MATHEMATICS MAGAZINE

Index to Volume 29   September-October 1955 - May-June 1956

Articles by Title

Articles by Authors

Problems and Questions

Contributors

Numbers refer to pages. Bold Type indicates a problem solved and solution published; italics, a problem solved but solution not published; ordinary type, a problem proposed.

Solutions

The page on which a solution appears is in the parentheses following the number of the problem.

Quickies

Trickies

Vol. 30, No. 1, Sept.-Oct. 1956

MATHEMATICS magazine

MATHEMATICS MAGAZINE

Formerly National Mathematics Magazine, founded by S.T. Sanders.

EDITORIAL STAFF

W. E. Byrne
Homer W. Craig
Rene Maurice Frechet
R. F. Horton
D. H. Hyers
Glenn James
N. E. Nörlund
A. W. Richeson
C. K. Robbins
Nilos Sakellariou
Joseph Seidlin
C. N. Shuster
C. D. Smith
Marion F. Stark
V. Thebault
C. W. Trigg
S. T. Sanders (emeritus)

Executive Committee:

D.H. Hyers, University of Southern California, Los Angeles, 7, Calif.
Glenn James, Managing Editor, 14068 Van Nuys Blvd., Pacoima, Calif.

Address editorial correspondence to Glenn James, special papers to the editors of the departments for which they are intended, and general papers to a member of the executive committee.

Manuscripts should be typed on 8½" x 11" paper, double-spaced with 1" margins. We prefer that, in technical papers, the usual introduction be preceded by a *Foreword* which states in simple terms what the paper is about.

The Mathematics Magazine is published at Pacoima, California by the managing editor, bi-monthly except July-August. Ordinary subscriptions are 1 yr. $3.00; 2 yrs. $5.75; 3 yrs. $8.50; 4 yrs. $11.00; 5 yrs. $13.00. Sponsoring subscriptions are $10.00; single copies 65¢. Reprints, bound 1¢ per page plus 10¢ each provided your order is placed before your article goes to press.

Subscriptions and related correspondence should be sent to Inez James, 14068 Van Nuys Blvd., Pacoima, California.

Entered as second-class matter March 23, 1948 at the Post Office Pacoima, California, under act of Congress of March 8, 1876.

SPONSORING SUBSCRIBERS

Hubert A. Arnold
E.F. Beckenbach
H.W. Becker
Clifford Bell
Raymond F. Bell
Frank Boehm
H.V. Craig
Joseph H. Creely
Paul H. Daus
Alexander Ebin
Theodore M. Edison
Henry E. Fettis
Curtis M. Fulton
J. Ginsberg
Merton T. Goodrich
Reino W. Hakala
M.R. Hestenes
Robert B. Herrera
Donald H. Hyers
Glenn James
Robert C. James
A.L. Johnson
Philip B. Jordain
John Kronsbein
Lillian R. Lieber
E.A. Petterson
Earl D. Rainville
John Teckzeh
Francis Regan
Charles K. Robbins
L.R. Robinson
S.T. Sanders
C.N. Shuster
H.A. Simmons
D. Victor Steed
E.M. Tingley
Morris E. Tittle
H.S. Vandiver
Alan Wayne

MATHEMATICS MAGAZINE

Vol. 30, No. 1, Sept.-Oct. 1956

CONTENTS

* * * * * * * * *

COUNTRIES IN WHICH THE MATHEMATICS MAGAZINE HAS SUBSCRIBERS *

Argentina	England	New Zealand	Spain
Australia	Formosa	Norway	Scotland
Belgium	France	Newfoundland	South Africa
Brazil	Germany	Nicaragua	Sweden
British West Indias	Greece	Nova Scotia	Switzerland
Canada	India	Peru	Thailand
Chile	Irak	Phillipine Islands	The Netherlands
China	Italy	Poland	Turkey
Colombia	Japan	Republic Populaire Romaine	U.S.
Cuba	Malaya	Ryukyus Islands	U.S.S.R.
Denmark	Mexico		Uruguay
Eire	Morrocco		Venezuela
			Yougaslavia

**Published by request.*

The First in a Series of Announcements on Progressive Expansion of Program and Facilities in Mathematics at the Knolls Atomic Power Laboratory:

GENERAL ELECTRIC'S
KNOLLS ATOMIC POWER LABORATORY

Announces

CONSTRUCTION OF A MODERN CENTER FOR MATHEMATICS

Because we believe that theory is our most powerful weapon in dealing with reality, we are expanding our Mathematical Analysis Program. One of the first elements in this expansion is the creation of a new and modern building for mathematicians and physicists, which will be the center of the Laboratory's efforts to meet by theoretical means the challenges of the nuclear energy field.

We are seeking men with strong mathematical training at all degree levels to participate in this expanding Numerical Analysis Program—a program growing not only in staff, equipment, and facilities, but also in concept and function. They will work in close association with our theoretical and experimental physicists. There are openings in each of the following fields:

RESEARCH IN MATHEMATICAL TECHNIQUES

Numerical solution of the diffusion equation for complicated geometrical arrays taxes even the most powerful electronic computers. Fundamental work in iterative techniques must be carried out.

FORMULATION AND EVALUATION OF THEORIES

Due to the nature of physical situations now being encountered, the rough approximations which were formerly adequate must now be improved. The ultimate test of such improvement is comparison with experiment.

APPLICATIONS TO REACTOR PROBLEMS

A broad program of computational tools for reactor design must be effected incorporating the best available techniques. Strong interests in computation and in machine properties are indicated. The program at Knolls offers the atmosphere, the equipment, the richness of subject matter and the material benefits conducive to a satisfying career in applications of mathematics.

A LETTER TO DR. S. R. ACKER, EXPRESSING YOUR INTEREST, WILL RECEIVE IMMEDIATE ATTENTION.

Knolls Atomic Power Laboratory

GENERAL ELECTRIC

SCHENECTADY, N. Y.

A DEVELOPMENT OF ASSOCIATIVE ALGEBRA AND AN ALGEBRAIC THEORY OF NUMBERS, IV

H. S. Vandiver and M. W. Weaver

Introduction: Three preceding papers under the above title have been published in this magazine. The first, (I), appeared in vol. 25, 233-250 (1952); the second, (II), appeared in Vol. 27, 1-18 (1953). Both of these were under the authorship of Vandiver. The third, (III) appeared in Vol. 29 135-149 (1956). In (I), foundations of ordinary algebra were developed from a standpoint which also yielded foundations for an infinity of finite algebras. In (II), foundations for the classical theory of algebraic numbers were discussed. In (III), an introduction to a theory of generalized substitutions (correspondences) was given, and properties were extracted from *semi-groups* of correspondences. These properties were used as defining postulates for abstract semi-groups.

In the present paper, we shall first discuss homomorphisms of an additive semi-group into itself. We shall extract properties from *semi-rings* of homomorphisms and use them as defining postulates for abstract semi-rings. Thus the procedure parallels that used in (III). Finally we shall discuss a homomorphism theorem of semi-rings which is due to S. Bourne.[1] Some well known theorems and slight generalizations of well known theorems are included among the problems stated in this present paper.

The work on this paper was done under National Science Foundation Grant G1397.

We are indebted for suggestions on and corrections to the material in this paper to F. C. Biesele, Anne Breese Barnes, A. Church O.B.Faircloth, R.P. Kelisky, C.A. Nicol, T.B. Pitts, and P.H. Thrower.

Semi-rings of endomorphisms on additive semi-groups.

In (III) we preceded our study of semi-groups, algebraic systems with one operation, by a study of *semi-groups* of correspondences and pointed out, in problem 29, that each finite semi-group is isomorphic to a semi-group of correspondences. We now wish to discuss a type of system with two operations. We will again start with a particular example.

Let A be a finite Abelian semi-group with operation $+$; consider the set R of endomorphisms (homomorphisms of A into itself) on A. We give to R the properties (using the notation of (III)):

---

1. *On the Homomorphism Theorem for Semirings*, Proc. Nat'l. Acad. Sci., Vol. 38, 119 (1952).

(i) If E_1, $E_2 \in R$, x varies over A, and $(E_1 + E_2)[x]$ means $E_1 + E_2$ applied to x, then $E_1 + E_2$ is defined by

$$(E_1 + E_2)[x] = E_1[x] + [E_2]x.$$

(ii) Under the hypothesis of (i), $E_1 \times E_2$ is defined by

$$E_1 \times E_2[x] = E_2 \quad [E_1[x]]:$$

A subset R' of R is called a *semi-ring of endomorphisms on* A if R' obeys: $E_1 + E_2 \cong u$, $E_2 + E_1 \cong v$, $E_1 \times E_2 \cong w$, and $E_2 \times E_1 \cong x$ have solutions $u, v, w, x \in R'$, for each E_1, $E_2 \in R'$. The operation + is called addition, and the operation $\times$, multiplication. The reader should construct examples of the addition and multiplication tables of the sets of endomorphisms on Abelian semi-groups. For example he might construct such for the endomorphisms on the cyclic semi-group whose non-equivalent elements are a, a^2, a^3, where $a^4 \cong a^2$.

Problems

If R is a semi-ring of endomorphisms on the additive Abelian semi-group A, show that:

1. R with operation +, satisfies the semi-group postulates.
2. R with operation $\times$, satisfies the semi-group postulates.

Combinations in a Semi-ring

The definitions below pertaining to combinations are to be used for all systems S with two operations which appear in this paper.

Definition. Any of the elements of S or any symbols denoting any of them (excluding +, $\times$, $\cong$, and parenthesis symbols) is said to be a *combination*. If A denotes a combination and B also, then $A + B$ is said to be a combination, also $A \times B$, as well as (A). A *subcombination* of a combination A is a combination consisting of a symbol contained in A or else such a symbol followed by others in order as they appaar in A.

Definition. If A denotes a combination, then (A) is called a *parenthesis enclosed combination.*

Definition. A *closed combination* C is a combination such that if any + sign occurs in it, there is a subcombination of C which contains this + sign, and which is also a parenthesis enclosed combination. If a combination contains no plus sign, it is said to be closed.

An alternative definition of combination is as follows: Consider a finite sequence of symbols containing only symbols of the following type: symbols (letters) denoting elements of S, symbols of conjunction + and $\times$, parenthesis symbols (and) which will be called a *left parenthesis symbol* (abbreviated L.P.S.) and a *right parenthesis symbcl* (abbreviated R.P.S.), respectively, and such that:

1. It contains at least one symbol denoting an element of S.
2. *It* begins with either a L.P.S. or a symbol denoting an element of S and ends with either a R.P.S. or a symbol denoting an element of S.
3. It has no L.P.S. immediately preceding a symbol other than another L.P.S. or a symbol denoting an element of S and no R.P.S. immediately preceded by a symbol other than a R.P.S. or a symbol denoting an element of S.
4. Any two successive symbols denoting elements of S are separated by just one symbol of conjunction.
5. The instances of the symbols (and) can be paired into sensed pairs (,).

The ordered set just described is said to be a *combination*. Further, if we replace any of the symbols denoting elements in S, which appear in the combination just mentioned, by symbols denoting combinations, the resulting set is also said to be a combination.

We return to the study of each semi-ring S of endomorphisms on each commutative additive semi-group A. We wish to obtain an endomorphism which is equivalent to a given combination on the semi-ring S, and to be able to substitute in equivalences involving combinations as we do in ordinary algebra. We recall that in the algebras of double composition in (I), we were able to do this by assuming three substitution postulates. We note that postulate 1 below holds for semi-rings of endomorphisms. Hence we assume that postulates 2 and 3 below hold for semi-rings of endomorphisms. These three postulates are re-statements of those used in (I).

Problem

3. Verify that postulates 6 and 7 below hold for semi-rings of endomorphisms; but that the A.S.G. of such a semi-ring is commutative.

S. Bourne[2] first noted the truth of the statements in Problems 1, 2, and 3.

Abstract semi-rings

Let S be a set of elements such that operation symbols $+$ and $\times$ and an equivalence symbol, $\cong$, are related to the elements of S. Combinations and elements[3] of S, $+$, $\times$, and $\cong$ are given meaning only by the

2. *The Jacobson Radical of a Semiring*, Proc. Nat'l. Acad. Sci., Vol.37 164 (1951).

3. Unless otherwise noted, capital letters will be used in the rest of this paper to denote combinations. This includes the use of capital letters to denote elements of S. If we mean to denote only an element of S, we shall use small letters. $a \in B$ shall be used to mean that either a is an element of the set B or that a denotes an element of the set B. We remark that for our purposes an element may denote itself.

postulates below. We extract the following properties from semi-rings of endomorphisms and use them as a set of postulates for S.

Postulate 1. (Identity) $A \cong A$.

Postulate 2. (Parenthesis) $(A) \cong A$.

Postulate 3. (Substitution) If $A \cong B$ and $D \cong C$, where C is a subcombination of B and B' is the combination obtained from B by putting D in place of C, then $B' \cong A$, provided that if C is immediately preceded by or immediately succeeded by $\times$ in B, then C and also D are closed combinations.

Postulate 4. (Additive Closure) If a and b are elements of S, then an element d exists, $d \in S$, such that $a + b \cong d$.

Postulate 5. (Multiplicative Closure) If a and b are elements of S, then an element k exists, $k \in S$, such that $a \times b \cong k$.

Postulate 6. (Distributive Law) If a, b, and k are elements of S, then $a \times (b + k) \cong a \times b + a \times k$, and $(b + k) \times a \cong b \times a + k \times a$.

Postulate 7. There exists a relationship, $\ncong$, called "not equivalent to", such that if a and b are elements of S then either $a \cong b$ or $a \ncong b$, these conditions being mutually exclusive.

In view of our definition of semi-group, a convenient way of defining a system S which amounts to the above is to say that *S forms a semi-group under addition, a semi-group under multiplication, and that postulates* 1, 2, 3, *and* 6 *hold.*

THEOREM 1. (Symmetry) If $A \cong B$, then $B \cong A$.

THEOREM 2. (Transitivity) If $A \cong B$ and $B \cong C$, then $A \cong C$.

