greater than zero. Then there are constants β_i, $i=1, 2, \cdots, p$, such that $\beta_1 e_1 + \beta_2 e_2 + \cdots + \beta_p e_p = e$ where e is a nonzero polynomial of degree less than k. Since e_1 has as its first term an x to a power higher than that of e and e_i for $i=2, 3, \cdots, p$, β_1 equals zero.

We now consider the reduced expression $\beta_2 e_2+\beta_3 e_3+\cdots+\beta_p e_p=e$, and by the same reasoning as above find β_2 equals zero. Continuing the process, we find that $\beta_i=0$ for $i=1, 2, \cdots, p$, implying e is a zero polynomial contrary to the supposition.

For k equal to zero, the theorem is trivially true.

THEOREM 3. *The last nonzero row of Sylvester's matrix when put in echelon form, using row transformation only, gives the coefficients of a* gcd.

Proof. Suppose the coefficients of the last nonzero row to be $c_0, c_1, \cdots, c_k$ where c_0 is the first nonzero constant; then $e_p=c_0x^k+c_1x^{k-1}+\cdots+c_k$. From the construction of Sylvester's matrix, any polynomial of the form $\alpha_1 p_1+\alpha_2 p_2+\cdots+\alpha_{m+m_1}p_{m+m_1}$ can be written in the form $g_rf+g_r'f_1$ where g_r and g_r' are polynomials of degrees no greater than m_1-1 and $m-1$ respectively. Obviously e_p can be written in the form $g_rf+g_r'f_1$. That e_p is divisible by a gcd follows immediately. Hence the degree of a gcd must be less than or equal to that of e_p. However, according to Theorem 2, there are no nonzero polynomials of degree less than k expressible in the form $g_rf+g_r'f_1$. Theorem 3 follows.

I wish to thank the referee for his helpful comments.

References

1. S. Borofsky, Elementary Theory of Equations, Macmillan, New York, 1960.
2. C. W. Curtis, Linear Algebra, Allyn and Bacon, Boston, 1963.
3. J. W. Uspensky, Theory of Equations, McGraw-Hill, New York, 1948.

REAL SOLUTIONS OF CLASSES OF POLYNOMIAL EQUATIONS

S. B. JACKSON, University of Maryland
and University of Liverpool

1. Introduction. The purpose of this paper is to determine an upper bound for the number of real and distinct roots for certain classes of polynomial equations with real coefficients. Thus, for the class of all polynomial equations of a given degree n having real coefficients, the Fundamental Theorem of Algebra asserts that there are at most n real and distinct roots. Moreover, this is a best possible result since it is trivial to produce an equation of the given class where the bound is actually attained. If, however, one restricts attention to classes of polynomial equations where certain of the coefficients are required to vanish, a sharper result may be possible. Thus for the class of cubic equations of the form $a_0+a_1x^3=0$, the number of real roots cannot exceed 1 since a real number has only one real cube root.

Consider the class of polynomial equations with real coefficients of the form

$$a_0 + a_1x^{p_1} + a_2x^{p_2} + \cdots + a_nx^{p_n} = 0 \tag{1}$$

where $0<p_1<p_2<\cdots<p_n$ and where not all a_i vanish. Since this class of

polynomials is uniquely determined by the sequence of exponents $\{0, p_1, \cdots, p_n\}$ it will be designated as the class $(0, p_1, \cdots, p_n)$. For this class of polynomial equations, let s denote the number of cases when two consecutive integers in the sequence $\{0, p_1, \cdots, p_n\}$ have the same parity, i.e., are both odd or both even. The principal result to be established is the following theorem.

THEOREM 1. *The number of real and distinct roots of a polynomial equation of class* $(0, p_1, \cdots, p_n)$ *cannot exceed* $n+s$. *Moreover the bound* $n+s$ *is actually attained by a polynomial equation of this class.*

2. Proof of the first half of Theorem 1. It is interesting that this proof requires nothing more complicated than the familiar Descartes Rule of Signs. It is to be shown that $n+s$ is an upper bound to the number of real and distinct roots for all polynomials of the given class. Consider first the special case of a polynomial of the given class $(0, p_1, \cdots, p_n)$ for which *all* a_i are different from zero. Then, in particular, $a_0 \neq 0$ so that $x=0$ is not a root. Thus all real roots are either positive or negative. By Descartes' Rule of Signs, the number of positive roots cannot exceed the number of variations in sign in the sequence $\{a_0, a_1, \cdots, a_n\}$, while the number of negative roots cannot exceed the number of variations in the sequence $\{a_0, (-1)^{p_1}a_1, (-1)^{p_2}a_2, \cdots, (-1)^{p_n}a_n\}$. Let a_k, a_{k+1} be any consecutive terms in the first sequence, whence the corresponding terms in the second sequence are $(-1)^{p_k}a_k$, $(-1)^{p_{k+1}}a_{k+1}$. If p_k and p_{k+1} have opposite parity then exactly one of these two pairs has a variation of sign. Hence, if there are d cases of different parity in the sequence $\{0, p_1, \cdots, p_n\}$ we can count exactly d corresponding variations in sign in the two coefficient sequences. If, on the other hand, p_k and p_{k+1} have the same parity, then the pairs a_k, a_{k+1} and $(-1)^{p_k}a_k$ and $(-1)^{p_{k+1}}a_{k+1}$ either both have a variation in sign or neither does. Hence, corresponding to the s cases of same parity in $\{0, p_1, \cdots, p_n\}$, there are at most $2s$ variations in sign in the two coefficient sequences. The total number of variations is therefore at most $d+2s$ which is thus an upper bound on the number of real roots. Since $d+s=n$ this is the desired upper bound $n+s$. This proves the stated result for the case when $a_i \neq 0$ for *all* i.

Consider next the case of a polynomial of the given class $(0, p_1, \cdots, p_n)$ having $a_0=0$ and let a_k, $k>1$, be the first nonvanishing coefficient. Furthermore, let $a_i \neq 0$ for $i=k, \cdots, n$. Then equation (1) has a root $x=0$ and the remaining roots are those of the equation.

$$a_k + a_{k+1}x^{(p_{k+1}-p_k)} + \cdots + a_nx^{(p_n-p_k)} = 0.$$

Since this is an equation of the type just considered, with n replaced by $n-k$, its number of real distinct roots cannot exceed $(n-k)+s'$ where s' is the number of cases of same parity of consecutive terms in the sequence $\{0, p_{k+1}-p_k, \cdots, p_n-p_k\}$. This is clearly the same as the number of cases of same parity in the sequence $\{p_k, p_{k+1}, \cdots, p_n\}$. Since this latter sequence is a section of $\{0, p_1, \cdots, p_n\}$ it follows at once that $s' \leqq s$. The number of real distinct roots of equation (1) for the case under consideration therefore cannot exceed $1+(n-k)+s'$. Since $k \geqq 1$ and $s' \leqq s$, this latter number cannot exceed $n+s$ which is therefore an upper bound for the number of real distinct roots.

Consider finally the general case of equation (1) where *any* proper subset of the coefficients a_i vanish, and let z be the number of zeros among the coefficients $a_1, a_2, \cdots, a_n$. Equation (1) then has the form

$$(2) \qquad b_0 + b_1x^{r_1} + b_2x^{r_2} + \cdots + b_mx^{r_m} = 0$$

where $b_0 = a_0$, $b_i \neq 0$ for $1 \leqq i \leqq m$, and $m = n - z$, and where each term in (2) is one of the terms in (1). Equation (2) is exactly of the form just considered. Hence the number of real distinct roots of (2), and therefore of (1), cannot exceed $m+s'$ where s' is the number of cases of same parity for consecutive terms of the sequence $\{0, r_1, \cdots, r_m\}$. Note that this latter sequence is, by definition, a subsequence of $\{0, p_1, \cdots, p_n\}$. Consider any case r_k, r_{k+1} of same parity in the sequence $\{0, r_1, \cdots, r_m\}$. Let $r_k = p_u$ and $r_{k+1} = p_{u+t}$. If $t = 1$, then p_u, p_{u+t} are a case of same parity in the sequence $\{0, p_1, \cdots, p_n\}$. If $t > 1$, then $a_{u+1}x^{p_{u+1}}$ was one of the omitted terms, so that $a_{u+1} = 0$. Thus each of the s' cases of same parity in $\{0, r_1, \cdots, r_m\}$ corresponds either to a case of same parity in sequence $\{0, p_1, \cdots, p_n\}$ or to a vanishing coefficient in (1). Since there are s cases of same parity in $\{0, p_1, \cdots, p_n\}$ and z vanishing coefficients in (1), this means that $s' \leqq s + z$. Hence the bound $m + s'$ for the number of distinct real roots of (2) is such that $m+s' \leqq m+s+z = n+s$, where the last equality follows from the fact that $m+z=n$. This completes the proof of the first part of Theorem 1, namely that $n+s$ is always an upper bound to the number of real distinct roots of a polynomial equation of the class $(0, p_1, \cdots, p_n)$.

3. Proof of the second half of Theorem 1. It is to be shown that there exists, in the class $(0, p_1, \cdots, p_n)$, a polynomial equation having $n+s$ real distinct roots. We proceed inductively.

Suppose that coefficients $a_0, a_1, \cdots, a_k$ for $k \leqq n-1$ have been chosen in such a way that the polynomial $P_k(x)$ given by $P_k(x) = a_0 + a_1x^{p_1} + \cdots + a_kx^{p_k}$ has the following properties:

(i) The a_i for $i = 0, \cdots, k$ are nonvanishing and alternate in sign, with $a_0 > 0$.

(ii) There is an increasing sequence $x_0 = 0 < x_1 < \cdots < x_k$ such that, for $0 \leqq i \leqq k$, $P_k(x_i)$ has the sign of a_i while $P_k(-x_i)$ has the sign of $(-1)^{p_i}a_i$.

It is to be shown that a_{k+1} can be chosen such that polynomial $P_{k+1}(x)$ defined by $P_{k+1}(x) = P_k(x) + a_{k+1}x^{p_{k+1}}$ satisfies (i) and (ii) for the case $k+1$. Let a_{k+1} be chosen opposite in sign to a_k and such that $|a_{k+1}x_k^{p_{k+1}}| < \text{Min}_{0 \leqq i \leqq k}[|P_k(x_i)|, |P_k(-x_i)|]$. It follows that, for every $x \in [-x_k, x_k]$, $|a_{k+1}x^{p_{k+1}}| < |P_k(x_i)|$ and $|a_{k+1}x^{p_{k+1}}| < |P_k(-x_i)|$. Since $P_{k+1}(x) = P_k(x) + a_{k+1}x^{p_{k+1}}$, this means that, for each $x_i (i = 0, 1, \cdots, k)$, $P_{k+1}(x_i)$ has the same sign as $P_k(x_i)$ and $P_{k+1}(-x_i)$ has the same sign as $P_k(-x_i)$. Hence, by property (ii) for $P_k(x)$, $P_{k+1}(x_i)$ and $P_{k+1}(-x_i)$ have, respectively, the signs of a_i and $(-1)^{p_i}a_i$ for $0 \leqq i \leqq k$.

Finally, let $x_{k+1} > x_k$ be chosen large enough such that at $x = \pm x_{k+1}$ the polynomial $P_{k+1}(x)$ is dominated by its final term, $a_{k+1}x^{p_{k+1}}$. Since $x_{k+1} > 0$, this means that, for $x = x_{k+1}$, $P_{k+1}(x_{k+1})$ has the sign of a_{k+1} and $P_{k+1}(-x_{k+1})$ has the sign of $(-1)^{p_{k+1}}a_{k+1}$. It is seen at once that polynomial $P_{k+1}(x)$ satisfies conditions (i) and (ii) for the case $k+1$.

Since, if a_0 is any positive number, the polynomial $P_0(x)=a_0$ trivially satisfies (i) and (ii) for the case $k=0$, it follows by induction that a polynomial $P_n(x)$ of class $(0, p_1, \cdots, p_n)$ satisfying (i) and (ii) for the case $k=n$ can be found.

To complete the proof it remains only to show that the polynomial equation $P_n(x)=0$ has $n+s$ real distinct roots. To this end consider the positive interval $[x_k, x_{k+1}]$. Since $P_n(x_k)$ and $P_n(x_{k+1})$ have the signs of a_k and a_{k+1}, respectively, by (ii), and since by (i) these numbers are of opposite sign, it follows that $P_n(x)=0$ has a root interior to the interval $[x_k, x_{k+1}]$. There are n such intervals and hence at least n distinct positive real roots. Consider now the negative interval $[-x_{k+1}, -x_k]$. By (ii) $P_n(-x_{k+1})$ and $P_n(-x_k)$ have the signs of $(-1)^{p_{k+1}}a_{k+1}$ and $(-1)^{p_k}a_k$ respectively. If p_k and p_{k+1} have the same parity these numbers are of opposite sign and there is a root between $-x_{k+1}$ and $-x_k$. Hence each of the s cases of same parity in the sequence $\{0, p_1, \cdots, p_n\}$ corresponds to a negative root, so there are at least s negative roots. Thus $P_n(x)=0$ has at least $n+s$ real distinct roots. Since, by the first part of Theorem 1, this number of roots cannot exceed $n+s$, the number of real distinct roots is exactly $n+s$. This completes the proof of Theorem 1.

4. **An extension.** A slight, but sometimes useful, extension of Theorem 1 can be readily deduced. Consider the class of polynomial equations with real coefficients given by

$$a_0 + a_1x^{p_1} + \cdots + a_nx^{p_n} + a_{n+1}x^{p_{n+1}} + \cdots + a_{n+r}x^{p_{n+r}} = 0 \tag{3}$$

where $0<p_1< \cdots <p_n<p_{n+1}< \cdots <p_{n+r}$ and not all a_i vanish and where, in addition, we require that integers $p_n, \cdots, p_{n+r}$ all have the same parity and that coefficients $a_n, \cdots, a_{n+r}$ all have the same sign. As before, let s be the number of cases of consecutive terms having the same parity in the sequence $\{0, p_1, \cdots, p_n\}$. For convenience, let the class of polynomial equations defined above be called class C. The following theorem can then be established.