THEOREM 3. (Composition under addition) If $A \cong B$ and $C \cong D$, then $A + C \cong B + D$.

THEOREM 4. (Composition under multiplication) If $A \cong B$ and $C \cong D$, and if A, B, C, and D are closed combinations, then $A \times C \cong B \times D$.

THEOREM 5. (General substitution) If $E \cong F$ and $G \cong H$, where G is a subcombination of E, and E' is the combination obtained from E by putting H in place of G, then $E' \cong F$ provided that if G is immediately preceded by or immediately succeeded by a $\times$ sign in E, then G and H must be closed combinations. Similarly, if G is a subcombination of F and F' is obtained from F by putting H in place of G, then $E \cong F'$ with the above mentioned restrictions on G and H.

THEOREM 6. If A is a combination, then an element of S denoted by c may be determined so that $A \cong c$.

THEOREM 7. (Associative law of addition) $(A + B) + D \cong A + (B + D)$.

THEOREM 8. (Associative law of multiplication). $(A \times B) \times D \cong A \times (B \times D)$, where A, B, and D are closed combinations.

As we have already noted, a semi-ring forms a semi-group under addition and a semi-group under multiplication, and postulates 1,2,3, and 6 hold. We shall use the abbreviations A.S.G. and M.S.G., respectively, for the additive and multiplicative semi-groups just mentioned.

Two semi-rings S_1 and S_2 are said to be *homomorphic* if there exists a mapping M of S_1 onto S_2 such that M is a *homomorphism* of the A.S.G. of S_1 onto S_2 and M is a homomorphism of the M.S.G. of S_1 onto S_2. If the mapping is one to one reversible then S_1 is said to be *isomorphic* to S_2, and M is said to be an *isomorphism*. The semi-ring S_3 is said to be *embedded* in the semi-ring S_4 if S_3 is isomorphic to a subset of S_4.

If the A.S.G. of a semi-ring S is an abelian group, then we say that S is a *ring*, and algebraic system which has been extensively studied. We note that the natural numbers form a semi-ring if we now interpret + as ordinary addition, $\times$ as ordinary multiplication, and $\cong$ as =. By adjoining zero and the negative integers to the natural numbers, as we did in (III), we obtain a semi-ring in which the additive group is an Abelian group so that our original semi-ring turns out to be embedded in a ring. *However, we shall point out that this is not possible for all semi-rings; hence, the ring is not the fundamental system for associative algebra of double composition.* For, consider the set (3). We showed that this set formed a semi-ring. We also showed, however, by assuming in (3) of (I) that C, $i = 1,2,\ldots 6$ are unequal and that $C_7 = C_3$. It follows that $C_6 + C_1 = C_2 + C_1$; yet we cannot cancel the C_1's. Now, if it were possible to embed this particular semi-ring S_1 in a ring R the A.S.G. of R would be a group and would include the A.S.G. of S_1 as a subgroup. However, the cancellation law holds for all the elements of a group; so this gives a contradiction. Hence we may state the

THEOREM 9. A semi-ring exists which cannot be embedded in any ring whatsoever.

The above theorem may be proved in a different way be starting with the natural numbers themselves and the familiar algebra governing them as we shall now explain. Consider the natural numbers and introduce a relation between them called (i,j) *equivalence*, where $j \geq i$. We denote the equivalence by $\cong$ as usual and define it as follows (each letter denotes a natural number): If $a < i$, then $a \cong b$, if and only if $a = b$; if $a \geq i$ and $b \geq i$, then $a \cong b$ if and only if $a \equiv b \pmod{m}$, where $m = j - i + 1$. Addition and multiplication yield the same elements as in ordinary arithmetic, except that in an (i,j) algebra we can "reduce" elements greater than j.

In view of the above there are exactly j natural numbers which are not (i,j) equivalent, namely 1, 2, ..., j. (This idea of (i,j) equivalence is due to A. Church and was communicated to Vandiver in a conversation which took place in the year 1934, (approximately). The additive cancellation law does not hold in an (i,j) algebra with $i > 1$; for if $j > i > 1$ and $i = k + 1$, it follows that $j + 1 \cong k + 1$, but $j \neq k$.

We have already noted that the set of rational integers forms a ring. If we adjoin the rational fractions to this ring, we obtain a ring in which the M.S.G., zero excluded, form an Abelian group. Such a semi-ring is called a *field*.

Problems

4. Show that we may obtain a theorem by substituting, in postulate 4, "combinations A, B, and D" for "elements a, b, and d," respectively; and also that we may obtain two other theorems by substituting "closed combinations" for "elements" in postulates 5 and 6.

5. If the A.S.G. of a semi-ring S is a skew-group, that is, a group in which the cancellation law holds, both left and right, and the M.S.G. of S has a left-identity element, then addition is commutative in S.

6. Each commutative semi-ring S may be embedded in a commutative semi-ring S' such that the cancellable elements in the M.S.G. of S (if they exist) are embedded in a group contained in the M.S.G. of S'.

7. If we exclude zero from the set of rational integers, any semi-ring contained in this system is contained in the set of positive integers.

8. How must a commutative semi-ring R be restricted so that it is possible to embed R in a ring?

9. Prove Theorem 9 in another manner by setting up a semi-ring in which addition is noncommutative. (Examples of such semi-rings were found by Olga Taussky-Ph. Furtwängler; and by H.S. Vandiver.)

The homomorphism theorem for semi-rings.

In the rest of the paper, each semi-ring S discussed is assumed to contain an element, 0, called the *zero* element such that if $s \in S$, then $s + 0 \cong s$ and $s \times 0 \cong 0 \cong 0 \times s$, and furthermore the A.S.G. of S is assumed to be commutative.

I is an *ideal* of the semi-ring S provided that for each i_1, i_2, I, there exists an $i_3 \in I$ such that $i_1 + i_2 \cong i_3$ and that for each $s_1 \in S$, there exist i_4, $i_5 \in I$ such that $s_1 \times i_1 \cong i_4$ and $i_1 \times s_1 \cong i_5$

Let H be a homomorphism of the semi-ring S with zero, 0, onto the semi-ring S', with zero, $0'$; then the set K of elements of S, such that from $k \in K$, it follows that $H[k] \cong 0$, is called the *kernel* of H. Furthermore if K consists of the element $0'$ alone, H is called a semi-isomorphism of S onto S', and S is said to be *semi-isomorphic* to S'.

Let I be an ideal of the semi-ring S and let $s_1, s_2 \in S$. Then s_1 is said to be *equivalent to* s_2 *modulo* I if there exist $i_1, i_2 \in I$ such that $s_1 + i_1 \cong s_2 + i_2$. We may describe this relationship by

$$s_1 \equiv s_2 \pmod{I}.$$

The set C_1 of elements of S which are equivalent modulo I is called a *coset of* S *relative to* I. We note that the cosets of S relative to I exhaust the elements of S and that each two of these cosets either are identical or have no elements in common. If a coset C_1 contains the same elements as the coset C_2, we write $C_1 = C_2$; otherwise, $C_1 \neq C_2$. Let $c_1 \in C_1$ and $c_2 \in C_2$, and $c_1 + c_2 \cong c_3$ and $c_1 \times c_2 \cong c_4$; then if $c_3 \in C_3$ and $c_4 \in C_4$, $C_1 + C_2$ and $C_1 \times C_2$ are defined respectively by

$$C_1 + C_2 = C_3 \text{ and } C_1 \times C_2 = C_4$$

(C_1) is defined as the set (c) where c varies over the elements of C_1. We replace each coset of any combination L on the set of cosets of S relative to I by elements of S, thus getting a combination L' on elements of S such that $L' \cong s$, $s \in S$. We define the combination L as being equivalent to the coset which contains s.

Problems

10. Each ideal of a semi-ring is itself a semi-ring.

11. The zero element of each semi-ring S is contained in each ideal of S.

12. Prove that if S is a semi-ring, s , s , s S, and I is an ideal of S, then

   a. $s_1 \equiv s_1 \pmod{I}$.
   b. If $s_1 \equiv s_2 \pmod{I}$, then $s_2 \equiv s_1 \pmod{I}$.
   c. If $s_1 \equiv s_2 \pmod{I}$ and $s_2 \equiv s_3 \pmod{I}$, then $s_1 \equiv s_3 \pmod{I}$.

13. If I is an ideal of the semi-ring S, then the cosets of S relative to I form a semi-ring. (We denote it by $S - I$).

14. If I is an ideal of the semi-ring S, then S is homomorphic to the semi-ring $S - I$. If $C_1 \in S - I$ and $c_1 \in C_1$, and the homomorphism is denoted by H, then $H[c_1] = C_1$.

15. If H is a homomorphism which maps the semi-ring S onto the semi-ring S' with zero element $0'$, and $H[I] = 0$, then I is an ideal, and H is a homomorphism of $S - I$ onto S'.

16. If I is an ideal of S then I is the zero element of $S - I$.

The homomorphism theorem of S. Bourne, mentioned in the introduction, follows from problems 14,15, and 16.

If I is an ideal of S then S is homomorphic to the difference semi-ring $S - I$. Conversely, if the semi-ring S is homomorphic to the semi-ring S', then the difference semi-ring $S - I$ is semi-isomorphic to S', where I is the ideal of elements mapped onto the zero element of S'.

Added in Proof. Dr. Bourne has kindly pointed out to us the following two references on the subject of semi-rings:

W. Slowikowski and W. Zawadowski, *A Generalization of the maximal ideals method of Stone and Gelfand,* FUNDAMENTA MATHEMATICAE, Vol 42,2, 215-231 (1955).

K. Iseki and Y. Miyanaga, *Notes on Topological Spaces* III. *On the space of maximal ideals in a semi-ring.* PRO. ACAD. SCI. OF JAPAN, Vol 32, 5, 325-328 (May, 1956).

The University of Texas

MODULATION PRODUCTS IN POWER-LAW DEVICES

H. Kaufman

Foreword

An analysis is made of a biased power-law device with a two-frequency input. The modulation products are the coefficients $A_{mn}^{(\nu)}(h,k)$ in the double Fourier series expansion of the output of such a device. Recurrence relations are established among the modulation products produced by a given ν-th law device and among the products produced by devices with different power-law characteristics. Modulation products associated with positive bias values are related to those associated with negative bias values.

Introduction

In a previous paper [1] a study was made of the relations among the harmonics in the output of a biased ν-th law device with a single frequency input. The object of the present paper is to derive similar relations for the modulation products in the output of a biased ν-th law device with a two-frequency input. The relations thus obtained include as special cases those for the biased linear rectifier given by Bennett [2] and Sternberg and Kaufman [3], and those for the unbiased ν-th law rectifier given by Sternberg, Shipman and Kaufman [4].

Analysis of Power-Law Characteristic

The basic definitions for the biased linear rectifier [3, pp. 236-239] are restated here in a form suitable to the analysis of the biased ν-th law rectifier. Consider a device whose output versus input characteristic is defined by

$$(1) \qquad Y(X;X_0) = \begin{cases} (X-X_0)^{\nu}, & X > X_0 \\ 0 \quad , & X \le X_0 \end{cases}$$

where ν is a nonnegative real number. Let the input $x(t)$ be given by

$$(2) \quad x(t) = P\cos(pt+\theta_p) + Q\cos(qt+\theta_q), \quad 0 < P < P+Q \le 2P$$

With the output $y(t) \equiv Y(x(t);X_0)$ is associated a double Fourier series

$$(3) \qquad y(t) = \tfrac{1}{2}C_{00} + \sum_{m,n=0}^{\infty}{}' C_{\pm mn}\cos(\omega_{\pm mn}t + \phi_{\pm mn})$$

where

(4) $\omega_{\pm mn} = mp \pm nq, \quad \phi_{\pm mn} = m\theta_p \pm n\theta_q, \quad (m,n = 0,1,2,\ldots)$

The symbol Σ' denotes that the summation extends over both the upper and lower signs when $m.n \neq 0$, and over the upper sign only when $m.n = 0$ with the exception that the term corresponding to $m = n = 0$ is not included in the summation.

The coefficients in (3) are given by

(5) $$C_{\pm mn} = \frac{1}{2\pi^2}\int_{-\pi}^{\pi}\int_{-\pi}^{\pi} f(u,v)\cos(mu \pm nv)\,du\,dv$$

where

(6) $$f(u,v) = Y(P\cos u + Q\cos v;\ X_0)$$

Introducting the parameters $h = X_0/P$, $k = Q/P$

(7) $$f(u,v) = \tfrac{1}{2}P^{\nu}A_{00}^{(\nu)}(h,k) + P^{\nu}\sum_{m,n=0}^{\infty}{}' A_{mn}^{(\nu)}(h,k)\cos(mu \pm nv)$$

where

(8) $$A_{\pm mn}^{(\nu)}(h,k) = [1/(2\pi^2P^{\nu})]\int_{-\pi}^{\pi}\int_{-\pi}^{\pi} f(u,v)\cos(mu \pm nv)\,du\,dv \qquad (m,n = 0,1,2,\ldots)$$

The double sign can be dropped since $A_{+mn}^{(\nu)}(h,k) = A_{-mn}^{(\nu)}(h,k)$.

The following five cases, defined by different values of h and k, must be considered [2, §4]:

(9) $$\text{(o)}\ h - k \geq 1, \quad \text{(i)}\begin{cases} h - k < 1 \\ h + k > 1\end{cases}, \quad \text{(ii)}\begin{cases} h - k \geq -1 \\ h + k \leq 1\end{cases}$$

$$\text{(iii)}\begin{cases} h - k < -1 \\ h + k > -1\end{cases}, \quad (\infty)\ h + k \leq -1$$

In case (o)

(10) $$A_{mn}^{(\nu)}(h,k) = 0, \qquad (m,n = 0,1,2,\ldots).$$

In cases (i), (ii) and (iii) $A_{mn}^{(\nu)}(h,k)$ can be expressed in either of the forms

(11) $$A_{mn}^{(\nu)}(h,k) = (2/\pi^2)\int_a^b R_m^{(\nu)}(v)\cos nv\,dv + (2/\pi^2)\int_0^a \overline{R}_m^{(\nu)}(v)\cos nv\,dv$$

(12)
$$A_{mn}^{(\nu)}(h,k) = (2/\pi^2)\int_{\alpha}^{\beta} S_n^{(\nu)}(u)\cos mu\,du + (2/\pi^2)\int_0^{\alpha} \overline{S}_n^{(\nu)}(u)\cos mu\,du$$
$(m,n = 0,1,2,\ldots)$

where in all three cases

(13)
$$\begin{cases} R_m^{(\nu)}(v) = \int_0^{c(v)} (\cos u + k\cos v - h)^{\nu}\cos mu\,du, & (m = 0,1,2,\ldots) \\ \overline{R}_m^{(\nu)} = \int_0^{\pi} (\cos u + k\cos v - h)^{\nu}\cos mu\,du, & (m = 0,1,2,\ldots) \end{cases}$$

(14)
$$\begin{cases} S_n^{(\nu)}(u) = \int_0^{\gamma(u)} (\cos u + k\cos v - h)^{\nu}\cos nv\,dv, & (n = 0,1,2,\ldots) \\ \overline{S}_n^{(\nu)}(u) = \int_0^{\pi} (\cos u + k\cos v - h)^{\nu}\cos nv\,dv, & (n = 0,1,2,\ldots) \end{cases}$$

(15) $c(v) = \cos^{-1}(h - k\cos v)$

(16) $\gamma(u) = \cos^{-1}(h' - k'\cos u)$

(17) $h' = h/k, \quad k' = 1/k$

and a, b, α, β, are defined in the three cases by

(i) $a = 0,\ b = \cos^{-1}(h' - k'),\ \alpha = 0,\ \beta = \cos^{-1}(h - k)$

(18) (ii) $a = 0,\ b = \pi,\ \alpha = \cos^{-1}(h + k),\ \beta = \cos^{-1}(h - k)$

(iii) $a = \cos^{-1}(h' + k'),\ b = \pi,\ \alpha = \cos^{-1}(h + k),\ \beta = \pi$.

Note that the second integral in eq. (11) is zero in cases (i) and (ii) for all m, n, and the second integral in eq. (12) is zero in case (i) for all m, n.

In case (∞)

(19)
$$A_{mn}^{(\nu)}(h,k) = (2/\pi^2)\int_0^{\pi} \overline{R}_m^{(\nu)}(v)\cos nv\,dv$$
$$A_{mn}^{(\nu)}(h,k) = (2/\pi^2)\int_0^{\pi} \overline{S}_n^{(\nu)}(u)\cos mu\,du$$
$(m,n = 0,1,2,\ldots)$

Lampard [5] has given an explicit expression for $A_{mn}^{(\nu)}(h,k)$, in case (∞), in terms of Appell's fourth type of hypergeometric function of two variables.

Recurrence Relations

From the definition of $R_m^{(\nu)}(v)$ and $S_n^{(\nu)}(u)$ integration by parts gives

(20) $$(m-\nu-1)R_{m-1}^{(\nu)} - 2m(h-k\cos v)R_m^{(\nu)} + (m+\nu+1)R_{m+1}^{(\nu)} = 0 \qquad (m=1,2,3,\ldots)$$

(21) $$(n-\nu-1)S_{n-1}^{(\nu)} - 2n(h'-k'\cos u)S_n^{(\nu)} + (n+\nu+1)S_{n+1}^{(\nu)} = 0 \qquad (n=1,2,3,\ldots)$$

where $R_m^{(\nu)} \equiv R_m^{(\nu)}(v)$, $S_n^{(\nu)} \equiv S_n^{(\nu)}(u)$. The same relations are satisfied by $\overline{R}_m^{(\nu)}(v)$ and $\overline{S}_n^{(\nu)}(u)$.

The definitions of $A_{mn}^{(\nu)}(h,k)$ then lead to the following set of recurrence relations valid in all five cases

(22a)
$$(m-\nu-1)A_{m-1,0}^{(\nu)} - 2mhA_{m0}^{(\nu)} + 2mkA_{m1}^{(\nu)} + (m+\nu+1)A_{m+1,0}^{(\nu)} = 0 \qquad (m=1,2,3,\ldots)$$

(22b)
$$(n-\nu-1)A_{0,n-1}^{(\nu)} - 2nh'A_{0n}^{(\nu)} + 2nk'A_{1n}^{(\nu)} + (n+\nu+1)A_{0,n+1}^{(\nu)} = 0 \qquad (n=1,2,3,\ldots)$$

(22c)
$$(m-\nu-1)A_{m-1,n}^{(\nu)} - 2mhA_{mn}^{(\nu)} + mkA_{m,n+1}^{(\nu)} + mkA_{m,n-1}^{(\nu)} + (m+\nu+1)A_{m,n+1}^{(\nu)} = 0 \qquad (m,n=1,2,3,\ldots)$$

(22d)
$$(n-\nu-1)A_{m,n-1}^{(\nu)} - 2nh'A_{mn}^{(\nu)} + nk'A_{m+1,n}^{(\nu)} + nk'A_{m-1,n}^{(\nu)} + (n+\nu+1)A_{m,n+1}^{(\nu)} = 0 \qquad (m,n=1,2,3,\ldots)$$

where $A_{mn}^{(\nu)} \equiv A_{mn}^{(\nu)}(h,k)$. Thus, for case (i), equations (22a), (22b) are obtained on integrating (20) between limits a and b, and (21) between limits α and β, where a, b, α, β, are defined in (18). A similar integration, with (20) multiplied by $\cos nv$ and (21) by $\cos mu$, yields equations (22c) and (22d). Proofs for the other cases follow along the same lines.

For purposes of computation, the following relations, derived from equations (22), are convenient

(23a)

$$(m-n+\nu+3)\,A^{(\nu)}_{m+2,n-1} = -(m+n-\nu-1)\,A^{(\nu)}_{m,n-1} - 2(m+1)\,kA^{(\nu)}_{m+1,n} + 2(m+1)\,hA^{(\nu)}_{m+1,n-1}$$
$$(m = 0,1,2,\ldots;\ n = 1,2,3,\ldots)$$

(23b)

$$(m+n+\nu+1)\,A^{(\nu)}_{m+1,n} = -(m-n-\nu-1)\,A^{(\nu)}_{m-1,n} - 2mk\,A^{(\nu)}_{m,n-1} + 2mhA^{(\nu)}_{mn}$$
$$(m,n = 1,2,3,\ldots)$$

(23c)

$$(n+m+\nu+1)\,A^{(\nu)}_{m,n+1} = -(n-m-\nu-1)\,A^{(\nu)}_{m,n-1} - 2n\,k'A^{(\nu)}_{m-1,n} + 2nh'A^{(\nu)}_{mn}$$
$$(m,n = 1,2,3,\ldots)$$

(23d)

$$(n-m+\nu+3)\,A^{(\nu)}_{m-1,n+2} = -(n+m-\nu-1)\,A^{(\nu)}_{m-1,n} - 2(n+1)\,k'A^{(\nu)}_{m,n+1} + 2(n+1)\,h'A^{(\nu)}_{m-1,n+1}$$
$$(m = 1,2,3,\ldots;\ n = 0,1,2,\ldots)$$

Equations (23a) for $n = 1$ and (23d) for $m = 1$ follow at once from (22a) (with m replaced by $m+1$) and (22b) (with n replaced by $n+1$). The remaining relations (23a) to (23d) are obtained from (22c) and (22d) by eliminating in turn $A^{(\nu)}_{m,n-1}$, $A^{(\nu)}_{m,n+1}$, $A^{(\nu)}_{m+1,n}$, and $A^{(\nu)}_{m-1,n}$, with appropriate renumbering of subscripts.

Relations between Modulation Products for Different Power-Law Devices

From the definition of $R_m^{(\nu+1)}(v)$ we obtain

(24) $$2R_m^{(\nu+1)} = R^{(\nu)}_{m-1} - 2(h-k\cos v)\,R^{(\nu)}_m + R^{(\nu)}_{m+1}, \qquad (m = 1,2,3,\ldots)$$

whence, combining (24) with (20)

(25) $$2mR_m^{(\nu+1)} = (\nu+1)R^{(\nu)}_{m-1} - (\nu+1)\,R^{(\nu)}_{m+1} \qquad (m = 1,2,3,\ldots)$$

The corresponding relation for $S_n^{(\nu+1)}(u)$ is

(26) $$2nS_n^{(\nu+1)} = k(\nu+1)\,S^{(\nu)}_{n-1} - k(\nu+1)\,S^{(\nu)}_{n+1}, \quad (n = 1,2,3,\ldots)$$

The same relations hold for $\overline{R}_m^{(\nu+1)}$ and $\overline{S}_n^{(\nu+1)}$, $(m,n = 1,2,3,\ldots)$.

In addition

$$(27)\quad \begin{cases} R_0^{(\nu+1)} = R_1^{(\nu)} - (h - k \cos v)R_0^{(\nu)} \\ \overline{R}_0^{(\nu+1)} = \overline{R}_1^{(\nu)} - (h - k \cos v)\overline{R}_0^{(\nu)} \end{cases}$$

The definitions of $A_{mn}^{(\nu)}(h,k)$ then lead to the following relations valid in all five cases

$$(28a)\quad A_{00}^{(\nu+1)} = A_{10}^{(\nu)} + kA_{01}^{(\nu)} - hA_{00}^{(\nu)}$$

$$(28b)\quad 2mA_{mn}^{(\nu+1)} = (\nu + 1)\, A_{m-1,n}^{(\nu)} - (\nu + 1)\, A_{m+1,n}^{(\nu)}$$
$$(m = 1,2,3,\ldots;\ n = 0,1,2,\ldots)$$

$$(28c)\quad 2nA_{mn}^{(\nu+1)} = k(\nu + 1)\, A_{m,n-1}^{(\nu)} - k(\nu + 1)\, A_{m,n+1}^{(\nu)}$$
$$(m = 0,1,2,\ldots;\ n = 1,2,3,\ldots)$$

Thus in case (i), equation (28a) is obtained by integrating the first equation in (27) between limits a and b specified by (18). Equations (28b) and (28c) are obtained on multiplying (25) by $\cos nv$, (26) by $\cos mu$, and integrating between the appropriate limits. Proofs for the other cases are similarly established.

Reflection Relations

Equations (4.8) of [3] relate $A_{mn}^{(1)}(h,k)$ to $A_{mn}^{(1)}(-h,k)$. We generalize these results for the functions $A_{mn}^{(\nu)}(h,k)$. Noting that when h is replaced by $-h$, $(h > 0)$, case (i) is carried into case (iii) and case (ii) is carried into case (ii), the following relation is readily established

$$(29)\quad A_{mn}^{(\nu)}(-h,k) = \hat{A}_{mn}^{(\nu)}(-h,k) + (-1)^{m+n+\nu+1} A_{mn}^{(\nu)}(h,k),$$
$$(m,n = 0,1,2,\ldots)$$

where

$$\hat{A}_{mn}^{(\nu)}(h,k) = (2/\pi^2)\int_0^{\pi}\int_0^{\pi}(\cos u + k\cos v - h)^{\nu} \cos mu \cos nv \, du\, dv.$$

Note that $\hat{A}_{mn}^{(\nu)}(h,k)$ is not in case (∞), despite the appropriate limits of integration, since the parameters h, k do not satisfy the conditions of that case.

Verification for $\nu = 1$ [3, eqs. (4.8)] is immediate, on recalling that $\hat{A}^{(1)}_{00}(-h,k) = 2h$, $\hat{A}^{(1)}_{10}(-h,k) = 1$, $\hat{A}^{(1)}_{01}(-h,k) = k$, $\hat{A}^{(1)}_{mn}(-h,k) = 0 \quad (m + n = 2,3,4,\ldots)$.

The above relation can easily be extended to more complicated types of characteristic. Thus if, in the integrals defining A_{mn} for the various cases, the function $(\cos u + k \cos v - h)^{\nu}$ is replaced by a function $F(\cos u + k \cos v - h)$ where $F(z)$ is either an even or an odd function of z; i.e., $F(-z) = \rho F(z)$ where $\rho = 1$ or -1 according as $F(z)$ is even or odd, then

$$(30) \qquad A_{mn}(-h,k) = \hat{A}_{mn}(-h,k) + (-1)^{m+n+1}\rho A_{mn}(h,k).$$

A proof of (30) is given in the Appendix. For the ν-th law characteristic $\rho = (-1)^{\nu}$.

Applications

The relations obtained in the preceding sections are of use in the computation of modulation products. The recurrence formulas (22) or (23) can be used to evalute the higher order functions $A^{(\nu)}_{mn}(h,k)$, $(m + n = 2,3,4,\ldots)$, in terms of the four lowest order functions $A^{(\nu)}_{00}(h,k)$ $A^{(\nu)}_{10}(h,k)$, $A^{(\nu)}_{01}(h,k)$, and $A^{(\nu)}_{11}(h,k)$. By means of (28) functions of the $(\nu+1)^{th}$ kind can be computed in terms of those of the ν^{th} kind. The reflection relations (29) are used in computing the functions for negative values of h in terms of those for positive h.

Acknowledgment

The author is indebted to Dr. R. L. Sternberg of Laboratory for Electronics, Inc., Boston, Mass. for valuable suggestions made during the course of a lengthy correspondence.

References

1. H. Kaufman, *Harmonic Distortion in Power-Law Devices*, Mathematics Magazine, 28, 245-250 (1955).

2. W. R. Bennett, *The Biased Ideal Rectifier*, Bell System Technical Journal, 26, 139-169 (1947).

3. R. L. Sternberg and H. Kaufman, *A General Solution of the Two-Frequency Modulation Product Problem*, Journal of Mathematics and Physics, 32, 233-242, (1953).

4. R. L. Sternberg, J.S. Shipman and H. Kaufman, *Tables of Bennett Functions for the Two-Frequency Modulation Product Problem for the Half Wave Square Law Rectifier*, to appear in Quarterly Journal of Mechanics and Applied Mathematics.