THEOREM 2. *The number of real and distinct roots of a polynomial equation of class C cannot exceed $n+s$. Moreover, the bound $n+s$ is actually attained by a polynomial equation of the class, and this polynomial equation can be chosen such that* $a_n=a_{n+1}= \cdots =a_{n+r}$.

The proof will be omitted, since it is a relatively trivial modification of that of Theorem 1. The crux of the matter is that, though (3) allows terms not present in (1), the fact that the last $r+1$ terms all have the same parity for their exponents and the same sign for their coefficients means there is no increase in the possible number of variations and hence no increase in the possible number of real distinct roots.

5. **An application.** As an illustration of these ideas, let us seek to determine the linear order of the plane curve given parametrically by

$$x = t^3, \quad y = t^4 \quad \text{where} \quad -\infty < t < \infty. \tag{4}$$

This means we wish to determine the maximum number of distinct real points in which curve (4) is met by any line. Since the general line has the equation $ax+by+c=0$, the intersections with (4) are given by the solutions of the equation

$$c + at^3 + bt^4 = 0. \tag{5}$$

Within the class of equations given by (5) we wish to find the maximum number of real distinct solutions. The class given by (5) is precisely the class (0, 3, 4) of Theorem 1 with $n=2$. Since the sequence $\{0, 3, 4\}$ of exponents has no case of consecutive members of the same parity, then $s=0$. Thus, by Theorem 1, the maximum number of real and distinct roots is $n+s=2+0=2$, so curve (4) has linear order 2. This is of some interest since the curve is actually one of degree 4, having nonparametric equation $x^4=y^3$.

In a similar way one may seek to determine the cyclic order of curve (4), i.e., the maximum number of real distinct intersections with the general circle (considering lines as special circles). The general circle has the form $a(x^2+y^2)+bx+cy+d=0$. The equation giving the desired intersections this time becomes

$$d + bt^3 + ct^4 + a(t^6 + t^8) = 0. \tag{6}$$

Equations (6) are precisely the set of equations considered in Theorem 2 with $n=3$, $r=1$, and an exponent sequence up to p_n of $\{0, 3, 4, 6\}$ so that $s=1$. By Theorem 2 the cyclic order of curve (4) is therefore precisely $n+s=3+1=4$.

Frequently only an upper bound on order is determined by these theorems. For example, if one seeks the cyclic order of the curve given by

$$x = t^2, \quad y = t^5 \quad \text{where} \quad -\infty < t < \infty, \tag{7}$$

the relevant equation becomes

$$d + bt^2 + at^4 + ct^5 + at^{10} = 0. \tag{8}$$

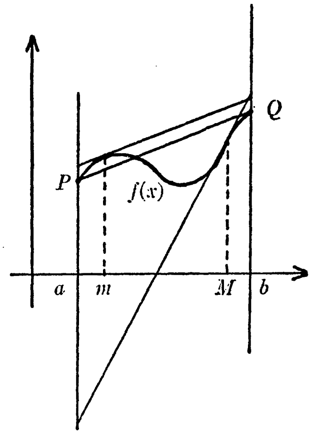
This is an equation of form (1) with $n=4$ and an exponent sequence $\{0, 2, 4, 5, 10\}$ for which $s=2$. Hence, by Theorem 1, the number of intersections is at most $n+s=6$. However, equations (8) are only a subset of the class (0, 2, 4, 5, 10) considered in Theorem 1 since in (8) the coefficients of t^4 and t^{10} must be equal. Whether there is, in this subset, an equation actually having six real distinct roots is not known from the given discussion. Hence it can only be concluded that 6 is an upper bound to the cyclic order of curve (7).

A THEOREM ON ARC LENGTH

JOHN KAUCHER, University of California, Santa Barbara

Many calculus textbooks apply the mean value theorem for integrals to interpret the area under a curve as the area of a related rectangle. The purpose of this note is to interpret the length of arc of a curve as the length of a related line segment.

THEOREM. *If $f'(x)$ is continuous for $a \leqq x \leqq b$ and $t(x)$ is the length of the segment of the tangent line at $(x, f(x))$ intercepted by the lines $x=a$ and $x=b$, then there exists a number w, $a \leqq w \leqq b$, such that $t(w)$ is the length of arc of $f(x)$ between $x=a$ and $x=b$.*



Proof. By the mean value theorem for derivatives, there exists a point m, $a \leqq m \leqq b$, such that $f'(m)=$slope of $\overline{PQ}$. Since the line $x=a$ is parallel to $x=b$, then $t(m)=$length of $\overline{PQ}$. But the length of $\overline{PQ}$ is less than or equal to the length of arc $\widehat{PQ}$. Therefore $t(m) \leqq$length of $\widehat{PQ}$.

Since $f'(x)$ is continuous, it has a maximum value at $x=M$, $a \leqq M \leqq b$. Now

$$t(M) = \sqrt{(b-a)^2 + [f'(M)(b-a)]^2} = (b-a)\sqrt{1+[f'(M)]^2}.$$

But since $f'(M) \geqq f'(x)$,

$$\sqrt{1+[f'(M)]^2} \geqq \sqrt{1+[f'(x)]^2}.$$

Integrating from $x=a$ to $x=b$, we get $t(M) \geqq$length of $\widehat{PQ}$.

Since $f'(x)$ is continuous, $t(x)$ is continuous. We proved that $t(m) \leqq$length of $\widehat{PQ} \leqq t(M)$. By the intermediate value theorem there must exist a number w such that $t(w)=$length of $\widehat{PQ}$.

BIORTHOGONALITY OF CHARACTERISTIC VECTORS

JOHN CHRISTIANO and ALBERT WIGGIN, N.I.U.

A fact known for some time, but for reasons unknown to the authors, the result as stated in Theorem 2 below does not seem to appear in the standard texts in linear algebra or matrices. Applicability of this result to Markoff theory and other areas makes the proof of this theorem both interesting and useful.

The following definitions and theorems are stated for background and completeness.

DEFINITION. *Let* $X=(x_1, x_2, \cdots, x_n)$ and $Y=(y_1, y_2, \cdots, y_n)$ *be vectors in either a Euclidean or unitary space, then the inner product of X and Y is defined as*

$$(X, Y) = \sum_{i=1}^{n} x_i y_i.$$

THEOREM 1. *The inner product has the following properties:*

1. $(X, Y)=(Y, X)$
2. $(\lambda X, Y)=\lambda(X, Y), \lambda \in R$
3. $(X+Z, Y)=(X, Y)+(Z, Y)$
4. $(X, X) \geqq 0$
5. $(X, X)=0 \leftrightarrow X=0$

DEFINITION. *X and Y are orthogonal if* $(X, Y)=0$.

DEFINITION. *The countable set* $\phi=\{R^1, R^2, \cdots, R^m\}$ *of vectors forms an orthogonal family if*

$$(R^j, R^k) = \sum_{i=1}^{n} r_i^j r_i^k = 0 \qquad j \neq k$$

$$(R^j, R^j) = \sum_{i=1}^{n} [r_i^j]^2 \neq 0 \qquad j = 1, 2, \cdots, m.$$

DEFINITION. *Two countable sets of vectors* $\phi_R=\{R^1, R^2, \cdots, R^m\}$ *and* $\phi_L=\{L^1, L^2, \cdots, L^m\}$ *are biorthogonal if* $(R^j, L^k)=0$ $j, k=1, 2, \cdots, m$ *and* $j \neq k$.

DEFINITION. *If* $A=(a_{ij})$ *is an* $n \times n$ *matrix and X is an n-dimensional vector, the vector-matrix right product is*

$$AX = \sum_{j=1}^{n} a_{ij} x_j, \qquad i = 1, 2, \cdots, n.$$

DEFINITION. *The vector-matrix left product is*

$$XA = \sum_{i=1}^{n} a_{ij} x_i, \qquad j = 1, 2, \cdots, n.$$

THEOREM 2. *If* $A=(a_{ij})$ *is an* $n \times n$ *matrix and* $\phi_L=\{L^1, L^2, \cdots, L^k\}$ *is the set of left characteristic vectors and* $\phi_R=\{R^1, R^2, \cdots, R^k\}$ *the set of right characteristic vectors of A corresponding to the distinct characteristic values* $\lambda_1, \lambda_2, \cdots, \lambda_k$, *then* ϕ_R *and* ϕ_L *are biorthogonal.*

To prove this theorem, we first prove the following:

LEMMA 1. *If* $A=(a_{ij})$ *is an* $n \times n$ *matrix, and X and Y are n-dimensional vectors, then* $(AX, Y)=(X, YA)$.

Proof.

$$\begin{aligned}(AX, Y) &= y_1 \sum_{j=1}^{n} a_{1j}x_j + y_2 \sum_{j=1}^{n} a_{2j}x_j + \cdots + y_n \sum_{j=1}^{n} a_{nj}x_j \\ &= x_1 \sum_{i=1}^{n} a_{i1}y_i + x_2 \sum_{i=1}^{n} a_{i2}y_i + \cdots + x_n \sum_{i=1}^{n} a_{in}y_i \\ &= (X, YA).\end{aligned}$$

The proof of Theorem 2 now follows: By definition for left and right characteristic vectors

$$AR^j = \lambda_j R^j \tag{1}$$

and

$$L^i A = \lambda_i L^i. \tag{2}$$

Taking the inner product of (1) with L^i and the inner product of (2) with R^j and subtracting yields

$$(AR^j, L^i) - (R^j, L^i A) = (L^i, \lambda_j R^j) - (R^j, \lambda_i L^i).$$

The left member of this equation is zero by Lemma 1. Applying properties 1 and 2 of Theorem 1 to the right member yields

$$0 = (\lambda_j - \lambda_i)(L^i, R^j).$$

Now $\lambda_j \neq \lambda_i$ for $i \neq j$; hence $(L^i, R^j) = 0$, $i \neq j$. Thus the assertion is proved.

Example. Let

$$A = \begin{bmatrix} 1 & 0 & 4 \\ 5 & 2 & 3 \\ 0 & 0 & 3 \end{bmatrix}.$$

The characteristic values of A are

$$\lambda_1 = 1, \quad \lambda_2 = 2 \quad \text{and} \quad \lambda_3 = 3.$$

The corresponding right vectors are

$$R^1 = (1, -5, 0), \quad R^2 = (0, 1, 0) \quad \text{and} \quad R^3 = (2, 13, 1).$$

The left vectors are

$$L^1 = (1, 0, -2), \quad L^2 = (5, 1, -23), \quad \text{and} \quad L^3 = (0, 0, 1).$$

It is observed that ϕ_R and ϕ_L are biorthogonal. That is, $(R^i, L^j) = 0$, $i \neq j$, $i, j = 1, 2, 3$.

A TRANSFORMATION FOR CLASSES OF GEOMETRIC CONFIGURATIONS

NORMAN R. DILLEY, THOMAS M. GREEN, and CHARLES HAMBERG

Coolidge [1] describes the notion of a geometrical transformation with the following, "First of all, a transformation is looked upon as a means of simplifying a figure, or of deducing the properties of one figure from those of another by expressing them in terms that are invariant under the general relation that connects the two."

In this paper a transformation is introduced which shows the area property of any pair of geometric configurations to exist as a magnification or a dilation invariant over the given class of geometric configurations.

To begin the discussion, one may allow the geometric configuration to be a triangle in the plane. This divides or decomposes into line elements as

$$\begin{aligned} L_1 &\rightarrow a_1x + b_1y = c_1 \\ L_2 &\rightarrow a_2x + b_2y = c_2 \\ L_3 &\rightarrow a_3x + b_3y = c_3 \end{aligned} \tag{1}$$

Any nonempty intersection of three line sets must describe a triangle element in the plane space S_2. Accordingly,

$$\{L_1 \cap L_2 \cap L_3\} \rightarrow \Delta ABC. \tag{2}$$

Next the triangle element, ΔABC, is fixed so that the vertices appear in the plane as (a_1, b_1), (a_2, b_2), and (a_3, b_3).

A vector space is required and is quickly found by noting the two dimensional vector space X_2 that is isomorphic to the plane space S_2. Since the space S_2 contains an origin (0, 0) and points that are the vertices of the ΔABC, one may recognize three vectors which connect the origin to the vertices. Designate these vectors as x_A, x_B, x_C. Now the situation shows a triangle in the plane with vectors connecting the origin (0, 0) to the vertices of the triangle. Stating this more concisely,

$$\begin{aligned} &S_2 \rightarrow X_2 \\ &X_2 \rightarrow \{x_A, x_B, x_C\} \\ &X_2 \cap S_2 = \{(0, 0), (a_1, b_1), (a_2, b_2), (a_3, b_3)\}. \end{aligned} \tag{3}$$

Now the transformation may be applied to the triangle element or ΔABC. The details of the transformation are a cyclic subtraction of the vectors x_A, x_B, x_C, in pairs. The result of each pairwise subtraction is a set of new vectors $\{x_1, x_2, x_3\}$. If the transformation is designated by the symbol β, then

$$\beta(\Delta ABC) \rightarrow \{x_1, x_2, x_3\} \tag{4}$$

where the subtraction is routine for $x_1 = x_A - x_B = (a_2 - a_1), (b_2 - b_1), \cdots$, and $x_3 = x_C - x_A = (a_1 - a_3), (b_1 - b_3)$.

The transformation β decomposes the ΔABC into its three line elements (the sides) and translates them to a new position about the origin (0, 0). What is translated is, of course, the length of each side. In the result of the transformation one notes the new set of vectors $\{x_1, x_2, x_3\}$ designating a new triangle, $\Delta A'B'C'$. Hence,

$$\beta(\Delta ABC) \rightarrow \Delta A'B'C'. \tag{5}$$

Since the first triangle was a closed figure, any system generated remains a static or closed system. Interestingly, the triangle $\Delta A'B'C'$ is oriented so that the origin is the centroid.

At this point one may ask with Coolidge, "What property is invariant over the class of pairs of triangles, ΔABC and $\Delta A'B'C'$?"

To search for the invariant over the transformation one uses the area property of the triangles. Let the area of ΔABC be given as

$$\begin{aligned} |\Delta ABC| &= \tfrac{1}{2}\begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ 1 & 1 & 1 \end{vmatrix} \\ &= \tfrac{1}{2}(a_1b_2 + a_2b_3 + a_3b_1 - a_1b_3 - a_3b_2 - a_2b_1). \end{aligned} \tag{6}$$

Then the area of the second or projected triangle that results from the transformation is

$$\Delta A'B'C' = \tfrac{1}{2}\begin{vmatrix} a_2 - a_1 & a_3 - a_2 & a_1 - a_3 \\ b_2 - b_1 & b_3 - b_2 & b_1 - b_3 \\ 1 & 1 & 1 \end{vmatrix}. \tag{7}$$

After some lengthy algebra, this reduces to

$$\Delta A'B'C' = 3[\tfrac{1}{2}(a_1b_2 + a_2b_3 + a_3b_1 - a_1b_3 - a_1b_3 - a_2b_1)]. \tag{8}$$

The invariant property over the transformation is, therefore, a threefold magnification of the area. Hence

$$\beta(\Delta ABC) \rightarrow |\Delta A'B'C'| = 3|\Delta ABC|. \tag{9}$$

In extending the discussion to another class of polygons, one may investigate a pair of convex quadrilaterals. Here the general quadrilateral is $ABCD$ and a plane figure with vertices $(a_1, b_1), \cdots, (a_4, b_4)$. The vectors which terminate upon the vertices are in the set $\{x_A, \cdots, x_D\}$. The transformation β, a cyclic subtraction of the terminating vectors, produces the set of vectors $\{x_1, x_2, x_3, x_4\}$. This new set of vectors determines the second quadrilateral $A'B'C'D'$.

When the area property of the two quadrilaterals is investigated in the same manner as with the case of the triangles, it is found that there exists a two-fold magnification of the area over the transformation. Hence,

$$|A'B'C'D'| = 2|ABCD|. \tag{10}$$

The transformation β has the invariant property that the projected quadrilateral is increased in area two-fold.

When one investigates further classes of polygons such as the pentagons, hexagons, etc., one notes that the magnification factor for the areas maximizes for the regular polygon of the given class. The following table gives the magnification factor (this is symbolized as α) for the various classes of polygons after the transformation β has taken place.

TABLE OF THE MAGNIFICATION OF AREAS

Polygon Class	Area Magnification Factor
Triangle	$\alpha=3$
Quadrilateral	$\alpha=2$
Pentagon	$\alpha\leqq 1.382$
Hexagon	$\alpha\leqq 1.000$
Heptagon	$\alpha\leqq 0.752$
Octagon	$\alpha\leqq 0.586$
Nonagon	$\alpha\leqq 0.468$
Decagon	$\alpha\leqq 0.382$
n-gon	$\alpha=4\sin^2(180/n)$

The figures in the table were calculated after the general expression for α was found. Here are the steps that led to this general expression:

a. Note that for the regular polygon, under the transformation β, the side of the given polygon becomes the radius of the circumscribing circle about the projected polygon about the origin.

b. The area of the first regular polygon in terms of its side is known to be $A=(n/4)s^2 \cot(180/n)$, where $s=$side, $n=$number of sides.

c. The area of the regular polygon in terms of its circumscribing radius is known to be $A'=(n/2)s^2\sin(360/n)$.

d. $$\alpha = A'/A = \frac{(n/2)s^2\sin(360/n)}{(n/4)s^2\cot(180/n)} = \frac{2\sin(360/n)}{\cot(180/n)}.$$

e. Let $A=180/n$, then

$$\alpha = \frac{2\sin 2A}{\cot A} = 2\sin 2A \tan A$$
$$= 2(2\sin A\cos A\tan A)$$
$$= 4(\sin A\cos A)(\sin A/\cos A)$$
$$= 4\sin^2 A.$$

f. Therefore, $\alpha=4\sin^2(180/n)$.

A remarkable thing about this area magnification factor is that taking limits one notes that

$$\lim_{n\to\infty} 4\sin^2(180/n) = 0$$

which implies that a circle is transformed into nothing, or in other words, under β as a transformation, the circle shrinks to zero. This is true regardless of the size of the circle that one began with before the transformation. The reason for this eludes the authors at this point of their investigation.

It so happens that there is an alternative expression for α. This results because of the identity

$$\alpha = 4 \sin^2 (180/n) = 2 - 2 \cos(360/n).$$

It appears that under β two space transforms to two space. Further investigation for β for three space, four space, etc., lies ahead.

It appears that β must have an inverse for it is certainly possible to decompose a polygon about the origin and send it into the plane. However, it is not an ordinary inverse because there will not be a uniquely situated polygon in the plane for the polygon about the origin. Hence, β^{-1} generates a polygon that must be independent of the axes that contained the polygon about an origin. This polygon, that is reduced in area according to the inverse of the α for the given class of polygons, is a 'stateless' polygon or 'abstract' polygon. One has the polygon, but one does not see where to place it in the plane. The reason that this condition exists is because of the plane space S_2 and the vector space X_2—they are infinitely removed from each other. The plane space S_2 induces an isomorphic vector space X_2, but the vector space X_2 does not induce a plane space S_2 under β^{-1}.

Perhaps there is a more adequate way to discuss β and β^{-1}. The authors would be pleased to see any discussion on the matter.

It is a pleasure to acknowledge that the initial stimulation for the thoughts in this paper were gained at a National Science Foundation Mathematics Institute held at the University of California, Santa Barbara, Calif., in 1964.

Reference

1. J. L. Coolidge, A History of Geometrical Methods, Dover, New York, 1963, p. 293.

ON SHUFFLING CARDS

EDWIN F. WILDE, Beloit College and DANIEL A. TOMANDL, Beloit College student

1. Introduction. Problems suitable for undergraduate research are not numerous, but with the availability of computers many areas deserve re-examination as possible sources. This paper contains the development of a number theoretic example. If an ordered deck of distinguishable cards is shuffled and reshuffled in a prescribed manner, the question may be asked as to whether the cards will return to their original order, and if so, after how many shuffles. The initial investigation for decks with two hundred or fewer cards was completed by a computer and study of the results yielded fruitful conjectures. The result was not only an answer to the original questions, but the development of an algorithm to determine the exponent to which 2 belongs modulo integers of the form $4n+1$ and the solution of an interesting distributional question.

2. Analysis.

DEFINITION 1. *A deck of cards is said to be shuffled if the second card is placed on top of the first, the third below the first two, and the cards continue to be placed alternately above and below the existing pile until no cards remain.*

Let $c_1, c_2, \cdots, c_{2n+1}$ denote a deck of $2n+1$ ordered cards. After one shuffle, the cards are in the order $c_{2n}, \cdots, c_2, c_1, c_3, \cdots, c_{2n+1}$. The cards return to their original order after repeated shuffling iff the first $2n$ cards do. Consequently, the analysis is restricted to decks containing an even number of cards.

DEFINITION 2. *Let $N(i, m, n)$ be the position number of the ith card after m shuffles if there are 2n cards. Let $N(i, 0, n)=i$.*

For example, $N(1, 1, 3)=4$ and $N(1, 2, 3)=2$. The first theorem pertains to the values of $N(i, m, n)$ and pleasantly enough the inelegant form of this natural result does not impede its use.

THEOREM 1. *$N(i, m, n)$ is the unique integer in the following set of 2^m rational numbers: $\{2^{-m}[(2n+1)(2^m+1)-(4n+1)r_i-\frac{1}{2}\pm(i-\frac{1}{2})]$, where $r_i=1, 2, 3, \cdots, 2^{m-1}\}$. The sign is $(-1)^c$ where c is the number of even terms in the set $\{N(i, 1, n), \cdots, N(i, m, n)\}$.*

Proof. The theorem holds for $m=1$; if i is odd, $N(i, 1, n)=(n+1)+(i-1)/2$, while if i is even, $N(i, 1, n)=(n+1)-i/2$. Suppose the theorem is true for $m=k$. If $N(i, k, n)$ is odd, then $N(i, k+1, n)=(n+1)+\frac{1}{2}[N(i, k, n)-1]$ $=N(i, k+1, n)$ where r_i is chosen from the integers $1, 2, 3, \cdots, 2^{k-1}$ and the sign selected is the same as that for $N(i, k, n)$. If $N(i, k, n)$ is even, then $N(i, k+1, n)=(n+1)-\frac{1}{2}N(i, k, n)=N(i, k+1, n)$ where $R_i=2^k-r_i+1$ is chosen from the integers $2^k, 2^k-1, \cdots, 2^{k-1}+1$ and the sign selected is the opposite of that for $N(i, k, n)$.

LEMMA 1. *If $N(i, m_1, n)=N(i, m_2, n)$, where $m_1>m_2$, then (1) $N(i, m_1-m, n)$ $=N(i, m_2-m, n)$ for integer m, $0\leqq m\leqq m_2$, and (2) $N(i, m_1+m', n)=N(i, m_2+m', n)$ for nonnegative integer m'.*

Proof by induction.

LEMMA 2. *There exists an integer x, $0<x\leqq 2n$, such that $N(i, x, n)=i$.*

The proof follows from the Dirichlet pigeonhole principle and Lemma 1.

DEFINITION 3. *Let $m(i, n)$ be the least positive integer, x, such that $N(i, x, n)=i$.*

LEMMA 3. *$N(i, x, n)=i$ iff $x=c\cdot m(i, n)$, where c is a nonnegative integer.*

The proof of necessity follows from Lemma 1 by induction. The proof of sufficiency follows directly from Lemma 1.

THEOREM 2. *$N(i, m(1, n), n)=i$.*

Proof. Since shuffling replaces the first card by the last, $m(1, n)=m(2n, n)$. By Theorem 1 with $m=m(1, n)$ there exists a positive integer r_1, r_{2n}, $1\leqq r_1$, $r_{2n}\leqq 2^{m(1,n)-1}$, and a choice of sign such that

$$(1) \qquad 2^{-m(1,n)}[(2n+1)(2^{m(1,n)}+1)-(4n+1)r_1-\tfrac{1}{2}\pm\tfrac{1}{2}]=1,$$

$$(2) \qquad 2^{-m(1,n)}[(2n+1)(2^{m(1,n)}+1)-(4n+1)r_{2n}-\tfrac{1}{2}\pm(2n-\tfrac{1}{2})]=2n,$$

respectively.

The sign selected in Equation (1) is determined inductively by the position numbers $N(1, m, n)$, where $m=1, 2, \cdots, m(1, n)$. Since $N(1, m-1, n)=N(2n, m, n)$, $m=2, 3, \cdots, m(1, n)+1$ and $N(2n, m(1, n)+1, n)=N(2n, 1, n)$, the signs selected in Equations (1) and (2) are the same.

To prove that the forthcoming selection of r_i is integer valued, it is now shown that $2n-1 \mid r_{2n}-r_1$. Subtraction of Equation (1) from Equation (2) yields $-(4n+1)(r_{2n}-r_1)=(2^{m(1,n)}\mp 1)(2n-1)$. From Equation (1), shown in detail in the next proof, $4n+1 \mid 2^{m(1,n)}\mp 1$. Hence, $2n-1 \mid r_{2n}-r_1$.

Now choose $r_i=r_1+(i-1)(r_{2n}-r_1)/(2n-1)$ and select the same sign as was chosen for Equation (1). Then $N(i, m(1, n), n)=2^{-m(1,n)}[(2n+1)(2^{m(1,n)}+1)-(4n+1)r_i-\frac{1}{2}\pm(i-\frac{1}{2})]=N(1, m(1, n), n)+[(i-1)/(2n-1)]\cdot[N(2n, m(1, n), n)-N(1, m(1, n), n)]=i$.

THEOREM 3. *$m(1, n)$ is the least positive integer, x, such that $4n+1$ divides 2^x+1 or 2^x-1.*

Proof. Theorem 1 with $i=1$, $m=m(1, n)$ and the positive sign chosen implies that $r_1=[2n(2^{m(1,n)}-1)/(4n+1)]+1$. Since $(2n, 4n+1)=1$, r_1 is integer valued iff $4n+1 \mid 2^{m(1,n)}-1$. If the negative sign is chosen, r_1 is integer valued iff $4n+1 \mid 2^{m(1,n)})+1$. To see that $m(1, n)$ is the least positive integer with the desired property, consider the positive integer y, $y\leqq m(1, n)$, and $4n+1 \mid 2^y+1$. Let $r_1'=2n(2^y+1)/(4n+1)$. Since $r_1'\leqq 2^{y-1}$, by Theorem 1, $N(1, y, n)=1$, and by Lemma 3 $y=c\cdot m(1, n)$. But $y\leqq m(1, n)$, so $c=1$. A similar argument may be given if $4n+1 \mid 2^y-1$.

COROLLARY. *$m(1, 2^s)=s+2$ for positive integer s.*

3. Prefatory remarks. Certain number theoretic results and definitions used in the remainder of the paper are now stated. For details see [1]. Euler's generalization of Fermat's Theorem states that $2^{\phi(4n+1)}\equiv 1 \pmod{4n+1}$. If h is the smallest positive integer such that $2^h\equiv 1 \pmod{4n+1}$ then 2 is said to belong to the exponent h modulo $4n+1$. If $h=\phi(4n+1)$ then 2 is called a primitive root modulo $4n+1$.

4. An algorithm. Theorem 3 provides an easily computerized algorithm for determining the exponent to which 2 belongs modulo integers of the form $4n+1$. Consider the recursion relation $N(1, m, n)=[(n+1)+N(1, m-1, n)-1]/2$ if $N(1, m-1, n)$ is odd, $N(1, m, n)=(n+1)+N(1, m-1, n)/2$ if $N(1, m-1, n)$ is even, with the initial condition $N(1, 0, n)=1$. Continue the process until $N(1, m, n)=1$ and denote this value of m by $m(1, n)$. Let N^* be the number of times that $N(1, m, n)$, $m=1, 2, \cdots, m(1, n)$, is even. If N^* is odd then $2\cdot m(1, n)$ is the exponent of 2 modulo $4n+1$, while if N^* is even then $m(1, n)$ is.

5. A distributional question. Attention is now directed to the question of whether there is a characterization for the values of n such that $2n$ shuffles, the maximum number, are necessary before the cards return to their original order.