5. D. G. Lampard, *Harmonic and Intermodulation Distortion in 'Power Law' Devices*, Proceedings of the Institution of Electrical Engineers, Part IV, Monograph No. 55 (15th December, 1952).

Appendix

Derivation of Equation (30)

Let $h > 0$, and assume that $A_{mn}(h,k)$ is in case (i) so that $A_{mn}(-h,k)$ is in case (iii). Then

$$\tfrac{1}{2}\pi^2 A_{mn}(h,k) =$$

$$\int_0^{\cos^{-1}(h'-k')}\int_0^{\cos^{-1}(h-k\cos v)} F(\cos u + k\cos v - h)\cos mu\cos nv\,du\,dv$$

$$\tfrac{1}{2}\pi^2 A_{mn}(-h,k) =$$

$$\left(\int_a^{\pi}\int_0^{\cos^{-1}(-h-k\cos v)} + \int_0^{a}\int_0^{\pi}\right) F(\cos u + k\cos v + h)\cos mu\cos nv\,du\,dv$$

$$= \left(\int_0^{\pi}\int_0^{\pi} - \int_a^{\pi}\int_{\cos^{-1}(h-k\cos v)}^{\pi}\right) F(\cos u + k\cos v + h)\cos mu\cos nv\,du\,dv$$

$$= K_1 - K_2.$$

$$K_1 = \int_0^{\pi}\int_0^{\pi} F(\cos u + k\cos v + h)\cos mu\cos nv\,du\,dv$$

$$= \tfrac{1}{2}\pi^2\hat{A}_{mn}(-h,k)$$

$$K_2 = \int_a^{\pi}\int_{\cos^{-1}(-h-k\cos v)}^{\pi} F(\cos u + k\cos v + h)\cos mu\cos nv\,du\,dv.$$

Substituting $v = \pi - v'$, $u = \pi - u'$

$$K_2 = \int_0^{\cos^{-1}(h'-k')}\int^{\cos^{-1}(h-k\cos v')} (-1)^{m+n}\rho F(\cos u' + k\cos v' - h)\cdot$$

$$\cos mu'\cos nv'\,du'\,dv' = (-1)^{m+n}\rho\left(\tfrac{1}{2}\pi^2\right)A_{mn}(h,k)$$

whence (30) follows. The proof is similar for case (ii).

Note

Equation (29) is of computational use only for ν = a positive integer. The equation is still formally correct for $\nu \neq$ a positive integer, but in this case multi-valued functions enter into each term on the right. The computation of $A_{mn}^{(\nu)}(-h, k)$ for $\nu \neq$ a positive integer can be carried out from the defining integrals.

Item 4 of the References has appeared in *Quarterly Journal of Mechanics and Applied Mathematics*, 8, Part 4, 457-467 (1955).

McGill University, Montreal.

POPULAR PAGES

INTRODUCING SYMBOLIC LOGIC[1]

Edgar L. Dimmick

That field of Mathematics which is variously termed "Symbolic Logic," "Mathematical Logic" or "Boolean Algebra" covers a much wider scope than the formal study of Logic alone though it does deal with this subject as completely as man's thinking has permitted.

Aristotle was one of the first to attempt to formulate laws for logical reasoning and since his time hosts of excellent minds have concerned themselves with the logic which was built upon the structure Aristotle raised and transmitted to the present day as "formal" or "Aristotelian" Logic with few innovations.

It was not until many years later when scholars and original thinkers conceived of a practical way to convert the material used in logic into symbols (which could be manipulated with ease) that any distinct advance was made in Symbolic Logic. Not only did symbolization of the cumbersome components of Aristotelian logic make for much greater ease and facility in dealing with logical structures but it made the interrelationships of parts more readily ascertainable at a glance. Moreover, it revealed extensions into fields of thought both general and mathematical which would not even have been suspected as existing without the convenience and power which lies in the ability to reduce a problem to a few, concise symbols. No one, for example, would have suspected that the study of the fundamental laws of logic would (when symbolically represented) furnish invaluable tools for simplifying electrical circuits or formulating insurance policies or feeding data to digital computers.

Because symbolic logic as a mathematical subject per se is an absorbing study, because newer and more extensive applications are

---

1. Dear Mr. James: Your letter of the 18th containing encouragement for my suggested undertaking to write a 'popular' type of article on *Symbolic Logic* has served as a stimulating incentive to set about it at once. This I have done.

I am aware of certain features about the article which may be criticized and yet which I have consciously done nevertheless:

a. I have again and again knowingly sacrificed mathematical precision in defining or explaining for the sake of initially rendering the material daily coming to light in the realm of practical usefulness and because symbolic logic is not so widely known and appreciated as some other branches of mathematics it was thought that an article dealing with the elementary "modus operandi" might prove of interest.

* * * *

It is the general experience of childhood to first associate numbers with concrete object - two apples, two pennies, two shoes, are instances in which the duality is a part of the thing itself. Later the more mature child begins to conceive of "two" separated and abstracted from its associated use with specific objects. Soon, in school, he is introduced to the symbol "2" and learns that it represents the abstract conception of "two". On being introduced to Algebra further symbolization, abstraction and generalization is continued. Now any symbol, such as "x" can represent any definite but unknown quantity of anything. It is probably not until this stage is achieved that the power and utility of reducing facts to symbols and the greater and greater generalizing of these facts becomes apparent.

Symbolic Logic has as its basis the symbolization and generalizing of the laws of reason and logical thinking. It reduces (broadly speaking) reasoning to a set of symbols and then proceeds to use these same symbols to valid conclusions much as is done in algebra or even in simple arithmetic.

Let us make a start by choosing some simple sentences which state a logical thought:

"Socrates is (a) man."
"Fido is (a) dog."
"(The) moon is (a) satellite."

(Note: The words enclosed in parenthesis are superflusous and may be omitted without affecting the fundamental thought conveyed by the sentence.)

---

understandable by those readers for whom it is designed, viz. the reader who is starting in "fresh" on the subject of Symbolic Logic. (Taking a beginner down too many side roads of precise explanation causes him to lose the main road of thought, is confusing and discourages his interest.)

b. I have been deliberately redundant and repetitious where I wished the reader to hold salient facts in mind while pursuing a main thread of thought.

c. I have deliberately oversimplified and "spelled out" in their entirety a number of lines of reasoning to make *doubly* certain that nowhere is there a break in the reader's ability to follow the line of reasoning because he comes upon a hiatus which is caused by my assumption that the ommission is one which is so apparent it need not be stated.

d. All of this has necessitated extra verbiage which means extra space if you print it and you may not consider devoting the space it takes proportionate to the main body of the material found in Mathematics Magazine.

I could shorten it considerably but then would sacrifice its clarity and I have made every endeavor to be diaphanously clear above all else. I even went so far as to have my wife read the article and, after reading it, to "explain" it *to me*. (Excellent procedure. Editor).

Edgar L. Dimmick

There is a myriad number of sentences (or statements) of this specific type.

They all have the form "*x* is *y*" and one has only to substitute any noun for *x* and another for *y* in order to create any number of sentences of the same identical form. We have taken the first step into symbolic logic by doing so. We have said "Let *x* and *y* (or any other two letters or symbols) represent any two nouns and let the structure '*x* is *y*' be a logical sentence," and, Lo! it is even so. All possible sentences of identical structural type are now contained in the simple formula "*x* is *y*".

There are times when, if we substitute random nouns for *x* and *y*, we derive factual nonsense from our formula "*x* is *y*." For example, if we substituted the word "virtue" for *x* and "pencil" for *y* we would come out with the *factually* meaningless sentence "virtue is pencil." Never-theless this factually meaningless sentence would still be of the exact form "*x* is *y*." It is nevertheless acceptable in symbolic logic because it is the *symbols* and the *form* with which we deal and in which we are interested. It is the logical abstraction, the divorcing of all symbols from specific concrete facts which enables us to employ symbolic logic in a manner more extensive than if we limited ourselves by tying ourselves entirely to that which is concretely factual.

Having described and illustrated what we are about let us go on a bit further and take the sentence:

"*If Socrates is a man <u>then</u> socrates is mortal.*"

Employing the method we have just devised of symbolizing and setting down a generalized form we may transpose the above sentence into:

"*If (x is y) <u>then</u> (x is z).*"

Now, the inovators and developers of symbolic logic perceived that even though there had been an initial symbolization and generalization of a sentence like this it would be possible to still further con-dense it and render it more concise without losing a whit of its value to portray accurately a distinct "type" of sentance. It is done in this manner. Let the symbol "$\supset$" stand for "If ... then" and place this symbol between the two portions of the sentence in the instance where the sentence states that one part of it is dependent on the other.

Thus: $(x \text{ is } y) \supset (x \text{ is } z)$. Since the symbol "$\supset$" is understood to represent both "if" and "then" there will be no misunderstanding if it is used in this manner alone instead of using two separate symbols, one to represent "if" at the beginning of the sentence and one for "then" in the middle.

$(x \text{ is } y) \supset (x \text{ is } z)$ is thus a further useful simplification.

But "x is y" and "x is z""are each a distinct sentence exactly of the form we first discussed. We can therefore let (x is y) be represented by "A" and (x is z) be represented by "B" and we arrive at the more condensed and generalized form $A \supset B$. This short, exact form tells us that "If (any) A then (any) B". We are now well within the realm of symbolic logic. Let us explore a bit further.

Though symbolic logic had its essential beginnings with Boole's "*Laws of Thought*" *it has not yet been possible* to agree on a standard set of symbols. Indeed it is not essential (though admittedly more convenient) that the symbols employed be invariable and fixed any more than in ordinary algebraic notation.

The following symbols are employed in some works on symbolic logic and will serve in explaining further steps in this study:

$\bar{x}$ (a bar over any symbol) represents the denial or negation of whatever x stands for.

Example: If x represents "Socrates is a man" or " Fido is a dog" then $\bar{x}$ represent "socrates is NOT a man" or "Fido is NOT a dog". Whatsover x may be,"$\bar{x}$"denies it and declares it to be false.

• (a dot) represent the *conjunction* of two parts. It is a substitute for the word "and"

Example: $x \cdot y$ represents "*x and y*"

v Represents the alternative (*alternation*) and is a substifor the words "either ... or".

Example: $x \vee y$ represents "*either x or y*".

$\supset$ Represents (as explained previously) a *conditional* and is a substitute for the words "if ... then".

Example: $x \supset y$ represents "*if x then y*".

Other symbols have been used as representative of still other meanings. Space, however, will not permit including them in a brief discussion such as this. A further word is necessary in explanation of the three symbols "•", "v" and " $\supset$ ". Since the possibility of ambiguity can arise in assigning meaning to them in their use.

1) When the conjunction "and" ("•") is employed as a symbolization $x \cdot y$, it signifies that *both x and y* are in existence or are logically true. When we say, "Jack *and* Jill" we mean *both* of them, not Jack without Jill nor Jill without Jack. This sense of the use of "and" as a conjunction is strictly followed in Symbolic Logic in attaching meaning to the symbol "•".

2) When we symbolized "either ... or" by use of the symbol "v" in some such form as $x \vee y$, it is understood in the sense that one ordinarily understands the possibility of various events occurring

when we say

"Either Tom will come OR Mary will come." This is ordinarily taken to mean that *one* of the two will come and it is even possible that *both* of them will come. Only in the single remaining instance where *neither* of them come is the whole sentence *untrue*.

We can thus assign to the symbol "v" the meaning that x is true, *or* y is true, *or both* are true. In only one of the four possible instances will $x \vee y$ turn out to be false or untrue and that is the case where *neither x nor y* is true.

If in the statement "*Either* Tom will come *or* Mary will come" we let x stand for "Tom will come," and y stand for "Mary will come" then the whole sentence is symbolized by "$x \vee y$". Now this *whole sentence* will be *true* and correct in three instances:

1) If it turns out that Tom alone comes.
2) If it turns out that Mary alone comes.
3) If it turns out that BOTH Tom and Mary come.

Only in the single remaining case where BOTH Tom and Mary fail to come is the whole statement false.

We can construct a simple chart which will demonstrate these facts with the utmost simplicity, as follows:

x	y	$x \vee y$
True	True	True
False	True	True
True	False	True
False	False	*False*

or more simply still letting

T = True
F = False

x	y	$x \vee y$
T	T	T
F	T	T
T	F	T
F	F	*F*

This shows at a glance that if it is true that Tom does come and Mary does come then the sentence "Tom will come or Mary will come" is itself True, etc., etc. The chart shows clearly the sentence is False only if it is False that either came.

4) When the symbol "$\supset$" is employed it is intended to convey the meaning that the only instance in which the form $(x \supset y)$ is considered to be False *as a whole* is the one case where x is *True* and y is *False*. This is seen to be the case when we construct the "Truth Function" chart as it is called for this symbol as we did for the symbol "v" in the preceding section.

x	y	$(x \supset y)$
T	T	T
F	T	T
T	F	*F*
F	F	T

For convenience and ready comparison the Truth Function Charts of all three symbols will now be presented

"·"

Symbol for Conjunction "and"

x	y	$x\ y$
T	T	*T*
F	T	F
T	F	F
F	F	F

($x.y$) is TRUE if *both* x is true and y is true.

"v"

Symbol for Alternation "Either...or"

x	y	$(x \vee y)$
T	T	T
F	T	T
T	F	T
F	F	*F*

($x \vee y$) is FALSE only if *both* x and y are false.

"⊃"

Symbol for the Conditional "If....then"

x	y	$(x\ \ y)$
T	T	T
F	T	T
T	F	*F*
F	F	T

($x \supset y$) is FALSE only in the single case where x is true and y is false.

Let us now pause to consider what fruits our labor has borne.

Let us symbolize a complex sentence occurring in the drawing up of a Will or Life Insurance Policy.

> "If the husband and wife both die or if the husband dies and the wife survives then the entire sum will go to John or Mary."

We will transpose this into symbolic logic symbolism.