THEOREM 4. *$m(1, n)=2n$ iff $4n+1$ is a prime, n is odd and 2 is a primitive root modulo $4n+1$.*

Proof. If $4n+1$ is a prime, by Fermat's theorem, either $2^{2n}\equiv 1 \pmod{4n+1}$ or $2^{2n}\equiv -1 \pmod{4n+1}$. Because 2 is not a square modulo primes of the form $4n+1$ if n is odd, $2^{2n}\equiv -1 \pmod{4n+1}$. Since 2 is a primitive root modulo $4n+1$, by Theorem 3, $m(1, n)=2n$. If 2 had not been a primitive root, then $2^h\equiv 1 \pmod{4n+1}$ where $h<4n$, so $m(1, n)\leqq h/2<2n$.

Suppose now that $4n+1$ is a prime and n is even. The square 2 is a solution of $x^{2n}\equiv 1 \pmod{4n+1}$ and consequently $4n+1$ divides 2^n+1 or 2^n-1. Hence, $m(1, n)\leqq n$.

Finally, suppose that $4n+1$ is not a prime: $\phi(4n+1)<4n$, and since $2^{\phi(4n+1)}\equiv 1 \pmod{4n+1}$, $2^{\frac{1}{2}\phi(4n+1)}\equiv 1 \pmod{4n+1}$ or $2^{\frac{1}{2}\phi(4n+1)}\equiv -1 \pmod{4n+1}$. Hence, $m(1, n)<2n$.

6. Conclusion. Undergraduate research can be a highly effective teaching method and the accessibility of computers to do extensive routine computational work has resulted in an increase of available research problems. The authors hope that this paper encourages college teachers to consider seriously the possibility of having their students do research.

Reference

1. Ivan Niven and H. S. Zuckerman, An Introduction to the Theory of Numbers, 2nd ed. Wiley, New York, 1960.

COFACTORAL MATRICES

R. BUCHER and S. GODBOLE, Virginia Polytechnic Institute

1. Introduction. Cofactoral matrices are presented here for their heuristic value. Nearly all the theorems given are accessible to a student just beginning the study of matrices, and many of the results are well known; yet the theory of cofactoral matrices is surprisingly rich and rewarding. The ring of cofactoral matrices of order two over a field K is isomorphic to $K[x]/(x^2+1)$. In particular, when K is the field of real numbers, this ring is isomorphic to the field of complex numbers. The study of real nonsingular cofactoral matrices leads naturally to the study of orthogonal matrices.

2. General theorems. Let $A=[a_{ij}]$ and let $\operatorname{cof}(a_{ij})$ denote the cofactor of a_{ij}. Throughout this paper cof A denotes $[\operatorname{cof}(a_{ij})]$.

DEFINITION. *If A is an n by n matrix over a field K, where $n\geqq 2$ and $A=\operatorname{cof} A$, then A is a cofactoral matrix over K.*

THEOREM 2.1. *The identity matrix I_n is a cofactoral matrix.*

THEOREM 2.2. *The null matrix 0_n is a cofactoral matrix.*

THEOREM 2.3. *If A is a cofactoral matrix over K, then* $|A| = \sum_{i=1}^{n}(a_{ij})^2$; $j=1, \cdots, n$ *and* $|A| = \sum_{j=1}^{n}(a_{ij})^2$; $i=1, \cdots, n$.

Proof. Let A_{ij} be the cofactor of a_{ij}. Then $|A| = \sum_{i=1}^{n} a_{ij}A_{ij}$. Since A is a cofactoral matrix, $a_{ij}=A_{ij}$. Therefore $|A| = \sum_{i=1}^{n}(a_{ij})^2$. In the same manner we can prove that $|A| = \sum_{j=1}^{n}(a_{ij})^2$.

THEOREM 2.4. *A is a cofactoral matrix over K if and only if* $\operatorname{adj} A = A^T$.

Proof. $A = \operatorname{cof} A \Leftrightarrow A^T = (\operatorname{cof} A)^T \Leftrightarrow A^T = \operatorname{adj} A$.

THEOREM 2.5. *Let A be a nonsingular matrix over K. Then A is a cofactoral matrix if and only if $A^{-1} = A^T/|A|$.*

Proof. If A is a cofactoral matrix, then $A^{-1} = (\operatorname{adj} A)/|A| = A^T/|A|$. Conversely, suppose $A^T/|A| = A^{-1}$. Since $A^{-1} = (\operatorname{adj} A)/|A|$, it follows that $(A^T) = (\operatorname{adj} A)$ and $A = \operatorname{cof} A$.

THEOREM 2.6. *If A and B are nonsingular cofactoral matrices over K, then AB is a nonsingular cofactoral matrix.*

Proof. Since $(AB)^{-1} = B^{-1}A^{-1}$, $(\operatorname{adj} AB)/|AB| = (\operatorname{adj} B/|B|)(\operatorname{adj} A/|A|)$. Therefore $\operatorname{adj} AB = \operatorname{adj} B \operatorname{adj} A$; hence $\operatorname{adj} AB = (AB)^T$; it follows from Theorem 2.4 that AB is cofactoral.

THEOREM 2.7. *If A is a nonsingular cofactoral matrix over K, then A^{-1} is a cofactoral matrix over K.*

Proof. By Theorem 2.5, $A^{-1} = A^T/|A|$. Thus $(A^{-1})^{-1} = (A^T/|A|)^{-1} = |A|(A^T)^{-1} = (A^T)^{-1}/|A^{-1}| = (A^{-1})^T/|A^{-1}|$. By Theorem 2.5, A^{-1} is a cofactoral matrix.

COROLLARY 2.8. *The set of n by n nonsingular cofactoral matrices over K is a group under matrix multiplication.*

Proof. Closure follows from Theorem 2.6, and the existence of inverses follows from Theorem 2.7. The proof of the following theorem is straightforward.

THEOREM 2.9. *If A is a cofactoral matrix over K of order n, and $k \in K$, then* $\operatorname{cof}(kA) = k^{n-1}A$.

COROLLARY 2.10. *If A is a cofactoral matrix of even order, then $-A$ is a cofactoral matrix over K.*

3. Cofactoral matrices of order 2.

THEOREM 3.1. *Let A be a 2 by 2 matrix over K. Then A is cofactoral if and only if A is of the form* $A = \begin{bmatrix} c & b \\ -b & c \end{bmatrix}$.

Proof.

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}. \qquad \operatorname{cof} A = \begin{bmatrix} a_{22} & -a_{21} \\ -a_{12} & a_{11} \end{bmatrix}.$$

Thus $(A = \text{cof } A) \Leftrightarrow a_{11} = a_{22};\ a_{12} = -a_{21}$.
The following corollaries may be easily verified.

COROLLARY 3.2. *Every 2 by 2 skew symmetric matrix over K is a cofactoral matrix.*

COROLLARY 3.3. *The set of 2 by 2 real cofactoral matrices forms a field with respect to matrix multiplication and addition, which is isomorphic to the field of complex numbers.*

COROLLARY 3.4. *The set of 2 by 2 cofactoral matrices over K is closed under matrix addition and multiplication.*

COROLLARY 3.5. *If A and B are 2 by 2 cofactoral matrices over K, then AB = BA.*

THEOREM 3.6. *The set of all 2 by 2 cofactoral matrices over K forms a commutative ring with unity.*

Proof. This theorem follows immediately from Corollaries 2.10, 3.4, 3.5, and Theorems 2.1 and 2.2.

THEOREM 3.7. *The ring of 2 by 2 cofactoral matrices over a field K is isomorphic to the ring* $K[x]/(x^2+1)$.

Proof. The elements of $K[x]/(x^2+1)$ are of the form $[(ax+b)]$. The correspondence of $\begin{bmatrix} b & a \\ -a & b \end{bmatrix} \leftrightarrow [(ax+b)]$ is the desired isomorphism.

THEOREM 3.8. *The characteristic values of a 2 by 2 cofactoral matrix* (a_{ij}) *over K are* $a_{11} \pm ia_{12}$ *(where K is the field of complex numbers).*

Proof. By Theorem 3.1, $|A - \lambda I| = 0$ becomes $\lambda^2 - 2a_{11}\lambda + (a_{11}^2 + a_{12}^2) = 0$ and the conclusion follows from the quadratic formula.

4. Real cofactoral matrices.

THEOREM 4.1. *If A is a real cofactoral matrix, then either A is nonsingular or A is the null matrix.*

Proof. By Theorem 2.3, $|A| = \sum_{i=1}^{n} (a_{ij})^2$ $(j = 1, \cdots, n)$. Therefore, since A is a real matrix, $|A| = 0$ if and only if $a_{ij} = 0$ for each entry a_{ij}.

THEOREM 4.2. *If A is a nonzero, real cofactoral matrix of order* $n \neq 2$, *then* $|A| = 1$.

Proof. By Theorem 4.1, A is nonsingular. Thus A adj $A = |A| I$. By Theorem 2.4, $AA^T = |A| I$, whence $|AA^T| = |A|^n$ or $|A|^2 = |A|^n$. Thus $|A|^{n-2} = 1$. By Theorem 2.3, $|A| > 0$. Therefore if $n \neq 2$, $|A| = 1$.

THEOREM 4.3. *If A is a nonzero real cofactoral matrix of order* $n \neq 2$, *then A is an orthogonal matrix.*

Proof. By Theorem 4.1, A is nonsingular and by Theorem 2.5, $A^{-1} = A^T/|A|$. The result now follows from Theorem 4.2.

Note. Because the determinant of an orthogonal matrix may be -1, the converse of Theorem 4.3 is not valid.

THEOREM 4.4. *If A is an n by n orthogonal matrix and if $|A|=1$, then A is cofactoral.*

Proof. $A^T=A^{-1}=\text{adj } A/|A|=\text{adj } A$. The result now follows from Theorem 2.4.

THEOREM 4.5. *The set of nonzero, real cofactoral matrices of order n, forms a group under matrix multiplication.*

Proof. Let A be a nonzero, real cofactoral matrix. By Theorem 4.1, A^{-1} exists and by Theorem 2.7, A^{-1} is cofactoral. The result now follows from Theorem 2.6.

THEOREM 4.6. *In the multiplicative group of nonzero, real, cofactoral matrices ($n\neq 2$), the symmetric matrices are the elements of order 2.*

Proof. Let A be a symmetric matrix in the group. Then $A^{-1}=(\text{cof } A)^T/|A| =(\text{cof } A)^T=A^T=A$. Let B be in the group and suppose $B^2=I$. Then $B=B^{-1} =(\text{cof } B)^T=B^T$.

The authors wish to thank Professors Hugh Campbell and Peter Fletcher for their guidance and assistance in the preparation of this paper.

A NOTE ON SUMS OF SQUARES OF CONSECUTIVE ODD INTEGERS

J. A. H. HUNTER, Toronto

In his paper, *Sums of squares of consecutive odd integers*, Brother Alfred [1] is led to the equation

$$X^2 - nY^2 = -(n^2 - 1)/3, \tag{1}$$

with $n\not\equiv 0 \pmod 3$. He proves certain theorems giving various sets of values of n, for which (1) has no solution. We prove here an additional theorem giving another set of values of n for which (1) has no solution.

THEOREM. *If $(n^2-1)/3=-p^{2r+1}M$, where p is a prime with $p\equiv -1 \pmod 4$ and M an integer not divisible by p, then (1) has no solution if $n\equiv -1 \pmod p$.*

Proof. Since an odd power of p divides $(n^2-1)/3$, it follows that $x^2-ny^2 \equiv 0 \pmod p$ for some integers x and y, neither one of which is divisible by p. Using the fact that $ny^2\equiv -y^2 \pmod p$, we have $x^2-ny^2\equiv x^2+y^2\equiv 0 \pmod p$, which is impossible for $p\equiv -1 \pmod 4$.

Reference

1. Brother U. Alfred, Sums of squares of consecutive odd integers, this MAGAZINE, 40 (1967), 194–199.

DETERMINANTS, PERMANENTS AND BIPARTITE GRAPHS

FRANK HARARY, University of Michigan

The combinatorial properties of a nonnegative matrix M are captured by t binary matrix $A=A(M)$ in which the entries are 1 whenever those of M positive. The entries of a binary matrix are 0 or 1. If A is a square matrix, n it can be regarded as the adjacency matrix of a directed graph (digraph). A is rectangular a bipartite graph (bigraph) can be associated with A; of rse this can also be done for A square. The determinant of the adjacency trix of a graph of digraph has been expressed in terms of its structure, and so the permanent. Our objects are:

(1) to express the permanent of a square or rectangular binary matrix in ms of the associated bigraph;

(2) to formulate the determinant of a square matrix in terms of its bigraph.

1. Nonnegative matrices, binary matrices, graphs, digraphs, and bigraphs. : $M=[m_{ij}]\geqq 0$ be a given nonnegative matrix. The *binary matrix of* M is de- ›d as $A=A(M)=[a_{ij}]$ where $a_{ij}=1$ when $m_{ij}>0$; $a_{ij}=0$ when $m_{ij}=0$. If A is quare matrix, $n\times n$, then as noted in [**1**, **2**, **3**, **4**, **5**] it can be regarded as the acency matrix of that directed graph $D=D(A)$ with n points (or vertices) $v_2, \cdots, v_n$ in which there is an arc (directed line) from v_i to v_j whenever $=1$; see Figure 1. In the event that A is symmetric and has trace zero, the raph $D(A)$ can also be considered as a graph; see [**3**].

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

$D(A)$

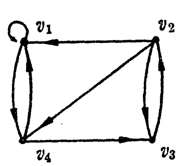


FIG. 1. A square binary matrix and its digraph.

If A is a rectangular matrix, $m\times n$ with $m<n$, then a digraph cannot be so ociated with A but another kind of graph can. A *bipartite graph* B, or *bigraph* brevity, has two sets of points $U=\{u_1, \cdots, u_m\}$ and $V=\{v_1, \cdots, v_n\}$, h no line joining two points in the same set. Thus the *bigraph of* A is defined expected as that bigraph $B=B(A)$ with point sets U and V in which u_i and ıre adjacent whenever $a_{ij}=1$. Of course a bigraph may also be associated h a square binary matrix in the same way.