We will let x stand for "the husband survives".

We will let $\bar{x}$ stand for the *denial* that the husband survives ($\bar{x}$ = the husband does NOT survive).

We will let y stand for "the wife survives".

We will let $\bar{y}$ stand for "the wife dies." That is $\bar{y}$ is a *denial* that the wife survives.

We will let J stand for John.

We will let M stand for Mary.

We will let the symbol ⊃ take on its assigned meaning and here it will denote that IF certain circumstances occur THEN "the entire sum will go to ...".

The transposed sentence will then read:

$$[(\bar{x} \cdot \bar{y}) \vee (\bar{x} \cdot y)] \supset (J \vee M)$$

It will be noted that in reducing the written sentence to its generalized and symbolized equivalent that parentheses and brackets are employed as a kind of "punctuation" to separate the component parts of the set of symbols "·", "v" and "⊃". In the above, the entire structure within the brackets is the first component of the two connected by the " v " sign, thus [.....] ⊃ (J v M). The first "v" sign connects the components within the third parenthesis, thus, (J v M).

We now have an understanding of how, not only this sentence but *any* sentence of the same form can be reduced to a brief, concise *generalized* set of symbols which clearly reveal the relationships of one part to another (which the *written* statement does NOT do) and which has been put into a form where we have gained the tremendous advantage of manipulating it with the same ease that we work with the numbers of ordinary mathematics.

REFERENCES

1. *Mits, Wits & Logic,* L.R. Lieber & H.G. Lieber, W.W. Norton & Co. New York.

- Very elementary. Written in exceptionally clear "popular" style.

2. *Methods of Logic,* W.V. Quine, Henry Holt & Co. New York.

- An elementary text. Requires close reading. Concise.

3. *An Introduction To Symbolic Logic,* S.K. Langer, Dover Publications.

- A good elementary text though sometimes too extensive in explaining adjunct concepts. Obtainable in inexpensive paper edition.

4. *Fundamentals of Symbolic Logic,* Alice Ambrose, Movitz Lazerowitz. Rhinehart and Co., New York.

- Good elementary text. Some spots at the beginning are puzzling.

5. *Symbolic Logic,* C.I. Lewis and C.H. Langford, Dover Publications, New York.

- A standard work. Invaluable for those somewhat at home in the subject.

6. *A Symbolic Analysis of Relay and Switching Circuits,* Paul Shannon, Reprint obtainable from Edmund C. Berkley, 36 W. 11 St. New York 11, New York.

- Of interest to those who already possess some mathematical skill and wish a practical application.

SAVINGS ACCOUNT ANNUITIES

Roger Osborn

This article treats a narrow segment of the mathematics associated with the operation of savings banks. It will be remarked later in the article that there is involved herein an example of a very important phase of business management - that of maximizing the return from an investment or of minimizing the investment for a fixed return.

Many savings banks or savings and loan associations credit interest to a savings account in the following fashion. A deposit made (and not withdrawn before the next conversion date) during the first ten days of a month earns simple interest from the first of that month to the next interest conversion date. Thereafter it draws compound interest for any integral number of interest conversion periods. An amount withdrawn at a date between two interest conversions draws no interest from the last conversion date preceding the withdrawal.

It is interesting to consider two types of problems. These problems may be stated in general terms as the present value problem (for an annuity which consists of withdrawals from an account) and the amount or sum problem (for an annuity which is paid into a savings account) for a savings account which is subject to the above conditions. The main point of interest lies in the results obtained when the first payment of the annuity is made at a date between two conversion dates.

To be more explicit in the statement of the problem, we shall adopt the following notation. Let

i = the interest rate per conversion period;

p = (the number of payment periods per year) $\div$ (the number of interest conversions per year);

n = (the total number of payment periods in the term of the annuity) $\div$ (p), which in general gives the total number of interest conversion periods;

R = the periodic payment of the annuity;

A = the present value of the annuity (the deposit necessary to allow for the proper number of withdrawals) on a date preceding the first payment by one payment period;

S = the sum of the annuity (the total of all payments and all interest earned) on the date of the last annuity payment;

b = the number of payment periods ($b < p$) from some conversion date to a date preceding the first annuity payment by one payment period (it should be emphasized that a payment period is a period of time equal to the time between two payments of the annuity and that a payment period in this sense does not imply the existence of a payment, but rather is merely an interval of time): in the present value problem, the deposit A is made b payment periods after some interest conversion date and the first withdrawal is to occur after $b+1$ payment periods, while in the sum problem, the first periodic deposit into the account is to occur after $b+1$ payment periods.

Let p, n, and b be integers. In an actual savings account situation, this condition is usually met, so it imposes no material restriction.

By the ordinary methods for finding sums and present values, adapted to the conditions of the savings account problem[1], the formulas for the present value and the sum of an annuity are:

(1)

$$A = R\left\{(p - b - 1) + \frac{p\, a_{\overline{n-1}|i}(1+i) + (b+1)(1+i)^{-n+1}}{1 + \frac{p-b}{p}\, i}\right\}$$

(2)

$$S = R\left\{(p - b)\left[1 + \frac{p-b-1}{2p}\, i\right](1+i)^{n-1} + \left[p + \frac{p-1}{2}\, i\right] s_{\overline{n-1}|i} + b\right\}$$

It may be remarked here, and it becomes amply apparent later, that the present value of an annuity (as here defined) is not the compound or simple present value of the sum of an annuity, or vice versa. The relation between the sum, as defined above (and given by formula 2) and the accumulated value of the present value (given by formula 1) may be obtained by applying the rules governing accumulation of savings accounts, but it will not be used here.

Consider now an example of a present value problem. Let a deposit be made, creating a savings account, which will be just sufficient to provide for 12 monthly withdrawals of \$100. (We assume that the bank waives its right to require notice of any length of time before a withdrawal.) Let the interest rate paid by the bank be 3% compounded semi-annually (that is, $i = 1\frac{1}{2}\%$). These data determine that $p = 6$ and $n = 2$. If we assign the value $b = 4$, we compute the necessary deposit by use of formula 1, to be $A = \$1187.17$.

Table I below shows the depletion of the account in the above example (in which $b = 4$).

---

1. A.H. Diamond, *Annuity Formulas for Payments Made between Conconversion Dates*, THE AMERICAN MATHEMATICAL MONTHLY, Vol. XLIV, no. 9 (November), 1937, pp. 583-585.

Month	In account at beginning of month	Interest credited to account at end of month	In account at end of month before withdrawal	Withdrawal at end of month
1	\$1187.17	\$ 0	\$1187.17	\$100
2	1087.17	5.44	1092.61	100
3	992.61	0	992.61	100
4	892.61	0	892.61	100
5	792.61	0	792.61	100
6	692.61	0	692.61	100
7	592.61	0	592.61	100
8	492.61	7.39	500.00	100
9	400.00	0	400.00	100
10	300.00	0	300.00	100
11	200.00	0	200.00	100
12	100.00	0	100.00	100

Table I

Table II shows the necessary deposit to provide for 12 withdrawals of \$100, with $i = 1\frac{1}{2}\%$, and for values of b between 0 and 5 inclusive. Also included in Table II is a row of values of S^*, in which S^* is defined to be the accumulated value of the account at the end of the 12 month period under the assumption that no monthly withdrawals were made. In this sense S^* represents the accumulated present value, and its values may be compared with the corresponding values from Table IV.

b	0	1	2	3	4	5
A	\$1188.20	\$1187.21	\$1186.70	\$1186.70	\$1187.17	\$1188.15
S^*	1224.11	1220.08	1216.56	1213.54	1211.01	1208.99

Table II

It appears from Table II above that as b varies, A assumes a minimum value at $b = 2$ and $b = 3$. (If A, as given by formula 1, is treated as a function of b, and if b is allowed to vary over the entire range $0 < b < p$, the variable A assumes a minimum value in the neighborhood of $b = p/2$.) For a student who is unfamiliar with the methods of calculus, the table illustrates the striking point that there would be a most advantageous time to make the original deposit!

The sum problem involves a set of periodic deposits which earn simple interest from the date of deposit to the next conversion date, and compound interest thereafter for all integral numbers of interest conversion periods. No interest is earned following a conversion date until the next conversion date. Let us consider an example of a series of 12 monthly deposits of \$100 each being deposited in an account earning 3% compounded semi-annually. As was stated above, let the first deposit be made $b + 1$ payment periods after an interest conversion date. Table III shows the accumulation of such an account for

$b = 3$. Similar table may be constructed for other values of b.

Month	Deposit at end of month	Interest credited to account at end of month.	Amount in account at end of month.
1	$100	$ 0	$ 100.00
2	100	0	200.00
3	100	0.75	300.75
4	100	0	400.75
5	100	0	500.75
6	100	0	600.75
7	100	0	700.75
8	100	0	800.75
9	100	8.26	909.01
10	100	0	1009.01
11	100	0	1109.01
12	100	0	1209.01

Table III

Table IV is a tabulation of values of S for integral values of b from 0 to 5, inclusive.

b	0	1	2	3	4	5
S	$1216.56	$1212.79	$1211.27	$1209.01	$1207.00	$1205.25

Table IV

It may be observed from Table IV that the values of S decrease steadily for increasing values of b. If S, as given by formula 2, is treated as a function of the variable b, $0 < b < p$, it is possible to verify that S is a decreasing function of b for all values of p, n, and i, and not just for the values selected above. The values of b used in Table IV were used as a consequence of the restriction that b be an integer (the only restriction consistent with savings account conditions). These same observations are true for the values of S^* and for S^* treated as a function of b, $0 < b < p$.

Another observation which is interesting is that S^* (for $b = 3$), which is the accumulated value of the minimum deposit, is equal to S (for $b = 0$), which is the maximum sum of a corresponding annuity. This somewhat startling observation might lead a student to the conclusion that a general truth had been stumbled upon. Further research, at an elementary level well within the reach of every student, will reveal that the accumulation of the minimum deposit will not, in general, yield a value equal to the maximum sum for a corresponding annuity.

The University of Texas.

INTEGERS, UNIQUE FACTORIZATION AND IDEALS

L.E Diamond

The concept of ideals was motivated by the extension of the word integer to numbers such as $(1 + \sqrt{5})/2$, and the consequent desire to restore unique factorization of integers into prime factors to those domains for which it failed. The technical definition of an ideal does not convey this motivation but for the moment we shall consider the subject merely from the aspect of unique factorization.

Even among integers difficulties arise in unique factorization. For example $-18 = (-2)(-3)^2 = (-2)(3)^2 = (3)(-3)(2)$. The factorization differs not only in the order of the factors but in the factors themselves. To avoid this, the concept of units is adopted. An integer, u, is a unit for the set if u divides every element of the set. ± 1 are units for the integers. Two factors are regarded as identical if they differ only by multiplication by a unit. $21 = (-3)(-7) = (3)(7)$ is then regarded as an identical factorization. Since negative prime numbers can be put in the form $(-1)p$, p a positive prime, only positive prime numbers need be considered. An integer, p, that is not zero nor a unit, is said to be prime if its only divisors are plus or minus p, and the units. An integer is completely factored when it is expressed as a product of positive prime factors and a unit, ± 1.

There are *two fundamental theorems for positive integers*. Given any two positive integers whatsoever, a and b, there always exists an integer N such that Na is greater than b. If $a = 1$, then $ab = b$. If a is greater than 1, then $a - 1$ is greater than zero, $(a - 1)\,b$ is greater than zero, and ab is greater than b. In either case $ab + a$ is greater than b so that we set $N = b + 1$, and the theorem is proved.

Every set of positive integers, whether finite or infinite, contains a least integer. This is intuitively clear but it can be considered a defining property of the integers. There not only exists at least one integer, N, such that Na is greater than b, but there exists *a least such integer*, n. For example if $a = 4$ and $b = 9$, $N = b + 1 = 10$, $N = 3$. $3 \cdot 4$ is greater than 9 and $N = 3$ is the least such integer since $2 \cdot 4$ is less than 9. Technically a set is said to be *well-ordered* if every non-empty subset has a least element. When ordered according to magnitude, it can be proved that the positive integers are *well-ordered*.

The division algorithm follows directly from this. It states that if a and b are any two positive integers whatsoever, there exist integers q and r, $q \geq 0$, $0 \leq r < a$, such that $b = qa + r$. The proof is trivial if $a = b$, $q = 1$, and $r = 0$, so let $b > a$. Then there exists a least positive integer n such that $na > b$. Let us now set $q = n - 1$. Then $qa \leq b < na = qa + a$. If $qa = b$, $r = 0$. If $qa < b$, then $b = qa + r$, and $0 < r < a$ since $b < qa + a$. It can be proved that q and r are unique.

If the positive integer, h, divides the positive integer, a, and h also divides the positive integer, b, then h is a positive common divisor of a and b. If every other common divisor, c, of a and b, divides h, then h is the *greatest common divisor* of a and b, and we write $h = (a,b)$.

Given the equation $b = aq + r$, $0 < r < a$. Let the integer c be a common divisor of the integers a and b. Hence it is a common divisor of $b - aq$. Since $b - aq = r$, c is a divisor of r. Conversely every common divisor of the integers a and r divides b, and is consequently a common divisor of the integers a and b. Therefore the common divisors of the integers a and b are only those numbers which are common divisors of the integers a and r. The greatest of these divisors, h, must also coincide, or in the usual notation $h = (a,b) = (a,r)$.

We shall illustrate the above principle numerically, thus showing the basis for the proof of what is called, after its originator, *Euclid's Algorithm*. The theorem can be stated in this form: If a and b are integers, there exists an integer h, unique apart from sign, such that h is the greatest common divisor of a and b. There also exist signed integers, A and B, such that $Aa + Ba = h$. We select as integers 2805 and 3094.

$$3094 = 2905 + 289$$

Any common divisor of 3094 and 2805 is a common divisor of 2805 and 289

$$2805 = (9)(289) + 204$$

Any common divisor of 2805 and 289 is a common divisor of 289 and 204. The problem of finding the G.C.D. of 2805 and 3094 becomes the problem of finding the G.C.D. of 2805 and 289.

$$289 = (1)(204) + 85$$

The problem now is reduced to finding the G.C.D. of 289 and 204.

$$\begin{aligned} 204 &= (2)(85) + 34 \\ 85 &= (2)(34) + 17 \\ 34 &= (2)(17) + 0 \end{aligned}$$

The successive remainders form a decreasing finite sequence of non-negative integers so that we eventually arrive at a zero remainder. The *last non-vanishing remainder*, 17, is the G.C.D. of 2805 and 3094.