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

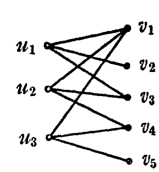


FIG. 2. A rectangular matrix and its bigraph.

2. Permanents and bigraphs. The *permanent* of a square matrix has been defined as:

$$\text{per } A = \sum a_{1\alpha_1}a_{2\alpha_2} \cdots a_{n\alpha_n} \tag{1}$$

where the sum is taken over all permutations $\alpha=(\alpha_1, \cdots, \alpha_n)$ of the set $N_n=\{1, 2, \cdots, n\}$. For a square binary matrix A, it was observed in [3] that per A can be expressed in terms of the digraph $D(A)$. A *linear subgraph* of digraph D is a spanning subgraph (on all the points of D) in which every point has both indegree and outdegree 1 (see [5] for digraph definitions). Then *per A is the number of different linear subgraphs of $D(A)$.* This is clearly only a rephrasing of (1).

The next remark, although elementary, does not appear to have been made in the literature. A *1-factor* of a graph G, or briefly *a factor* (since it is the only kind of factor we will consider), is a spanning subgraph of G in which every point has degree 1. Clearly there is a 1-1 correspondence between the linear subgraphs of the digraph $D(A)$ and the factors of the bigraph $B(A)$. Thus *per A is the number of different factors of $B(A)$.*

The permanent can also be defined for an $m \times n$, $m<n$, rectangular matrix A; see Ryser [6], as the sum of the permanents of all its $m \times m$ submatrices. If A is regarded as an incidence matrix with rows as sets and columns as elements, then it is well known that *per A is the number of SDR's* (systems of distinct representatives).

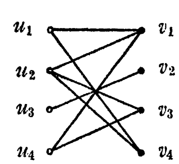


FIG. 3. The bigraph of matrix A of FIG. 1.

We illustrate with Figure 3 which shows the bigraph $B(A)$ of the matrix A of Figure 1. Since the line u_3v_2 is a connected component of $B(A)$, it must occur in every factor of $B(A)$. We show in Figure 4 the bigraph $B'=B(A)-u_3-v_2$ and its three factors, verifying that per $B(A)=3$.

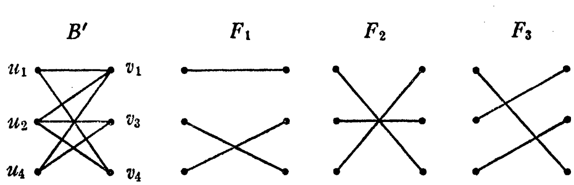


FIG. 4. The factors of a bigraph.

3. Determinants and bigraphs. An expression for the determinant of the adjacency matrix of a graph or digraph was obtained in [3] in terms of the linear subgraphs and the number of even directed cycles in each. This was used in [1] to derive a graph theoretic criterion for the equality per A = det A for a given square binary matrix A. We now derive an expression for det A in terms of $B(A)$ rather than $D(A)$. The *crossing number* $\nu(G)$ of a graph G has been defined, see [4], as the minimum possible number of intersections of pairs of edges when G is drawn in the plane. We modify this definition slightly for the present purpose.

Let A be a square binary matrix and let $B(A)$ be its bigraph with point sets $U=\{u_1, \cdots, u_n\}$ and $V=\{v_1, \cdots, v_n\}$. Let the factors of $B(A)$ be $F_1, F_2, \cdots$. The *intersection number* $\nu(F_i)$ of a factor F_i of $B(A)$ is the number of intersections of its edges when F_i is drawn with u_1 above u_2 above $u_3 \cdots$ on the left and v_1 above $v_2 \cdots$ on the right. With only a slight change in numbering, this is illustrated in Figure 4, where $\nu(F_1)=1$, $\nu(F_2)=3$, and $\nu(F_3)=2$.

THEOREM. *The determinant of A is given by the crossing numbers of the factors of $B(A)$ in accordance with*

$$\det A = \sum_i (-1)^{\nu(F_i)}. \tag{2}$$

Proof. It is only necessary to verify that for any factor F of $B(A)$, the sign of the term in det A corresponding to F is $(-1)^{\nu(F)}$. Using induction, if $\nu(F)=0$, then the term in det A must be $a_{11} a_{22} \cdots a_{nn}$ which is positive. For each increase in the crossing number $\nu(F)$ by 1, exactly one transposition is juxtaposed to the corresponding permutation α which determines the sign of the term.

Alternatively, the crossing number $\nu(F)$ of the factor F is always equal to the number of "inversions" (deviations from increasing order) in the sequence $i_1, i_2, \cdots, i_n$ corresponding to the nonvanishing term $a_{1i_1} a_{2i_2} \cdots a_{ni_n}$.

Thus the bigraph of a square binary matrix leads to still another equivalent definition of the determinant of an arbitrary square matrix.

The preparation of this note was supported in part by a grant from the U. S. Air Force Office of Scientific Research.

References

1. L. W. Beineke and F. Harary, Binary matrices with equal determinant and permanent, Studia Sci. Acad. Math. Hung., 1 (1966) 179–183.

2. A. L. Dulmage and N. S. Mendelsohn, Graphs and Matrices, Chap. 6 in Graph Theory and Theoretical Physics, F. Harary, ed., Academic Press, London, 1967, pp. 167–227.

3. F. Harary, The determinant of the adjacency matrix of a graph, SIAM Rev., 4 (1962) 202–210.

4. ———, Graph Theory, Addison-Wesley, Reading, 1969, to appear.

5. ———, R. Norman and D. Cartwright, Structural Models: An Introduction to the Theory of Directed Graphs, Wiley, New York, 1965.

6. H. J. Ryser, Combinatorial Mathematics, Carus Monograph 14, MAA, New York, 1965

ANSWERS

A454. The trains cover $1/6+1/9$ or $5/18$ of the distance between the towns in one hour. Hence, they will meet at $10+18/5-12$ or 1:36 p.m.

A455. We have

$$\begin{aligned} t_i &= (2a_j a_k \cos a_i/2)/(a_j + a_k) \\ &< (2a_j a_k)/(a_j + a_k) \\ &\leqq (a_j + a_k)/2. \end{aligned}$$

Also $1/t_i > \frac{1}{2}(1/a_j + 1/a_k)$. The result follows.

A456. The arithmetic mean-geometric mean inequality guarantees that:

$$\begin{aligned} &(\text{A}) \quad 1 + x^2 \geqq 2x \\ &(\text{B}) \quad x^2 + x^6 \geqq 2x^4 \\ &(\text{C}) \quad x^6 + 4x^8 \geqq 4x^7 \\ &(\text{D}) \quad 4x^8 + 1 \geqq 4x^4. \end{aligned}$$

Equality results in (A) only when $x=1$ and in (C) only when $x=1/2$. Summing (A), (B), (C), and (D) must, therefore, yield the strict inequality

$$8x^8 + 2x^6 + 2x^2 + 2 > 4x^7 + 6x^4 + 2x^2$$

which yields the desired conclusion.

A457. $\int_0^{\pi/2} \sin x\, dx$ is the area of the region bounded by the curve $y = \sin x$ and the lines $x = \pi/2$ and $y = 0$. Rotating this region about the line $y = x$, the region is bounded by the curve $y = \text{arc} \sin x$ and the lines $y = \pi/2$ and $x = 0$. The area of this region is $\pi/2 - \int_0^1 \text{arc} \sin x\, dx$. Hence the result.

(Quickies on page 164)

BOOK REVIEWS

Prepared by Dmitri Thoro, San Jose State College

BRIEF MENTION

Essentials of Basic Mathematics. By A. J. Washington, H. R. Boyd, and S. H. Plotkin. Addison-Wesley, Reading, Mass., 1967. ix+292 pp. $7.50.

Intended for students in technical or liberal arts programs as well as those needing a review or remedial proficiency in secondary school mathematics. An informal and intuitive approach is used. A 60-page instructor's guide is available.

Elements of Mathematics. By B. E. Meserve and M. A. Sobel. Prentice-Hall, Englewood Cliffs, N. J., 1968. xi+303 pp. $7.95.

The first chapter, "Explorations in Mathematics," affords the student an opportunity to make discoveries on his own. The pace is leisurely; however, there are chapters on numbers, logic, geometry (including analytic geometry), mathematical structures, and probability and statistics.

The Nature of Mathematics. By F. H. Young. Wiley, New York, 1968. xi+407 pp. $7.50.

"The general purpose of the text is to leave the student with a knowledge of some of the aims, techniques, and results of mathematics and with an appreciation of the role of mathematics in the world today." Although the selection of topics is fairly traditional and the author avoids recreational mathematics, there are pertinent historical remarks and such embellishments as an application of simultaneous congruences, Huntington's postulates, and binary adders. The book ends with a brief introduction to computers.

Mathematics: The Alphabet of Science. By M. F. Willerding and R. A. Hayward. Wiley, New York, 1968. xii+285 pp. $6.95.

"The presentation is designed so that even persons who have had little or no high school mathematics . . . will have no trouble following the explanations." There are chapters on logic, number theory, groups and fields, probability and statistics, finite geometry, matrices, computers and numeration systems, and Fortran. Very attractive format.

Stories About Sets. By N. Vilenkin. Academic Press, New York, 1968. xiii+152 pp. $6.50.

This beautiful gem, translated from the Russian, explores the notion of cardinality and traces the evolution of such concepts as function, curve, surface, and dimension. In one chapter, "Remarkable Functions and Curves, or a Stroll through a Mathematical Art Museum," there are such delightful sections as "The Genie Escapes from the Bottle," "Wet Points," "The Devil's Staircase," "A Prickly Curve," "Everything Had Come Unstrung," "The Great Irrigation Project." Included are numerous little anecdotes and quotations; e.g., Hermite's remark written to Stieltjes: "I turn away in horror from this regrettable plague of continuous functions that do not have a derivative at even one point." One of the outstanding expositions of this decade!

A Survey of College Mathematics. By D. R. Horner. Holt, Rinehart and Winston, New York, 1967. ix+308 pp. $6.95.

This attractive survey for the nonscience student covers topics "chosen for functional reasons rather than esthetic whims." It starts with the rudiments of set theory, basic number systems, and logic, and terminates with analytic geometry, trigonometry and elementary calculus.

Fundamental Mathematics. By B. K. Youse. Dickenson, Belmont, Calif., 1967. x+394 pp. $8.95.

The essential topics of algebra and trigonometry as well as an introduction to analytic geometry and calculus are presented in "the modern spirit."

The Elementary Functions. By C. R. Fleenor, M. E. Shanks, and C. F. Brumfiel. Addison-Wesley, Reading, Mass., 1968. ix+293 pp. $6.95.

Designed to provide the foundation for a standard course in calculus. "Since there is more than enough material for a one-semester course, selection can be made on the basis of student background."

A Prelude to the Calculus. By M. W. Pownall. McGraw-Hill, New York, 1967. x+315 pp. $6.95.

This book is the outcome of summer workshops and courses preparing teachers to teach advanced placement calculus. "Its purpose is not merely to review high school mathematics, nor to give an extensive treatment of the elementary functions; rather, it is designed to provide the student with a solid foundation in certain concepts on which the calculus rests . . . " It contains a large number of examples, counterexamples and problems.

An Introduction to Analytic Geometry and Calculus. By A. C. Burdette. Academic Press, New York, 1968. xii+412 pp. $8.95.

Written for a one-year course, meeting three times a week and presupposing a preparation equivalent to three semesters of high school algebra and one semester of trigonometry. An essentially traditional treatment.

Polynomials, Power Series, and Calculus. By H. Levi. Van Nostrand, Princeton, N. J., 1968. viii+158 pp. $5.75.

"This book is not intended for use as a text for the calculus course now generally given . . . , but rather as a text for a proposed replacement for that course." Consideration is given to current problems which arise from attempts to make simultaneous provision for divergent professional needs of two groups of students. This indeed leads to a completely new first course in analysis.

Infinite Series. By A. I. Markushevich. Heath, Boston, 1967. viii+188 pp. $4.95 (paper).

A translation and adaptation of the third Russian edition of a book first published thirty years ago, it is intended "to help the young reader interested in mathematics to approach infinite series with the facility with which one handles polynomials by following the methods begun by Newton and Euler. . . . This book might be viewed as a mathematical narrative in which the binomial theorem plays the part of the hero."

Basic Algebraic Systems: An Introduction to Abstract Algebra. By R. Laatsch. McGraw-Hill, New York, 1968. xii+224 pp. $7.95.

Assumed as a prerequisite is the "maturity acquired by a student in a semirigorous calculus course." Suitable for a one semester course; contains 460 exercises and three appendices.

Matrices and Linear Algebra. By H. Schneider and G. P. Barker. Holt, Rinehart and Winston, New York, 1968. ix+385 pp. $7.95.

"In this book, written mainly for students in physics, engineering, economics, and other fields outside mathematics, we attempt to make the subject accessible to a sophomore or even a freshman with little mathematical experience."

An Introduction to Vector Functions. By J. A. Hummel. Addison-Wesley, Reading, Mass., 1967. x+372 pp. $9.75.

Intended for mathematicians, engineers, and physicists; emphasis is on concepts rather than examples. The style is formal, but ostensibly topics in vector spaces, linear transformations, determinants, matrices, functions of several variables, differentials, integration, an introduction to curves and surfaces, and vector analysis are presented at the sophomore-junior level.

Teaching Modern Mathematics in the Elementary School. By H. Fehr and J. M. Phillips. Addison-Wesley, Reading, Mass., 1967. xvi+448 pp. $7.95.

Appropriate for a methods course for preservice elementary school teachers; included are chapters on enrichment topics and a comprehensive view of the elementary school mathematics program. This is a readable, relevant treatment of a much-neglected area.

Mathematics for Elementary School Teachers: A First Course. By J. W. Armstrong. Harper and Row, New York, 1968. xii+320 pp. $9.50.

An algebraic treatment of the number concept; number systems are introduced in approximately the same order they are introduced in the elementary grades. It is assumed the book will be used as a text for a terminal course.