From the above equations we now write the following. (We would point out that in practical operations both the preceding work and that which follows can be considerably shortened.) Our purpose here is to show the principles.

$17 = 85 - (2)34$	$34 = 204 - (2)(85)$
$17 = 85 - (2)\ [204 - (2)(85)]$	
$17 = (5)(85) - (2)(204)$	$85 = 289 - 204$
$17 = (5)(289) - (204) - (2)(204)$	
$17 = 5(289) - 7(204)$	$204 = 2805 - (9)(289)$
$17 = 5(289) - 7\ [2805 - (9)289]$	
$17 = 68(289) - 7(1805)$	$289 = 3094 - 2805$
$17 = 68(3094 - 2805) - 7(1805)$	
$17 = (68)(3094) - (75)(2805)$	i.e. $h = Aa + aB$.

If $h = 1$, a and b are mutually prime, or, equivalently, co-prime. In fact two integers, a and b, are co-prime, if and only if there exist integers A and B such that $Aa + Bb = 1$.

From the above it follows that if p is a prime number and p divides ab, then p divides a, or p divides b. The possibility that p divides both a and b is not excluded. Either p divides a and the theorem is proven, or else p and a are co-prime. If they are co-prime then integers P and A can be found such that $Pp + Aa = 1$. Then $b = bPp + Aab$. Since p divides ab, it divides Aab. Since p is a factor of bpP, p must divide b, i.e. p divides the right hand side of the equation and hence must divide the left hand side.

The *unique factorization theorem*, sometimes called the fundamental theorem of arithmetic, in a simple form, says that if an integer is expressed in two ways as a product of prime factors, then the prime factors will be the same, apart from order, in the two factorizations. Let the two prime factorizations of an integer n be written as $n = p_1 p_2 \dots p_i = P_1 P_2 \dots P_j$. Obviously p_1 divides n. Hence from the preceding theorem p_1 must also divide $P_1 P_2 \dots P_j$. If p_1 divides P_1 $p_1 = P_1$ since both are primes. If $p_1 \neq P_2$, then p_1 divides $P_2 P_3 \dots P_j$ and we try $p_1 = P_2$. If $p_1 \neq p_2$, then p_1 divides $P_3 \dots P_j$ and we try $P_3 = p_1$ and so on since clearly p_1 must equal one of the factors P_r. Similarly the factor p_2 must then equal one of the factors $P_1 P_2 \dots P_j$ from which the prime equal to p_1 has been removed. And similarly with each of the remaining factors of $p_3 \dots p_i$.

The theorems which have been given are essential for a clear understanding of our further discussion. If we consider integral domains in which there is no way of ensuring that the remainder, on dividing one integer by another, is less than the divisor, Euclid's Algorithm is not applicable. In these domains it is possible to factorize a number in different ways into prime factors.

In the set of integers it seems so obvious that factorization into primes is unique that a glance at a subset of integers will be illuminating. The one that follows is due to Hilbert. Consider a subset of the odd integers, 1,5,9,13,... of the form $4k+1$, $k=0,1,2,3,...$ In this set let us by analogy call a number, a, a prime number if it cannot be expressed in the form $a = bc$ unless b or c equals one, a,b, and c all members of the set. For example 21 is a prime since 3 and 7 are not members of the set. A number a, is composite if it can be expressed in the form $a = bc$, $b \neq 1$, $c \neq 1$. This subset is closed under the operation of multiplication. Hence we might assume that the product of any two primes is a composite number in the set. For example $5 \cdot 9 = 45$. However 9 and 49 are also primes but their product is a third prime, 21, squared. This contradicts the theorem which in effect states "the product offtwo integers, a and b, cannot be divisible by a prime, p, unless either a or b is divisible by p."

Factorization is not unique. The number 693 of this set can be factorized into primes in essentially two different ways. $693 = (9)(77) = (21)(33)$. The question arises, how can unique factorization be restored to this set? First we observe that there are numbers in the set which are "divisible" in an extended sense by their own square roots, which are not, however, members of the set. If we consider the set of all these square roots, not members of the set, as numbers which we can add to the set, and which we can couple together in factorization, we find that factorization becomes unique. For example 693 has the two factorizations (9)(77) and (21)(33). Among these square roots, which are not members of the set, are the numbers 3, 7, and 11. We find that both the above factorizations are identical with the coupling $(3)^2(11)(7)$. The "primes" in this set as originally given are not necessarily the fundamental building blocks from which the integers of the set are constructed. We can enlarge the set to contain them, and then factorization becomes unique.

It is customary to call the integers which belong to the set of real numbers, *rational integers*. The adjective rational distinguishes them from the integers which are now to be introduced. When we come to complex numbers, we must first define what we mean be an integer. Hence we shall mention some of the properties of the integers because the extension of the word must be logically consistent. At the same time it is quite convenient to use certain words, such as ring, integral domain, and field, which we shall define as they apply to our subject.

The set of rational integers obey the associative and commutative laws of addition and the associative law of multiplication. The set also obeys the distributive law of multiplication with respect to addition. The sum of two integers is again an integer. The product of two integers is again an integer. The equation $a + x = b$ always has a solution in integers. This last requirement might be changed to read "the difference of two integers is always an integer." Any set that fulfills these conditions is called a ring.

As a logical consequence of these requirements a ring must have the following properties. A ring has a zero element. The element x in $a + x = b$ is unique. A product is zero if one of the factors is zero. The converse is not necessarily true.

If a ring obeys the commutative law of multiplication and contains a multiplicative identity, i.e. an element e such that $ae = ea = a$, then the ring is a commutative ring with unit. The integers form a commutative ring. The even integers form a ring but they have no multiplicative unit.

In the set of rational integers the equation $xy = 0$ implies that at least either x or y is equal to zero. This is not a requirement for a commutative ring, but when it is satisfied by a commutative ring, the ring is called an integral domain. The rational integers are the simplest example - hence the name, integral domain. An integral domain in which every nonzero element, a, has an inverse, a^{-1}, such that $aa^{-1} = 1$, is called a field. The rational integers do not form a field. The rational numbers form a field usually designated by R. The integral domain of rational integers is denoted by J.

Numbers of the form $a + bi$, where a and b are rational integers, and i has its usual significance in the complex number field, are called complex or *Gaussian* integers. Without going into details the definition is logical since it can be proven that the Gaussian integers form an integral domain, denoted by G.

In the integral domain, J, the number 1 is exactly divisible by only two integers, plus and minus one. In G, 1 is exactly divisible by four integers, plus and minus one and i. Hence *there are four units in* G since a unit is defined as an element in G which divides one and hence also divides every element of G. (The unit can also be defined as an integer of which the reciprocal exists and is also an integer.) In G, since $(1 + 2i) = i(2 - i)$, $(2 - i)$ and $(1 + 2i)$ are regarded as the same factor: and similarly, since $(2 + i) = i(1 - 2i)$, $(2 + i)$ and $(1 - 2i)$ are regarded as identical factors.

Two integers in G, α and δ, are called *associates* if $\alpha = \delta e$, where e is a unit. Consequently $(1 + 2i)$ and $(2 - i)$ are associates, and $(2 + i)$ and $(1 - 2i)$ are associates.

A). $5 = (2+i)(2-i) = (1-2i)(1+2i)$
$5 = (2+i)(2-i) = [i(1-2i)][-i(1+2i)]$

The two factorizations of 5 as shown in A) are considered equivalent. This is analogous to the following factorization in J.

$$10 = (2)(5) = [(-1)(2)][(-1)(5)]$$

Observe that $(-1)(-1) = 1 = (+i)(-i)$. In J we ignore the factors (-1).

A Gaussian integer, P', is a prime in G if it is not a unit, and if in every factorization, $P' = \alpha\delta$, one of α or δ is a unit. Obviously 5 is a prime in J but composite in G. Omitting 2, the primes in J can be divided into two sets, A and B. A consists of all primes which leave the remainder 1 when divided by 4, i.e. they are of the form $4n+1$. This set includes 5,13,17,29,37,... Every prime of this set can be expressed in the following manner. $4n+1 = (a+bi)(a-bi) = a^2+b^2$. This fact was first stated by Fermat and proved by Euler. That this is reasonable can be shown in the following manner. In J let a rational prime p equal a^2+b^2. Then one of a or b must be odd, the other even. Otherwise the sum of their squares would be even and all rational primes except two are odd. Let $a = 2n$ and $b = 2m+1$:

$$4n^2 + 4m^2 + 4m + 1 = a^2 + b^2 = 4(n^2 + m^2 + m) + 1.$$

Hence for a rational prime to have the form a^2+b^2, it must be a prime of the form $4n+1$, i.e. $p \equiv 1 \pmod 4$. We have already illustrated this principle for 5. As further examples

$$13 = (3+2i)(3-2i) = 3^2 + 2^2$$
$$17 = (4+i)(4-i) = 4^2 + 1^2$$
$$29 = (5+2i)(5-2i) = 5^2 + 2^2$$
$$37 = (6+i)(6-i) = 6^2 + 1^2$$
$$41 = (5+4i)(5-4i) = 5^2 + 4^2$$

All primes in J of set A are composite numbers in G:

In G the primes fall into three classes. 1) B is the set of primes in J of the form $4n+3$, i.e. 3,7,11,19,... All positive rational primes of this form and their associates in G are Gaussian primes. 2) $1+i$ and its associates. 3) the integers in G, $a+bi$, $a-bi$, where $a > 0$, $b > 0$, a is even, and a^2+b^2 is a rational prime of the form $4n+1$, and their associates. Hence factorizations such as shown for 5, 13, 17 etc. are factorizations into primes. From 2) above the factorization of $2 = (1+i)(1-i)$ is a prime factorizations It is interesting to note that in G the integer two acts almost as a perfect square. $2 = i(1 - i)^2$. The existence of an infinite number of Gaussian primes can be proven in a similar manner to the proof in J, provided that the existence of a prime can be shown in G. We shall show that 3 is a prime in G since in so doing the norm of a Gaussian integer is defined and some of its fundamental properties are proved.

The *norm*, $N\alpha$, of a Gaussian integer $\alpha = a + bi$ is defined to be $(a + bi)(a - bi) = a^2 + b^2$, or $\alpha\bar{\alpha} = N\alpha$, where $\bar{\alpha}$ is the complex conjugate of α. $N\alpha$ is a non-negative integer. $N(\alpha\delta) = N\alpha N\delta$. If $\alpha = a + bi$, $\delta = c + di$, then $\alpha\delta = (ac - bd) + i(ad + bc)$, $\overline{\alpha\delta} = (ac - bd) - i(ad + bc)$. $(\alpha\delta)(\overline{\alpha\delta}) = (a^2 + b^2)(c^2 + d^2) = (\alpha\bar{\alpha})(\delta\bar{\delta})$, $N\alpha = 1$ *if and only if* α *is a unit.* Let $N\alpha = 1$. Then $a^2 + b^2 = 1$ so that $a = 0$ or $b = 0$, and $\alpha = 1, -1, i$, or $-i$, which are units. Conversely it can be shown that if α is a unit, $N\alpha = 1$.

Let $3 = \alpha\delta$, where neither α nor δ is a unit and hence 3 is not a prime in G then $N\alpha \neq 1$, $N\delta \neq 1$. $N3 = 9 = N\alpha\delta = N\alpha N\delta$. Then $N\alpha = N\delta = 3$. Hence if $\alpha = a + bi$, $a^2 + b^2 = 3$. But in J this equation has no solution. Hence either α or δ is a unit and 3 is a prime. In complex theory the primes can be shown to have properties practically identical with those of rational primes. In J, $b = qa + r$, where q and r are unique. A similar theorem is proved for Gaussian integers but the complex integers analogous to q and r are not unique. Euclid's algorithm is used in the proof of uniqueness of factorization. Since complex numbers do not differ in magnitude, i.e. two complex numbers are either equal or unequal, their norms are used. The complex number with the larger norm is divided by the complex number with the less norm so as to obtain a remainder whose norm is less than the norm of the divisor.

The concept of integers is now further extended and their form in many cases is quite different from that of rational integers. As an example one of the three cube roots of unity is $1/2(-1 + \sqrt{-3})$, symbolized by ω. The numbers, $a + b\omega$, a and b rational integers, form a set of "integers" for which, incidentally, unique factorization holds.

Let R be a rational number field as defined earlier. *A number,* α, *is said to be algebraic over* R *if it satisfies a polynomial equation* $a_0x^n + a_1x^{n-1} + \ldots + a_n = 0$, *with coefficients in* R *and* n *a positive integer.* The number α is not necessarily in R. Any field, K, containing R, is called an extension of R. For example any *number* field is an extension of the field of rational numbers. The extension field above is $R(\alpha)$.

Any rational number, a/b, is algebraic since it satisfies the equation $bx - a = 0$. Some irrational numbers, such as the square roots of the rational primes, are *algebraic numbers*. There are also complex numbers which are algebraic, as plus and minus i, since they satisfy equations of they type $x^2 + 1 = 0$. The Gaussian integers are in $R(i)$.

Let a_0, the nonzero coefficient of the highest power of x, called the leading coefficient, be unity. The polynomial in x is then called a a monic polynomial. Let the coefficients be rational integers. An algebraic number, α, satisfying this equation is defined as an *algebraic integer*. If α and δ areiintegers in an extension field of the rationals, $R(\rho)$, it can be shown that so are $\alpha+\delta$, $\alpha-\delta$, and $\alpha\delta$.