Number Systems: An Elementary Approach. By J. R. Byrne. McGraw-Hill, New York, 1967. xiii+291 pp. $6.95.

Can be used for courses of various lengths; effective use is made of color and marginal notes.

Introduction to Number Systems. By G. A. Spooner, and R. L. Mentzer. Prentice-Hall, Englewood Cliffs, N. J., 1968. x+339 pp. $7.95.

A leisurely development with more than lip service paid to "modern" terminology.

Guidelines for Teaching Mathematics. By D. A. Johnson and G. R. Rising. Wadsworth, Belmont, Calif., 1967. viii+446 pp. $6.95.

This text appears to consist of a splendid mixture of nontrivial content and imaginative pedagogy. Excellent references, appendices, and the inclusion of often neglected topics (such as the role of computers) should be appealing to both the prospective and experienced secondary school teacher.

NEW EDITIONS

Plane Trigonometry, 2nd ed. By N. O. Niles. Wiley, New York, 1968. xv+282 pp. $5.95.

The chapter on vectors and complex numbers has been revised, logarithmic and exponential equations have been added and nearly all of the computational problems have been changed; more challenging problems and "theory" problems have been added.

Introductory Algebra, 2nd ed. By M. D. Eulenberg and T. S. Sunko. Wiley, New York, 1968. xi+317 pp. $6.50.

Sections on inequalities, rational and real numbers have been added.

Elementary Algebra for College Students, 2nd ed. By I. Drooyan and W. Wooton. Wiley, New York, 1968. x+302 pp. $6.95.

Functional use is made of a second color and new problems have been added.

College Algebra, 2nd ed. By A. Leonhardy. Wiley, New York, 1968. xiii+468 pp. $7.95.

Introduction to Algebra for College Students. By W. A. Rutledge and S. Green. Prentice-Hall, Englewood Cliffs, N. J., 1968. x+310 pp. $7.50.

Concepts and notation of sets and set operations are introduced in the first chapter.

PROBLEMS AND SOLUTIONS

EDITED BY ROBERT E. HORTON, Los Angeles Valley College

Readers of this department are invited to submit for solution problems believed to be new that may arise in study, in research, or in extra-academic situations. Proposals should be accompanied by solutions, when available, and by any information that will assist the editor. Ordinarily, problems in well-known textbooks should not be submitted.

Solutions should be submitted on separate, signed sheets. Figures should be drawn in India ink and exactly the size desired for reproduction.

Send all communications for this department to Robert E. Horton, Los Angeles Valley College, 5800 Fulton Avenue, Van Nuys, California 91401.

To be considered for publication, solutions should be mailed before October 1, 1969.

PROPOSALS

725. *Proposed by W. J. Blundon, Memorial University of Newfoundland.*

Prove that for every triangle ABC,

$$(\sin A+\sin B+\sin C)/\sin A \sin B \sin C \geqq 4$$

with equality only for the equilateral triangle.

726. *Proposed by Willy Enggren, Copenhagen, Denmark.*

Solve the following cryptarithm:

$$\begin{array}{ccccccc} & & & & T & H & E \\ & & E & A & R & T & H \\ & & V & E & N & U & S \\ & S & A & T & U & R & N \\ & U & R & A & N & U & S \\ \hline N & E & P & T & U & N & E \end{array}$$

727. *Proposed by John E. Prussing, University of California, San Diego.*

a] What is the range of positive values of x such that for a given x, the only positive value of y which satisfies the equation $y^x = x^y$ is the trivial solution $y = x$?

b] For those positive values of x for which nontrivial positive solutions for y exist, how many solutions are there?

c] If a value of x is selected at random from the open interval $(0, e)$, what is the probability that a nontrivial solution for y lies in the same interval?

728. *Proposed by G. L. N. Rao, J. C. College, Jamshedpur, India.*

Find the sum of the infinite series:

$$\frac{x-2}{x^2-x+1} + \frac{2x^2-4}{x^4-x^2+1} + \frac{4x^4-8}{x^8-x^4+1} + \cdots$$

when $|x| > 1$.

729. *Proposed by T. J. Burke, R.C.A. Moorestown, New Jersey.*

Prove that for any set of real numbers $\{T_i\}$, $(i=1, 2, \cdots, n)$,

$$\sum_{k,j=1}^{n} \cos (T_k - T_j) \geqq 0.$$

730. *Proposed by Mannis Charosh, New Utrecht High School, Brooklyn, New York.*

Prove that all rhombuses inscribed in a given rectangle are similar.

731. *Proposed by Santosh Kumar, Ministry of Defense, New Delhi, India.*

a] Express a factorial polynomial of degree n, the coefficients of which are taken as the coefficients in the expansion of $(1+x)^n$, as an ordinary power polynomial and prove that the sum of the coefficients of this ordinary power polynomial is $(n+1)$.

b] Assuming binomial coefficients of a factorial polynomial of degree n, prove that the factorial polynomial behaves simply as the factorial function of the same degree with respect to the difference operator Δ.

732. *Proposed by Douglas Lind, University of Virginia.*

Form the decimal number $x = x_0.x_1x_2x_3 \cdots$ as follows. Let $x_0 = 1$ and x_n be the least positive remainder upon division by 9 of $x_0 + x_1 + \cdots + x_{n-1}$. Show that x is rational.

SOLUTIONS

Late Solutions

B. McMillan, Morgan State College, Maryland: **698, 700, 703, 704**; *Huseyin Demir, Middle East Technical University, Ankara, Turkey*: **699, 702, 703.**

A Recurrence Relation

690. [March and November, 1968] *Proposed by J. M. Gandhi, University of Alberta, Canada.*

Prove that

$$\sum_{j=0}^{\gamma-1} \sum_{i=0}^{j} j!/(j-i)!$$

$$= \left| \begin{array}{cccccc} 0! & -\binom{1}{1} & 0 & 0 \cdots & 0 \\ 1! & +\binom{2}{1} & -\binom{2}{2} & 0 \cdots & 0 \\ 2! & -\binom{3}{1} & +\binom{3}{2} & -\binom{3}{3} \cdots & 0 \\ - & - & - & - \cdots & - \\ (\gamma-2)! & - & - & - \cdots & -\binom{\gamma-1}{\gamma-1} \\ (\gamma-1)! & -1^{\gamma}\binom{\gamma}{1} & +(-1)^{\gamma-1}\binom{\gamma}{2} & - \cdots & +\binom{\gamma}{\gamma-1} \end{array} \right| .$$

Solution by E. P. Starke, Plainfield, New Jersey.

We study first $S_j \equiv \sum_{i=0}^{j} i!/(j-i)!$, noting that $S_0 = 1$, $S_j = j\, S_{j-1} + S_0$. Now consider

$$T_n \equiv \sum_{j=0}^{n} (-1)^j \binom{n}{j} S_{n-j}. \tag{1}$$

Replace each S_k by $k\, S_{k-1} + S_0$ $(k = 1, 2, \cdots, n)$ and collect terms as follows:

$$T_n = \sum_{j=0}^{n} (-1)^j (n-j) \binom{n}{j} S_{n-j-1} + S_0 \sum_{j=0}^{n} (-1)^j \binom{n}{j}$$

$$= n \sum_{j=0}^{n-1} (-1)^j \binom{n-1}{j} + S_0(1-1)^n = nT_{n-1} + 0.$$

Since $T_0 = S_0 = 1$, we have

$$T_n = n! \tag{2}$$

Let $F_{\gamma+1} = \sum_{j=0}^{\gamma} S_j$, which can be put

$$F_{\gamma+1} = \sum_{j=0}^{\gamma}\binom{\gamma+1}{j}\sum_{k=0}^{\gamma-j}(-1)^k\binom{\gamma-j}{k}S_{\gamma-j-k}$$
$$= \sum_{j=0}^{\gamma}\binom{\gamma+1}{j}T_{\gamma-j} = \sum_{j=0}^{\gamma}\binom{\gamma+1}{j}(\gamma-j)!$$

Thus, for the left member of the proposed equation we have

$$F_\gamma = \sum_{j=0}^{\gamma-1}\binom{\gamma}{j}(\gamma-j-1)! \tag{3}$$

Let D_γ be the determinant as printed. Expand according to the elements of the last column, to get

$$D_\gamma = \binom{\gamma}{\gamma-1}D_{\gamma-1} + \binom{\gamma-1}{\gamma-1}\Delta, \qquad \gamma > 1.$$

Expanding Δ similarly, we have

$$D_\gamma = \binom{\gamma}{\gamma-1}D_{\gamma-1} - \binom{\gamma}{\gamma-2}D_{\gamma-2} + \Delta!$$

Continuing in the same fashion we reach at last

$$D_\gamma = \sum_{i=1}^{\gamma-1}(-1)^{i-1}\binom{\gamma}{\gamma-1}D_{\gamma-i} + (\gamma-1)! \tag{4}$$

Now consider the j equations (4) for $\gamma = 1, 2, \cdots, j$.

$$D_1 = 0!$$

$$D_2 = \binom{2}{1}D_1 + 1!$$

$$D_3 = \binom{3}{2}D_2 - \binom{3}{1}D_1 + 2!$$

$$D_4 = \binom{4}{3}D_3 - \binom{4}{2}D_2 + \binom{4}{1}D_1 + 3!$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$D_j = \binom{j}{j-1}D_{j-1} - \binom{j}{j-2}D_{j-2}\cdots$$
$$+ (-1)^{j-1}\binom{j}{2}D_2 + (-1)^j\binom{j}{1}D_1 + (j-1)!$$

Multiply the equation for D_k by $\binom{j}{k}$ and add. All terms cancel except D_j and the terms involving factorials. We have

$$(5)\qquad \begin{aligned} D_j = (j-1)! + \binom{j}{j-1}(j-2)! + \binom{j}{j-2}(j-3)! + \cdots \\ + \binom{j}{2}1! + \binom{j}{1}0! \end{aligned}$$

By (3) and (5) we have $D_\gamma = F_\gamma$, and the proof is complete.

It may be worth noting that, making use of the known relation:

$$\sum_{i=0}^{s} (-1)^i \binom{r}{i} = (-1)^s \binom{r-1}{s},$$

we can add successive columns beginning at the right (but leaving the first untouched) and repeat the process a sufficient number of times to put D_γ in the following form, from which (5) is evident:

$$D_\gamma = \begin{vmatrix} 0! & -1 & 0 & 0 & 0 & \cdots & 0 \\ 1! & 0 & -1 & 0 & 0 & \cdots & 0 \\ 2! & 0 & 0 & -1 & 0 & \cdots & 0 \\ 3! & 0 & 0 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\ (\gamma-2)! & 0 & 0 & 0 & 0 & \cdots & -1 \\ (\gamma-1)! & \binom{\gamma}{1} & \binom{\gamma}{2} & \binom{\gamma}{3} & \binom{\gamma}{4} & \cdots & \binom{\gamma}{\gamma-1} \end{vmatrix}$$

Comments and solutions also submitted by Arnold Hammel, Central Michigan University; C. B. A. Peck, State College, Pennsylvania; Stephen Spindler, Purdue University; and the proposer.

A Square Array

705. [November, 1968] *Proposed by Max Rumney, London, England.*

Devise a method and a proof for the method of placing the natural numbers 1 to n^2 in a square array n by n so that: (a) the column sums $\equiv 0 \pmod{n^2+1}$, (b) the differences of the products of the extreme numbers of the diagonals of every square in the array $\equiv 0 \pmod{n^2+1}$, and (c) the difference of the products of any two rows $\equiv 0 \pmod{n^2+1}$.

Solution by the proposer.

Let m^2+1 equal the prime number p. Then if q is a primitive root mod p, the power residues mod p in the array below is the desired array:

$$\begin{matrix} 1 & q & q^2 & \cdots & q^{n-1} \\ q^n & q^{n+1} & q^{n+2} & \cdots & q^{2n-1} \\ \vdots & & & & \\ q^{n(n-1)} & \cdot & \cdot & \cdots & q^{n^2-1} \end{matrix}$$

Proof:

a] The sum of the elements in any column is congruent to

$$q^r(1 + q^n + \cdots + q^{n(n-1)}) \equiv q^r(q^{n^2} - 1)/(q^n - 1) \equiv 0$$

by Fermat's Theorem.

b] Any such difference is congruent to $q^r \cdot q^{s+t} - q^s \cdot q^{r+t} \equiv 0$.

c] Any such difference is congruent to

$$q^{rn} \cdot q^{rn+1} \cdots q^{rn+n-1} - q^{sn} \cdot q^{sn+1} \cdots q^{sn+n-1} q^{rn^2}(1 \cdot q \cdot q^2 \cdots q^{n-1}) - q^{sn^2}(1 \cdot q \cdot q^2 \cdots q^{n-1}) \equiv 0$$

since $q^{n^2} \equiv 1$ and so $q^{sn^2} \equiv q^{rn^2} \equiv 1$.

It also follows easily that the determinant of the array $\equiv 0 \pmod p$.

A Strengthened Inequality

706. [November, 1968] *Proposed by Leon Bankoff, Los Angeles, California.*

In Problem 594 [this MAGAZINE, March, 1966] it was shown that

$$AD + BE + CF \leqq 2R + 5r$$

where R is the circumradius, r the inradius, and AD, BE and CF the altitudes of the triangle ABC. Strengthen this inequality by showing $AD+BE+CF \leqq 2R+4r+2r^2/R$.

Solution by L. Carlitz, Duke University.

Let h_a, h_b, h_c denote the altitudes of ABC, so that the stated inequality is

$$h_a + h_b + h_c \leqq \frac{2}{R}(R + r)^2. \tag{1}$$

Since $h_a = 2R \sin \beta \sin \gamma = bc/(2R)$, (1) may be replaced by

$$bc + ca + ab \leqq N(R + r)^2. \tag{2}$$

This result has been proved by J. Stenig (*Inequalities Concerning the Inradius and Circumradius of a Triangle*, Elem. Math., 18 (1963) 127–131). Stenig proves also that $bc+ca+ab \geqq 4r(5R-r)$, so that

$$h_a + h_b + h_c \geqq \frac{2r}{R}(5R - r). \tag{3}$$

Stronger results can be obtained. We have (see W. J. Blundon, *On Certain Polynomials Associated with the Triangle*, this MAGAZINE, 4 (1963) 247–248),

$$bc + ca + ab = r^2 + s^2 + 4Rr. \tag{4}$$

Using (4), Blundon (*Inequalities Associated with the Triangle*, Canad. Math. Bull., 8 (1965) 615–626) has proved the inequalities

$$2R^2 + 14Rr - 2(R - 2r)(R^2 - 2Rr)^{1/2} \leqq bc + ca + ab \leqq 2R^2 + 14Rr + 2(R - 2r)(R^2 - 2Rr)^{1/2}.$$

Hence

$$(5) \quad \begin{aligned} R + 7r - (R - 2r)(R^2 - 2Rr)^{1/2}/R &\leqq h_a + h_b + h_c \\ &\leqq R + 7r + (R - 2r)(R^2 - 2Rr)^{1/2}/R. \end{aligned}$$

It is easily verified that (5) is indeed stronger than (1) and (3).

Also solved by Joseph D. E. Konhauser, Macalester College; and the proposer.

Dissection into Squares and Equilateral Triangles

707. [November, 1968] *Proposed by Joseph Malkewitch, University of Wisconsin.*

For what values of k is there a convex polygon with k sides which can be dissected into squares and equilateral triangles which have the same length of side?

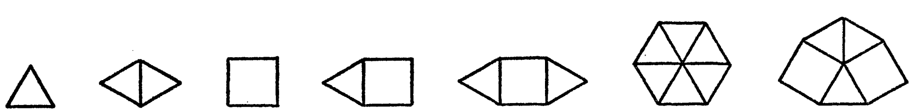
Solution by Michael Goldberg, Washington, D. C.

The only angles which the convex polygon can have are 60°, 90°, 120° and 150°. They are made of one or more of the angles of the triangle and the square. The greatest number of sides is obtained when only the largest angle is used. If all the angles are 150°, then the number of sides is 12.

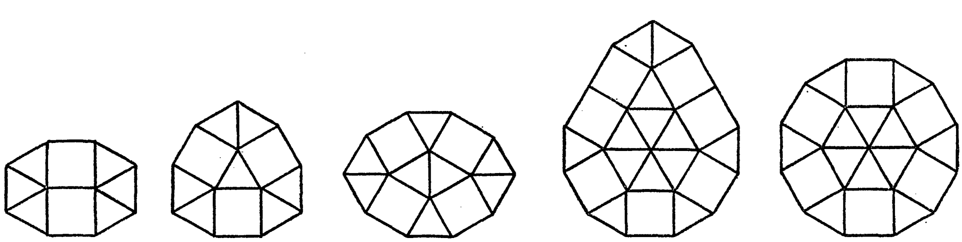
All smaller values of k are also possible. Examples for all the cases are shown in the figure. For some values of k, more than one polygon is shown. Note that, except for $k=11$, the polygons shown are equilateral.

Of course, each component square or triangle can be decomposed into smaller squares and triangles with equal edges.

If we assume that each dissected polygon must contain at least one equilateral triangle and at least one square, we eliminate the figures with $k=3$, 4 and the second figure with $k=6$. In addition, if we restrict the length of the sides of the polygon to be the same as those of the squares and equilateral triangles, we eliminate $k=11$.



$k=3$ $k=4$ $k=4$ $k=5$ $k=6$ $k=6$ $k=7$



$k=8$ $k=9$ $k=10$ $k=11$ $k=12$

Also solved by Ned Harrell, Los Altos, California; James R. Kuttler, Johns Hopkins Applied Physics Laboratory; T. P. Lin, San Fernando State College, California; Don N. Page, William Jewell College, Missouri; Bernard J. Portz, Jesuit College, Minnesota; Charles W. Trigg, San Diego, California; and the proposer.

A Trigonometric Sum

708. [November, 1968] *Proposed by Norman Schaumberger, Bronx Community College, New York.*

Prove that $\sum_{k=1}^{n-1} (n-k) \cos(2k\pi/n) = -n/2$.

I. *Solution by J. F. Leetch, Bowling Green State University, Ohio.*

Consider the nth roots of unity, $w_k = \cos(2k\pi/n) + i \sin(2k\pi/n)$, where $n > 1$ and $k = 0, 1, 2, \cdots, n-1$. It is easy to see that $\sum_{k=0}^{n-1} w_k = 0$ and $\sum_{k=0}^{n-1} \sin(2k\pi/n) = 0$. Thus $\sum_{k=1}^{n-1} \cos(2k\pi/n) = -1$. Now let $S = \sum_{k=1}^{n-1} (n-k) \cos(2k\pi/n) = \sum_{k=1}^{n-1} k \cos(2k\pi/n)$, so $2S = n\sum_{k=1}^{n-1} \cos(2k\pi/n) = -n$. Hence, $S = -n/2$.

II. *Solution by Joseph D. E. Konhauser, Macalester College, Minnesota.*

For $n=2$ the statement is trivially true, so assume $n \geqq 3$. Since $\cos(2\pi(n-k))/n = \cos(2\pi k/n)$, the sum $S = \sum_{k=1}^{n-1} (n-k) \cos(2k\pi/n)$ may be written as $S = \sum_{k=1}^{n-1} k \cos(2k\pi/n)$, so that $2S = n\sum_{k=1}^{n-1} \cos(2k\pi/n)$. Multiplying by $2\sin(2\pi/n)$, we obtain $4S \sin(2\pi/n) = n\sum_{k=1}^{n-1} \cos(2k\pi/n)\, 2 \sin(2\pi/n) = n\sum_{k=1}^{n-1} [\sin 2\pi(k+1)/n - \sin 2\pi(k-1)/n] = -2n \sin(2\pi/n)$. For $n \geqq 3$, $\sin(2\pi/n) \neq 0$, and $S = -n/2$.

Also solved by Arlo D. Anderson, US Naval Research Laboratory; Donald Batman, Parsippany, New Jersey; Sister Marion Beiter, Rosary Hill College; Robert Bridgman, Mansfield State College, Pennsylvania; J. L. Brown, Jr., Ordnance Research Laboratory, University Park, Pennsylvania; Mannis Charosh, Brooklyn, New York; Michael Goldberg, Washington, D. C.; John E. Hafstrom, California State College, San Bernardino; Curtis Herink, North Central College, Illinois; Ignacio D. Herssein, Brooklyn, N. Y.; T. W. Johnson and E. W. Seaholm (Jointly) Birmingham, Michigan; Lew Kowarski, Morgan State College, Maryland; J. R. Kuttler, Johns Hopkins Applied Physics Laboratory; B. McMillan, Morgan State College Maryland; John J. Moore, Niagara University, N. Y.; R. A. Moore, Oswego N. Y.; Don N. Page, William Jewell College, Missouri; Henry S. Lieberman, Newtonville, Maine; Charles Linett, Bowne High School, Flushing, New York; Kim R. Penrose, Rocky Mountain College; Henry J. Ricardo, Yeshiva University; S. Rohde, Lehigh University; Nathan Rubinstein, Johns Hopkins Applied Physics Laboratory; Edward F. Schmeichel, College of Wooster, Ohio; Stephen Spindler, Purdue University; E. P. Starke, Plainfield, New Jersey; Howard L. Walton, Decision Studies Group, Washington, D. C.; Kenneth M. Wilke, Topeka, Kansas; Gregory Wulczyn, Bucknell University; Kenneth L. Yocom, South Dakota State University; and the proposer.

A Convex Body

709. [November, 1968] *Proposed by H. S. Hahn, West Georgia College.*

Consider a convex body every point of whose surface is at a distance r from the surface of a regular tetrahedron with edges of length one. Find its surface area and its volume.

Solution by Joseph D. E. Konhauser, Macalester College, Minnesota.

Let T be the given tetrahedron and let T_r be the surface at distance r from T and enclosing T. First, consider the line segments of length r which are perpendicular to T and which, except for an endpoint on T, lie outside T. These line segments form four triangular prisms each having a face of T as base and an altitude of length r. The total volume of the four prisms is equal to the surface area of T (which is $\sqrt{3}$) times r.

Second, consider the line segments of length r which are perpendicular to an edge of T and which, except for an endpoint on T, lie outside T. These segments form six portions of solid circular cylinders of unit length whose volume is $\frac{1}{2}(\pi-\theta)r^2$, where $\theta=\text{Arccos } 1/3$ is the measure of the dihedral angles of T.

Finally, consider the line segments of length r which lie outside T except for an endpoint at a vertex of T and which are not already considered above. These line segments can be fitted together to form a solid sphere of radius r with volume $4\pi r^3/3$.

The total volume bounded by T_r is therefore $(\sqrt{2}/12)+r\sqrt{3}+3\ (\pi-\text{Arccos } 1/3)r^2+4\pi r^3/3$, where $\sqrt{2}/12$ is the volume bounded by T.

The surface area of T_r is $\sqrt{3}+6\ (\pi-\text{Arccos } 1/3)\ r+4\pi r^2$.

If r is less than $\sqrt{6}/12$, the inradius of T, and if the line segments are taken interior to T, then T_r is a regular tetrahedron with inradius $\sqrt{6}/12-r$ and bounds volume $8\sqrt{3}\ (\sqrt{6}/12-r)^3$ and has surface area $24\sqrt{3}\ (\sqrt{6}/12-r)^2$. Generalizations of these results to convex bodies were known to Steiner and Minkowski.

Also solved by Michael Goldberg, Washington, D. C.; James R. Kuttler, Johns Hopkins Applied Physics Laboratory; B. McMillan, Morgan State College, Maryland; Don N. Page, William Jewell College, Missouri; Nathan Rubinstein and James T. Stadter (Jointly), Johns Hopkins Applied Physics Laboratory; and the proposer.

Division Without Given Digits

710. [November, 1968] *Proposed by J. A. H. Hunter, Toronto, Canada.*

Solve the "no given digits" puzzle noting the decimal points and the repeating decimal in quotient.

```
x x x x ) x · x x x x ( · ẋ x x x x x ẋ
          x · x x x x
          -----------
              x x x x x
              x x x x x
              ---------
                    x x x x
                    x x x x
                    -------
                          x
```

Solution by Charles W. Trigg, San Diego, California.

From the structural details of the long division, it is clear that the period of the repeating decimal has the form $000ab0c$. Since a repeating decimal is a geometric progression with infinitely many terms, we have

$$\frac{x\cdot xxxx}{xxxx}=\frac{xxxxx}{xxxx0000}=\frac{0.000ab0c}{1-(0.1)^7}=\frac{ab0c}{9999999}=\frac{ab0c}{9\ (239)\ (4649)}$$

The last four x's of the original dividend must each be zero, so $d/xxxx=ab0c/(9)\ (239)\ (4649)$. Now $ab0c$ cannot be a multiple of 4649, hence $xxxx=4649$. Then $2151(d)=ab0c$, whereupon $d=2$ or 4. But in the division 4/4649, the difference from the second subtraction has three digits, so the unique reconstruction is

```
4649) 2.0000        (0.0004302̇
      1 8596
      ------
        14040
        13947
        -----
           9300
           9298
           ----
              2
```

Also solved by E. P Starke, Plainfield, New Jersey; Kenneth M. Wilke, Topeka, Kansas; and the proposer.

A Product of Sums

711. [November, 1968] *Proposed by Thomas Shewczyk, University of Wisconsin at Waukesha.*

If the numbers $a_1, a_2, \cdots, a_n$ are positive, then show that

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{i=1}^{n} \frac{1}{a_i}\right) \geqq n^2$$

I. *Solution by W. Moser, McGill University.*

For any permutation $b_1, b_2, \cdots, b_n$ of $a_1, a_2, \cdots, a_n$

$$\left(\sum_{i=1}^{n} \frac{a_i}{b_i}\right)^n/n \geqq \prod_{i=1}^{n} \frac{a_i}{b_i} = 1 \quad \text{or} \quad \sum_{i=1}^{n} \frac{a_i}{b_i} \geqq n.$$

Hence (taking subscripts mod n) $\left(\sum_{1}^{n} a_i\right)\left(\sum_{1}^{n} \frac{1}{a_i}\right) = \sum_{k=0}^{n-1}\sum_{i=1}^{n} \frac{a_i}{a_{i+k}} \geqq \sum_{k=0}^{n-1} n = n^2.$

II. *Solution by Michael Goldberg, Washington, D. C.*

Let $x+y=k$. Then, $1/x+1/y$ is minimized when $x=y=k/2$. Hence, the left member of the given relation is reduced when two unequal members of the a_i are each replaced by their arithmetic mean. The least value occurs when all the members are equal. But, in that case, $a_1=a_2=a_3= \cdots =a_n=(\sum a_i)/n$, $1/a_i=n/\sum a_i$, $\sum 1/a_i=n^2/\sum a_i$, and $(\sum a_i)$ $(\sum 1/a_i)=n^2$. Hence, the given inequality is confirmed.

III. *Solution by Brother T. Brendan, St. Mary's College, California.*

It is evident that for $n=1$, the relation holds. If for $n=k$ it holds, then the product

$$P = \left(\sum_{i=1}^{k} a_i + a_{k+1}\right)\left(\sum_{i=1}^{k} \frac{1}{a_i} + \frac{1}{a_{k+1}}\right) \geqq k^2 + \sum_{i=1}^{k} \frac{a_i}{a_{k+1}} + \sum_{i=1}^{k} \frac{a_{k+1}}{a_i} + 1,$$

where each of the k numbers a_i/a_{k+1} can be paired with the corresponding number a_{k+1}/a_i to give, by a well known result, a sum$\geqq 2$. Hence $p \geqq k^2+2k+1 =(k+1)^2$ and so, by induction, the relation is established.

IV. *Solution by John M. Howell, Los Angeles City College.*

If we multiply $(\sum_{i=1}^{n} a_i)(\sum_{i=1}^{n} 1/a_i)$ we obtain n^2 terms of which n would be unity since they are a_i/a_i. Then there would be $(n^2-n)/2$ terms which could be paired: $a_i/a_j+a_j/a_i$. That is the sum of a number and its reciprocal which is greater than or equal to 2. Thus

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{i=1}^{n} 1/a_i\right) \geqq n + \left(\frac{n^2-n}{2}\right)(2) = n^2.$$

The equality holds if and only if each $a_i = 1$.