Now let $R(\alpha)$ be a quadratic field where α is a root of a monic quadratic equation with rational integral coefficients. Then $R(\alpha) = R(\sqrt{D})$, where D is a rational integer, positive or negative, free of square factors. We first consider algebraic integers of the form $a + b\sqrt{D}$, where a and b are rational integers. The interesting fact is that we can introduce into the field of rational numbers, or "*adjoin*" to the field of rationals *some particular set of surds, and this extension* of the rational field *retains the property of being a field.*

Consider algebraic integers of the form $a + b\sqrt{2}$, where a and b are rational integers. This extension field is symbolized by $R(\sqrt{2})$. In a fixed algebraic field, K, such as this one, an integer, α, divides an integer ρ, if ρ/α is an integer of K. e is a unit if e divides 1. α is a prime if it is not zero or a unit, and if any factorization $\alpha = \rho\omega$ implies that either ρ or ω is a unit. These definitions present no difficulties but it might be wondered why a fixed field was mentioned. In the early part of this article the ring of all integers was considered and the factorization theorem, etc was applied to the ring. However there are no primes in the ring of *all* algebraic integers. If α is an algebraic integer which is neither zero nor a unit, and which satisfies $f(x) = 0$, we can always write $\alpha = \sqrt{\alpha}\sqrt{\alpha}$, and $\sqrt{\alpha}$ satisfies $f(x^2) = 0$.

In the field $R(\sqrt{2})$ there are an endless number of units, and in this respect the field $R(\sqrt{2})$ is more typical of the general case than are the fields R, $R(i)$, and the imaginary quadratic fields, $R(\sqrt{D})$, where D is negative and square free.

$$(\sqrt{2} - 1)(\sqrt{2} + 1) = 1$$
$$(5\sqrt{2} - 7)(5\sqrt{2} + 7) = 1$$
$$(17 - 12\sqrt{2})(17 + 12\sqrt{2}) = 1$$
$$(99 - 70\sqrt{2})(99 + 70\sqrt{2}) = 1$$

All of the integers on the left hand side of the above equations are units. To obtain additional units we need only substitute any positive rational integer for n in the equation $(\sqrt{2} - 1)^n(\sqrt{2} + 1)^n = 1$. If these units were not disregarded, any integer in this field could be factored in an endless number of ways. However by ignoring the unites factorization can be shown to be unique. The norm of $a + b\sqrt{2}$ is defined as $|a^2 - 2b^2|$.

In $R(\sqrt{5})$ there are two factorizations for 4, since

$$(\sqrt{5} - 1)(\sqrt{5} + 1) = 4 = (2)(2).$$

However

$$x^2 - x - 1 = \left[x - \left(\frac{1+\sqrt{5}}{2}\right)\right]\left[x - \left(\frac{1-\sqrt{5}}{2}\right)\right] = 0.$$

The polynomial is nonic and has rational integral coefficients. Hence by definition $(1 + \sqrt{5})/2$ and $(1 - \sqrt{5})/2$ are algebraic integers. Their product is unity and by definition they are units in this field. Hence $(\sqrt{5} + 1)$ and 2 are equivalent factors of 4.

So far unique factorization has in general been resotred by units and by the definition of algebraic integers. However if we adjoin to the field of rationals all algebraic integers of the form $a + b\sqrt{-5}$ i.e. the extension field $R(\sqrt{-5})$, this method of restoring unique factorization falls down. (First observe that the integer $a + b\sqrt{-5}$ resembles only in appearance the Gaussian integer $a + bi$. In both cases a and b are rational integers, but if $a + b\sqrt{-5}$ is written in the form $a + bi$, b would no longer be a rational integer since it would consist of the product of a rational integer by $\sqrt{5}$).

Having in mind the infinite number of units in $R(\sqrt{2})$ and $R(\sqrt{5})$, We first investigate the units in $R(\sqrt{-5})$. In a quadratic field norms are used in considering the divisibility of integers. The definition for the norm depends essentially upon the automorphisms of the field. In $R(\sqrt{D})$ there is the isomorphism $\alpha = a + b\sqrt{D} \longleftrightarrow \bar{\alpha} = a - b\sqrt{D}$, so that each integer α is carried into its conjugate, $\bar{\alpha}$. For $\alpha = a + b\sqrt{-5}$. $N(\alpha) = \alpha\bar{\alpha} = a^2 + 5b^2$. The norm of the algebraic integer is a rational integer. The problem of the units is then the solution of $a^2 + 5b^2 = 1$. The only solution is $b = 0$ and $a =$ plus or minus one. [In this con. nection if $D = -1$, $R(\sqrt{D}) = R(i)$, in which case we have already found the units by a similar method to be plus and minus 1 and i. It is of interest to note that every algebraic number field except R and the quadratic field $R(\sqrt{D})$, D negative and square free, has an infinite number of units.]

As a specific case, consider the factorization of 21 in $R(\sqrt{-5})$. $21 = (3)(7) = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})(1 - 2\sqrt{-5}) = (4 + \sqrt{-5})(4 - \sqrt{-5})$. The factors are not units in the field. Are these factors primes in the field? Every integer in the field has the form $a + b\sqrt{-5}$ a and b rational integers. Hence all the integers form an integral domain $J[\sqrt{-5}]$. Assume that 3 is not a prime and $3 = \alpha\rho$, where neither α nor ρ is a unit. $N(3) = 9 = N(\alpha)N(\rho)$. $N(\alpha) \neq 1$, $N(\rho) \neq 1$. Then $N(\alpha) = N(\rho) = 3$. $a^2 + 5b^2 = 3$. If $b \neq 0$, $a^2 + 5b^2 > 3$, so $b = 0$, If $b = 0$, $a^2 = 3$ which is impossible for an integer a in J. Similarly if $7=\alpha\rho, N\alpha \neq 1$, $N\rho \neq 1$, $a^2 + 5b^2 = 7$. If $b^2 \neq 0$, $b^2 \neq 1$, $a^2 + 5b^2 = 7$. Hence either $b = \pm 1$, $a^2 = 2$, or $b = 0$, $a^2 = 7$, both of which are impossible. Hence both 3 and 7 are primes in $R(\sqrt{-5})$. The integers $1 \pm 2\sqrt{-5}$ are primes. For if $1 + 2\sqrt{-5} = \alpha\rho$, $N(1 + 2\sqrt{-5}) = 21 = N\alpha N\rho$, if neither α nor ρ is a unit, $N\alpha = 3$ or $N\rho = 3$, and this is impossible as already shown. A similar proof applies $1 - 2\sqrt{-5}$ and to the factors $4 \pm \sqrt{-5}$. Hence 21 is expressed as a product of prime factors in 3 entirely different ways which cannot be reconciled by any interpretation of the word algebraic integer.

The integer 3 *divides the product* of the two primes, $1 + 2\sqrt{-5}$ and its conjugate, but 3 does not divide either one in $R(\sqrt{-5})$. Let us, therefore, assume that if α and ρ are integers in $R(\sqrt{-5})$, α divides ρ if ρ/α is an algebraic integers, *not restricted to be in* $R(\sqrt{-5})$. Instead of confining ourselves to algebraic integers of the form $a + b\sqrt{-5}$, we shall consider a new set of algebraic integers defined by $(\rho/\alpha)^2 = a + b\sqrt{-5}$. The further discussion will be simplified, the desire being merely to clarify by examples the principles utilized in restoring unique factorization to $R(\sqrt{-5})$. Let $\delta = 2 + \sqrt{-5}$, $\bar{\delta} = 2 - \sqrt{-5}$, $3^2 = (2 + \sqrt{-5})(2 - \sqrt{-5})$. Then $9/\delta = 2 - \sqrt{-5}$. The square root of $9/\delta$ or $3/\sqrt{\delta}$ is an algebraic integer, although it is not in $R(\sqrt{-5})$. Observe that

$$\frac{(\sqrt{10} + \sqrt{-2})}{2} = \sqrt{\delta} = \sqrt{2+\sqrt{-5}} \qquad \frac{3}{\sqrt{\delta}} = \frac{(\sqrt{10} - \sqrt{-2})}{2} = \sqrt{\bar{\delta}} \,.$$

Hence $3 = \sqrt{\delta}\,\sqrt{\bar{\delta}}$. We have two algebraic integers, not in $R(\sqrt{-5})$, whose product is 3, and the square of each of these integers is an algebraic integer in $R(\sqrt{-5})$.

Let $\alpha = 1 + 2\sqrt{-5}$. $\alpha^2/\delta = -2 + 3\sqrt{-5}$. The square root of α^2/δ is

$$\frac{\alpha}{\sqrt{\delta}} = \frac{\alpha\sqrt{\bar{\delta}}}{\sqrt{\delta}\,\sqrt{\bar{\delta}}} = \frac{\alpha\sqrt{\bar{\delta}}}{3} = \frac{(\sqrt{10} + 3\sqrt{-2})}{2},$$

an algebraic integer not in $R(\sqrt{-5})$. In this extended type of division both 3 and $1 + 2\sqrt{-5}$ are divided by an algebraic integer, $\sqrt{\delta}$, not in $R(\sqrt{-5})$.

$$\begin{aligned} 2 + \sqrt{-5} &= (-2)(1 + 2\sqrt{-5}) - (12 - 3\sqrt{-5})3 \\ &= 38 - 8\sqrt{-5} - 36 + 9\sqrt{-5} \\ \delta &= -2\alpha^2 = (12 - 3\sqrt{-5})3 \\ \sqrt{\delta} &= (-2\alpha/\sqrt{\delta})\alpha - [(12 - 3\sqrt{-5})/\sqrt{\delta}\,]3 \end{aligned}$$

Hence any other factor common to $1 + 2\sqrt{-5}$ and 3 divides $\sqrt{\delta}$. The situation is similar to that discussed earlier when we considered the set of rational integers of the form $4K + 1$.

We found that $\alpha/\sqrt{\delta} = (\sqrt{10} + 3\sqrt{-2})/2$. Let this algebraic integer $= \sqrt{\rho}$, and let its conjugate $= \sqrt{\bar{\rho}}$. Both ρ and $\bar{\rho}$ are algebraic integers in $R(\sqrt{-5})$. Then $\sqrt{\rho}\,\sqrt{\bar{\rho}} = 7$. Calculation then shows us that $\alpha = \sqrt{\delta}\,\sqrt{\rho}$ and $\bar{\alpha} = \sqrt{\bar{\delta}}\,\sqrt{\bar{\rho}}$. $\alpha\bar{\alpha} = 21 = \sqrt{\delta}\,\sqrt{\bar{\delta}}\,\sqrt{\rho}\,\sqrt{\bar{\rho}}$. In the factorization of 21 the primes $4 - \sqrt{-5}$ and $4 + \sqrt{-5}$ also occurred. $\sqrt{\delta}\,\sqrt{\bar{\rho}} = 4 - \sqrt{-5}$. $\sqrt{\bar{\delta}}\,\sqrt{\rho} = 4 + \sqrt{-5}$. The original factorization of 21 into primes in $R(\sqrt{-5})$ was not unique. We repeat it.

$$21 = (3)(7) = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}) = (4 + \sqrt{-5})(4 - \sqrt{-5})$$

$$21 = (\sqrt{\delta}\,\sqrt{\bar{\delta}})(\sqrt{\rho}\,\sqrt{\bar{\rho}}) = (\sqrt{\delta}\,\sqrt{\rho})(\sqrt{\bar{\delta}}\,\sqrt{\bar{\rho}}) = (\sqrt{\delta}\,\sqrt{\bar{\rho}})(\sqrt{\bar{\delta}}\,\sqrt{\rho})$$

Using theiintegers $\sqrt{\delta}$, $\sqrt{\bar{\delta}}$, $\sqrt{\rho}$, $\sqrt{\bar{\rho}}$, the factorization becomes unique apart from the order of the factors. However this factorization is not in $R(\sqrt{-5})$. It is necessary to enlarge the ring of integers to include such numbers as $\sqrt{\delta}$ etc which are not originally members of it. These "ideal" numbers, or "ideals" take the place of primes in this unique factorization.

Let us now consider the technical concept of ideals from a simplified standpoint. A set, S, of one or more elements of a commutative ring, Q, is an ideal if it has the following properties. S is closed to the operations of addition, subtraction, and multiplication. In any commutative ring there are two trivial ideals. The zero ideal, symbolized by (0), consists only of the zero element. The unit ideal, (1), consists of the entire ring. For example the set of all rational integers is closed to the operations of addition, subtraction, and multiplication and forms the unit ideal. The ideal, (0), contains only zero.

Now consider a *subset*, A, of the rational integers, R, which fulfills the conditions of an ideal, $A \neq (0)$. Since A is an ideal in R, all its elements are rational integers and it must contain a positive integer. For let α be an element of A. $\alpha - \alpha = 0$, and $0 - \alpha = -\alpha$. Since A contains $\pm\alpha$, one of these must be a positive integer. Let m be the least positive integer in A, and n any other positive integer in A. Then $n = mq + r$, $0 \leq r < m$. Since m is the least positive integer in A, $r = 0$, and $n = mq$, i.e. every element of A is a multiple of m. Every number $ns + mt$ is in A. Every multiple of m is in A. This ideal is symbolized by $[m]$, or $A = [m]$.

A principal ideal is symbolized by one symbol, $[A_1]$, in the bracket and consists of all the multiples of A_1 by all the integers of Q. The principal ideal is generated by a single integer. $[m]$ is a principal ideal. It contains all the multiples of m and no other integers. Every ideal in R is a principal ideal. If A contains any two integers m and n, then Mm and $Nn = h$. m and n are multiples of h and $[m,n] = [h]$. Factorization of ideals over the rational integers is the same as factorization of integers. Nothing new is added by their introduction since as regards multiplication principal ideals in R are simply isomorphic with the numbers to which they correspond.

Every ideal in $R(i)$ is a principal ideal. The principal ideal is generated by the integer with the least norm instead of by the least positive integer.

The product of two ideals is an ideal which contains the product of two numbers, one from each ideal, and all numbers that can be formed from them by addition and subtraction. The product of [3] and [2] contains (3)(2) = 6, (3)(4) = 12, (9)(2) = 18, and all multiples of 6. Hence the product [3][2] = [6].