V. *Solution by John E. Hafstrom, California State College, San Bernardino.*

By the Schwartz inequality, we have

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{i=1}^{n} 1/a_i\right) = \left(\sum_{i=1}^{n} (\sqrt{a_i})^2\right)\left(\sum_{i=1}^{n} (1/\sqrt{a_i})^2\right)$$

$$\geqq \left(\sum_{i=1}^{n} \sqrt{a_i}/\sqrt{a_i}\right)^2 = n^2.$$

References or solutions were also submitted by Leon Bankoff, Los Angeles, California; Donald Batman, Parsippany, New Jersey; Sister Marion Beiter, Rosary Hill College; Brother Thomas Bennett, Xaverian College, Maryland; Wray G. Brady, University of Bridgeport, Connecticut; Robert Bridgman, Mansfield State College, Pennsylvania; Gary L. Britton, University of Wisconsin in West Bend; Bruce A. Broemser, University of California at Berkeley; John L. Brown, Jr., Ordnance Research Laboratory, University Park, Pennsylvania; Mannis Charosh, Brooklyn, N. Y.; Santo M. Diano, Philadelphia, Pennsylvania; Fred Ficken, New York University; Robert J. Herbold, Procter and Gamble Company, Cincinnati, Ohio; Curtis Herink, North Central College, Illinois; James C. Hickman, University of Iowa; John E. Homer, Jr., Union Carbide Company, Illinois; Bruce W. King, Adirondack Community College, Glens Falls, New York; J. D. E. Konhauser, Macalester College, Minnesota (three solutions); Norbert J. Kuenzi, Iowa City, Iowa; James R. Kuttler, Johns Hopkins Applied Physics Laboratory; Henry S. Lieberman, Newtonville, Maine; Charles Linett, Bowne High School, Flushing, New York (two solutions); Peter A. Lindstrom, Genesee Community College, Batavia, New York; B. McMillan, Morgan State College, Maryland; John J. Moore, Niagara College, N. Y.; R. A. Moore, Oswego, N. Y.; Don N. Page, William Jewell College, Missouri; Frank J. Papp, University of Delaware; C. B. A. Peck, State College, Pennsylvania; Kim R. Penrose, Rocky Mountain College; Willis B. Porter, New Iberia, Louisiana; John E. Prussing, University of California at San Diego; Kenneth A. Ribet, Brown University; Henry J. Ricardo, Yeshiva University; Nathan Rubinstein, Johns Hopkins Applied Physics Laboratory; Edward F. Schmeichel, College of Wooster, Ohio; E. P. Starke, Plainfield, New Jersey; Zalman Usiskin, Ann Arbor, Michigan; Julius Volpe, Newark, N. J.; Howard L. Walton, Washington, D. C.; Gregory Wulczyn, Bucknell University; K. L. Yocom, South Dakota State University; Sze-Chung Yuan, Lakehead University, Canada; and the proposer.

The problem was found in *Geometric Inequalities*, by Kazarinoff, *Inequalities*, by Korovkin, *The USSR Olympiad Problem Book*, and in *The Pleasures of Mathematics*, by Goodman.

Comment on Problem 680

680. [January and September, 1968] *Proposed by Huseyin Demir, Middle East Technical University, Ankara, Turkey.*

Let E be an ellipse and t', t'' be two variable parallel tangents to it. Consider a circle C, tangent to t', t'' and to E externally. Show that the locus of the center of C is a circle.

Comment by A. W. Walker, Toronto, Canada.

Many interesting properties of an ellipse are associated with its so-called Chasles circles of radius $a \pm b$ concentric with the ellipse. If the center of the variable circle C lies on the *inward* normal, its locus is the inner Chasles circle. The result in Problem 680 was established by Mannheim, Nouvelles Annales de Math., 4, 3, (1903) 483, and is equivalent to the following old Japanese theorem (Iwata, 1862):

If an ellipse touches externally two equal nonoverlapping fixed circles and their parallel common tangents, the sum of its major and minor axes is equal to the distance between the centers of the circles.

See Tôhoku Math. J., (1), 11, (1917) 65, where with rather obscure justification, it is asserted that the theorem is untrue!

Comment on Q411

Q411. [May, 1967] Show that the sum of two successive odd primes is the product of at least three (not necessarily distinct) prime factors.

[*Submitted by John D. Baum*]

Comment by Charles W. Trigg, San Diego, California.

$3+5=2^3$. If the primes are greater than 3, then $(p_1+p_2)/2$ is not only even but is divisible by 3, so p_1+p_2 is divisible by 12. (Cf. Problem 652, November, 1967, Page 282.)

Comment on Q440

Q440. [November, 1968] A lady made three circular doilies with radii of 2, 3, and 10 inches, respectively. She placed them on a circular table so that each doily touched the other two. If each doily also touched the edge of the table, what was its radius?

[*Submitted by Walter W. Howard*]

Comment by Leon Bankoff, Los Angeles, California.

Curiously enough, the three doilies can be rearranged so as to cover an entire diameter of the table. An infinite number of cases exist in which the particular method of solution given in A440 can be applied, and again, in each case, the three doilies can be rearranged to cover a diameter of the table. Several other examples of this special situation are: (3, 2, 1), (21, 4, 3), (36, 5, 4), etc., *ad infinitum*. The formula for generating combinations of three radii yielding this curious result is n, $(n+1)$, $n(2n+1)$, where n is any positive integer. In each case, the circumscribing circle has a radius equal to the combined radii of the three smaller circles.

To unravel the apparent mystery behind this phenomenon, consult articles by M. G. Gaba and by Victor Thébault, in the American Mathematical Monthly, January 1940, pp. 19–24, and November, 1940, pp. 640–642.

Comment on Q442

Q442. [November, 1968] E. T. Bell ("Men of Mathematics") relates an amusing story of Descartes assigning his pupil, Catherine the Great, the famous Appollonian problem of constructing a circle tangent to three given circles. To vent his hidden contempt for her scholarly pretensions, he neglected to warn the poor girl that synthetic geometry should be used. She used his new analytic geometry and, supposedly, was led into a trap, the required solution of three simultaneous quadratics. On the contrary, show how an easy triumph was possible.

[*Submitted by Charles E. Maley*]

Comment by Leon Bankoff, Los Angeles, California.

It is easy to prove that Descartes' contempt for Catherine the Great was entirely unjustified.

Proof. Descartes was born in 1596 and died in 1650. Catherine the Great was born in 1729 and died in 1796.

Note. The royal personage mentioned in Bell's anecdote (Page 48) was Princess Elizabeth of Bohemia. Some eminent scholars do not concur with Bell's disparaging interpretation of Descartes' opinion of Elizabeth. The Princess was Descartes' favorite disciple. Her friendship and correspondence with the great man continued until the time of his death.

QUICKIES

From time to time this department will publish problems which may be solved by laborious methods, but which with the proper insight may be disposed of with dispatch. Readers are urged to submit their favorite problems of this type, together with the elegant solution and the source, if known.

Q454. Two trains start at 10 a.m., one going from Brownsville to Jamestown, and the other from Jamestown to Brownsville. The first train takes 6 hours and the second takes 9 hours for the trip. Each travels at a constant rate with no stops. At what time of the day will the trains meet each other?

[*Submitted by Charles W. Trigg*]

Q455. Let t_i be the angle bisectors of a triangle $A_1A_2A_3$. Show that $\sum_{i=1}^{3} 1/t_i > \sum_{i=1}^{3} 1/a_i$ and that $\sum_{i=1}^{3} t_i < \sum_{i=1}^{3} a_i$.

[*Submitted by Simeon Reich, Israel*]

Q456. For each real x prove that

$$4x^8 - 2x^7 + x^6 - 3x^4 + x^2 - x + 1 > 0.$$

[*Submitted by Erwin Just*]

Q457. Without evaluating either of the following definite integrals show why

$$\int_0^{\pi/2} \sin x dx = \pi/2 - \int_0^1 \text{arc} \sin x dx.$$

[*Submitted by Peter A. Lindstrom*]

(Answers on page 149)

ANSWERS

A454. The trains cover $1/6+1/9$ or $5/18$ of the distance between the towns in one hour. Hence, they will meet at $10+18/5-12$ or 1:36 p.m.

A455. We have

$$\begin{aligned} t_i &= (2a_ja_k \cos a_i/2)/(a_j + a_k) \\ &< (2a_ja_k)/(a_j + a_k) \\ &\leqq (a_j + a_k)/2. \end{aligned}$$

Also $1/t_i > \frac{1}{2}(1/a_j + 1/a_k)$. The result follows.

A456. The arithmetic mean-geometric mean inequality guarantees that:

$$\begin{aligned} &\text{(A)} \quad 1 + x^2 \geqq 2x \\ &\text{(B)} \quad x^2 + x^6 \geqq 2x^4 \\ &\text{(C)} \quad x^6 + 4x^8 \geqq 4x^7 \\ &\text{(D)} \quad 4x^8 + 1 \geqq 4x^4. \end{aligned}$$

Equality results in (A) only when $x=1$ and in (C) only when $x=1/2$. Summing (A), (B), (C), and (D) must, therefore, yield the strict inequality

$$8x^8 + 2x^6 + 2x^2 + 2 > 4x^7 + 6x^4 + 2x^2$$

which yields the desired conclusion.

A457. $\int_0^{\pi/2} \sin x\, dx$ is the area of the region bounded by the curve $y = \sin x$ and the lines $x = \pi/2$ and $y=0$. Rotating this region about the line $y=x$, the region is bounded by the curve $y = \arcsin x$ and the lines $y=\pi/2$ and $x=0$. The area of this region is $\pi/2 - \int_0^1 \arcsin x\, dx$. Hence the result.

(Quickies on page 164)

BOOK REVIEWS

PREPARED BY DMITRI THORO, San Jose State College

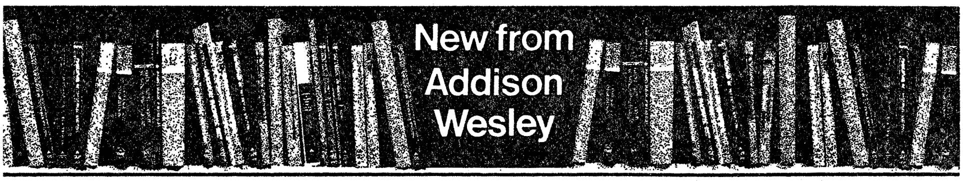
BRIEF MENTION

Essentials of Basic Mathematics. By A. J. Washington, H. R. Boyd, and S. H. Plotkin. Addison-Wesley, Reading, Mass., 1967. ix+292 pp. $7.50.

Intended for students in technical or liberal arts programs as well as those needing a review or remedial proficiency in secondary school mathematics. An informal and intuitive approach is used. A 60-page instructor's guide is available.

Elements of Mathematics. By B. E. Meserve and M. A. Sobel. Prentice-Hall, Englewood Cliffs, N. J., 1968. xi+303 pp. $7.95.

The first chapter, "Explorations in Mathematics," affords the student an opportunity to make discoveries on his own. The pace is leisurely; however, there are chapters on



INTRODUCTION TO MATHEMATICS FOR COLLEGE STUDENTS

By KENNETH C. SKEEN and CHARLES W. WHEELER, *Diablo Valley College.*

This text provides an extension of concepts and a review of skills for a basic course. Exposition and exercises are spirally developed and reinforced with discovery-type problems. By Chapter 5, the working tools of a basic course are developed and the last three chapters are devoted to applications.

424 pp., $7.95

INTRODUCTORY COLLEGE MATHEMATICS WITH BUSINESS APPLICATIONS

By KENNETH C. SKEEN, CHARLES W. WHEELER, *and* RALPH L. JOHNSON, *Diablo Valley College*

This text provides a review of basic skills and essential foundations of practical mathematics. It also offers a comprehensive introduction to the applications of mathematics in business. The material covers the mathematical range and content of the pre-algebra courses prevalent at the secondary level. The developmental exercises gives ample opportunity to improve computational skills through the motivation of practical applications in personal finance. *456 pp., $8.50*

ELEMENTS OF PRE-CALCULUS MATHEMATICS

By DANIEL M. DRIBIN, *The George Washington University.*

The primary purpose of this text is to provide a sound treatment of the material needed for the calculus, in one semester. The book covers the nature of the number and function concepts, the analytic geometry of the line in the plane, the elementary functions (algebraic, trigonometric, exponential and logarithmic) and their graphs, plane vectors, polar coordinates, and an introduction to the concept of differentiation. *274 pp., 162 illus., $6.95*

AN INTRODUCTION TO MATRICES AND LINEAR TRANSFORMATIONS

By JOHN H. STAIB, *Drexel Institute of Technology.*

This book is introductory in nature and is designed primarily as a one-semester, sophomore text in linear algebra for engineering and science students. The author has developed the material using a classroom style presentation, with all its informality and experimentation. Theoretical concepts are lavishly illustrated both by examples and by computational type exercises that relate directly to the theory.

336 pp., $8.95

ELEMENTARY GEOMETRY FOR TEACHERS

By MERLIN M. OHMER, *F.T. Nicholls State College.*

The primary purpose of this book is to train elementary and junior high school teachers of mathematics. The book is also intended to be useful to teachers engaged in self-study programs. It includes most of the topics recommended by CUPM for the Level I Geometry course and follows these recommendations very closely. *152 pp., $7.50*

ESSENTIALS OF ALGEBRA

By ROSS H. BARDELL and ABRAHAM SPITZBART, *University of Wisconsin, Milwaukee.*

Designed to fill the requirements of the student who begins his college mathematics with inadequate preparation, this book introduces algebra at a lower level and at a slower pace than in the usual college algebra course and brings the student in the span of one semester to the stage where he is prepared to continue in the study of mathematics. At each stage of the development, further material is introduced which may be properly studied with the principles presented up to that point.

264 pp., $6.95

Write for approval copies

Addison-Wesley
PUBLISHING COMPANY, INC.
Reading, Massachusetts 01867

THE SIGN OF EXCELLENCE