If α and ρ are any two integers in $R(\sqrt{-5})$, then the set of numbers $3\alpha + \rho(1 + 2\sqrt{-5})$ is closed to the operations of addition and subtraction, and is closed to multiplication by any integer in $R(\sqrt{-5})$. This set is an ideal generated by 3 and $1 + 2\sqrt{-5}$, and is symbolized by $[3, 1 + 2\sqrt{-5}]$. Now in R we found that if m and n were any two rational integers, $[m, n] = [h]$, a principal ideal. But $[3, 1 + 2\sqrt{-5}]$ is not a principal ideal in $R(\sqrt{-5})$ as there is no integer of the field $R(\sqrt{-5})$ which divides both 3 and $1 + 2\sqrt{-5}$. For let us assume that this ideal is a principal ideal and $[3, 1 + 2\sqrt{-5}] = [\alpha]$. Then α, an integer in $R(\sqrt{-5})$ divides both 3 and $1 + 2\sqrt{-5}$. But 3 and $1 + 2\sqrt{-5}$ are both prime in $R(\sqrt{-5})$ and hence relatively prime. Hence α must be a unit. The only units in $R(\sqrt{-5})$ are ± 1 so $[3, 1 + 2\sqrt{-5}] = [1]$. Now it can be shown that every element of $[3, 1 + 2\sqrt{-5}]$ is divisible by $\sqrt{\delta}$ since 3 and $1 + 2\sqrt{-5}$ are so divisible. Hence $1/\sqrt{\delta}$ is an integer, $1/\delta = 1/(2 + \sqrt{-5}) = (2 - \sqrt{-5})/9$, which is not an integer in $R(\sqrt{-5})$, since every integer in $R(\sqrt{-5})$ has the form $a + b\sqrt{-5}$, a and b rational integers.

From the factorization of 21 we set up the ideals generated by the factors shown. $P_1 = [3, 1 + 2\sqrt{-5}]$. $P_2 = [3, 1 - 2\sqrt{-5}]$. $P_3 = [7, 1 - 2\sqrt{-5}]$. $P_4 = [7, 1 + 2\sqrt{-5}]$. The ideal $[3, 4 - \sqrt{-5}]$ is not listed since it contains $1 + 2\sqrt{-5}$, and conversely.

$$4 - \sqrt{-5} - 3(1 - \sqrt{-5}) = 1 + 2\sqrt{-5}. \qquad (1 + 2\sqrt{-5}) + 3(1 - \sqrt{-5}) = 4 - \sqrt{-5}.$$

By the definition of multiplication of ideals P_1P_2 contains (3)(3) or 9, $3(1 - 2\sqrt{-5})$, $3(1 + 2\sqrt{-5})$, $(1 - 2\sqrt{-5})(1 + 2\sqrt{-5})$ or 21. All four elements given of P_1P_2 are multiples of 3, and P_1P_2 is a principal ideal [3] in $R(\sqrt{-5})$. Similarly

$$P_1P_3 = (4 - \sqrt{-5}), \quad P_1P_4 = (1 + 2\sqrt{-5}) \quad P_2P_3 = (1 - 2\sqrt{-5}), \; P_3P_4 = [7].$$

$$21 = (3)(7) = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

$$21 = P_1P_2P_3P_4 = P_1P_4P_2P_3.$$

Both factorizations reduce to the same ideal factorization which is unique. The same type of procedure is valid for algebraic fields similar to $R(\sqrt{-5})$.

The factorization of integers is thus transferred to the factorization of ideals. There is an entirely satisfactory arithmetic for ideals and by its use the problem of unique factorization in algebraic number fields of this type is settled. The ideals which replace the prime rational integers are those ideals, P, which have no factors except P and units. These ideals are called irreducible. It can be proved that every ideal in K, different from (0) and (1) can be represented uiiquely as a product of irreducible ideals to within order and to within multiplication by (1).

Milford, Texas

MISCELLANEOUS NOTES

Edited by

Charles K. Robbins

Articles intended for this Department should be sent to Charles K. Robbins Department of Mathematics Purdue University, Lafayette, Indiana.

ON EXPLICIT SOLUTIONS OF SOME TRINOMIAL EQUATIONS IN TERMS OF THE MAXIMUM OPERATION

Richard Bellman

§1. *Introduction*

Consider the trinomial equation

$$x^n + ax = b, \tag{1}$$

where a and b are nonnegative quantities, and n is positive. We wish to show that the unique positive root of the equation can be exhibited in explicit form, if we allow the operation of taking the maximum or minimum of a function.

§2. *The Quadratic Case*

Let us begin with the equation

$$x^2 + ax = b, \tag{2}$$

to illustrate the method. For all $x \geq 0$, we have

$$x^2 = \operatorname*{Max}_{u \geq 0} [2xu - u^2] \tag{3}$$

Hence (2) may be written

$$\operatorname*{Max}_{u \geq 0} [2xu + ax - u^2] = b. \tag{4}$$

From this equation, we conclude that

$$2xu + ax - u^2 \leq b \tag{5}$$

for all $u \geq 0$, with equality for one value of u. Since $2u + a > 0$, we can write

$$x \leq \left(\frac{u^2 + b}{2u + a} \right) \tag{6}$$

for all $u \geq 0$, with equality for one value of u. Thus, the non-negative solution of (2) is given by

$$(7) \qquad x = \operatorname*{Min}_{u\geq 0} \left(\frac{u^2 + b}{2u + a} \right)$$

On the other hand, we may write $x^2 = y$, and

$$(8) \qquad y + ay^{\frac{1}{2}} = b.$$

Let us now employ the relation

$$(9) \qquad 2y^{\frac{1}{2}} = \operatorname*{Min}_{u\geq 0} \left[\frac{y}{u} + u \right],$$

for $y \geq 0$. Then (8) becomes

$$(10) \qquad \operatorname*{Min}_{u\geq 0} \left[\frac{ay}{2u} + \frac{au}{2} + y \right] = b,$$

and thus

$$(11) \qquad \frac{ay}{2u} + \frac{au}{2} + y \geq b,$$

for all $u \geq 0$, with equality for one value of u.

Using the same reasoning as above, this lead to

$$(12) \qquad y = \operatorname*{Max}_{u\geq 0} \left[\frac{b - au/2}{1 + a/2u} \right].$$

Combining (12) and (7), we see that

$$(13) \qquad \sqrt{\frac{b - au/2}{1 + a/2u}} \leq x \leq \frac{b + u^2}{a + 2u}$$

for all $u \geq 0$.

§ 3. $x^n + ax = b$

Let us now see how this result extends to the genral trinomial equation. Take $n > 1$. We wish to write

$$(1) \qquad x^n = \operatorname*{Max}_{u\geq 0} [xu - g(u)]$$

for a suitable function $g(u)$. If so, we have, upon differentiation,

$$(2) \qquad x = g'(u)$$

and thus

$$x^n = xu - g(u) \tag{3}$$
$$nx^{n-1} = u + (x - g'(u))\frac{du}{dx} = u.$$

Thus

$$x = \left(\frac{u}{n}\right)^{1/(n-1)} \tag{4}$$

Comparing the two values for x, we wee that

$$g'(u) = \left(\frac{u}{n}\right)^{1/(n-1)} \tag{5}$$
$$g(u) = (n - 1)\left(\frac{u}{n}\right)^{n/(n-1)}$$

Using this value of $g(u)$ in (1), the equation $x^n + ax = b$ yields, as above,

$$x = \min_{u\geq 0}\left[\frac{b + (n - 1)(u/n)^{n/(n-1)}}{a + u}\right] \tag{6}$$

Similarly for $0 < n < 1$, we have

$$x^n = \min_{u\geq 0}\,[xu + h(u)], \tag{7}$$

where

$$h(u) = (1 - n)(u/n)^{n/(n-1)} \tag{8}$$

Thus

$$x = \max_{u\geq 0}\left[\frac{b - (1 - n)(u/n)^{n/(n-1)}}{1 + au}\right] \tag{9}$$

§ 4. *The Equation* $\phi(x) + ax = b$.

In the case where $\phi(x)$ is a strictly convex function of x, we may write

$$\phi(x) = \max_{u\geq 0}\,[xu - g(u)], \tag{1}$$

where

$$g(u) = \int_0^u f(s)\,ds, \tag{2}$$

where $f(s)$ is the inverse function to $\phi'(x)$. A similar expression holds for a strictly concave function. These expressions may be used to obtain upper and lower bounds for the solution of $\phi(x) + ax = b$.

§5. *Newton's Method.*

Newton's method furnishes a sequence of successive approximations

(1) $$x_{n+1} = x_n - f(x_n)/f'(x_n), \qquad n = 1, 2, \ldots,$$

to the solution of the equation $f(x) = 0$.

Let us show that if $f'(x) > 0$ in $[a\ \ b]$, and $f''(x) > 0$ in this interval, we have

(2) $$x = \operatorname*{Min}_{0 \le x \le b} [y - f(y)/f'(y)] ,$$

for a root x lying in $[a, b]$.

The minimum of $y - f(y)/f'(y)$ occurs at the point where

(3) $$\frac{f(y)f''(y)}{f'(y)^2} = 0$$

or $f(y) = 0$. The second derivative is $f''(y)/f'(y) \neq 0$ at this point.

There are equivalent expressions for functions of several variables.

The Rand Corporation, Santa Monica, Calif.

PROBLEMS AND QUESTIONS

Edited by

Robert E. Horton, Los Angeles City College

Readers of this department are invited to submit for solution problems believed to be new and subject matter questions 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 twice the size desired for repreduction.

Send all communications for this department to *Robert E. Horton, Los Angeles City College, 855 North Vermont Ave., Los Angeles 29, California.*

PROPOSALS

278. *Proposed by M. N. Gopalan, Mysore, India.*

The sum of the perpendiculars drawn from the vertices of a cyclic quadrilateral $ABCD$ to the sides a, b, c, d is equal to

$$\frac{(a + b + c + d)(e + f)}{2R}.$$

where e and f are the diagonals of the quadrilateral and R is the circumradius.

279. *Proposed by J. M. Howell, Los Angeles City College.*

A multiple choice test with $n \geq 10$ questions and $k > 1$ choices on each question is made. If the scoring is $\left(\frac{r - w}{k - 1}\right)\left(\frac{100}{n}\right)$ where r is the number right and w the number wrong, how many tests with different values of n and k can be constructed such that all possible scores will be integers?

280. *Proposed by T.F. Mulcrone, St. Charles College, Louisiana.*

If the cevian AD of the acute triangle ABC is the arithmetic, (geometric), [harmonic] mean of the sides b and c of the triangle, show that $\sin\delta$, δ being the acute angle between the cevian and a, is the arithmetic, (geometric), [harmonic] mean between $\sin B$, and $\sin C$.

281. *Proposed by Michael J. Pascual. Siena College, New York.*

$$\text{Let } D = \begin{vmatrix} \Sigma x_i^{2n} & \Sigma x_i^{2n-1} & \cdots & \Sigma x_i^n & \Sigma x_i^n y_i \\ \Sigma x_i^{2n-1} & \Sigma x_i^{2n-2} & \cdots & \Sigma x_i^{n-1} & \Sigma x_i^{n-1} y_i \\ \vdots & \vdots & & \vdots & \vdots \\ \Sigma x_i^n & \Sigma x_i^{n-1} & \cdots & (n+1) & \Sigma y_i \\ x^n & x^{n-1} & \cdots & 1 & y \end{vmatrix}$$

where the sums range from 0 to n. If $x_i \neq x_j$ prove that the necessary and sufficiant condition that $D = 0$ is that

$$\begin{vmatrix} x_0^n & x_0^{n-1} & \cdots & 1 & y_0 \\ x_1^n & x_1^{n-1} & \cdots & 1 & y_i \\ \vdots & \vdots & & \vdots & \vdots \\ x_n^n & x_n^{n-1} & \cdots & 1 & y_n \\ x^n & x^{n-1} & \cdots & 1 & y \end{vmatrix} = 0$$

282. *Proposed by Chih-yi Wang, University of Minnesota.*

One studant solved the problem, "Compute the area of the ellipse $x = 2\cos\theta$, $y = \sin\theta$", by using polar coordinates in the following manner:

$$\rho^2 = 4\,\mathrm{Cos}^2\theta + \sin^2\theta$$

$$A = 4(\tfrac{1}{2})\int_0^{\pi/2} (4\cos^2\theta + \sin^2\theta)\, d\theta =$$

$$4\int_0^{\pi/2}(1 + \cos 2\theta)\, d\theta + \int_0^{\pi/2}(1 - \cos 2\theta)\, d\theta = (5/2)\,\pi \text{ sq. units.}$$

As the correct answer is 2π sq. units what is wrong with his work?

283. *Proposed by Jack Winter and Richard C. Kao, The Rand Corporation, Santa Monica, California.*

For every non negative integer n prove that

$$\sum_{a_n=0}^{n} \sum_{a_{n-1}=0}^{a_n} \sum_{a_{n-2}=0}^{a_1} \cdots \sum_{a_1=0}^{a_2} 1 = \binom{2n}{n}$$

284. *Proposed by M.S. Klamkin, Polytechnic Institute of Brooklyn.*

Determine the envelope of convex polygons of n sides inscribed in the ellipse $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ and having a maximum area.

SOLUTIONS

Late Solutions

251, 252, 253. *J.M. Gandhi, Lingraj College, Belgaum, India.*

A Volume of Revolution

257. [January 1956] *Proposed by S.C. Ogilvy, Hamilton College, New York.*

Given a curve $y = f(x)$ and a straight line $Ax + By + C = 0$ intersecting at P and Q so as to bound an area, and such that any normal to the line between P and Q meets the curve exactly once; find the volume of the solid formed by rotating the area about the line.

Solution by Chih-yi Wang, University of Minnesota. If either A or B is zero, the volume may be calculated by the familiar method with a simple translation. Let us assume that neither A nor B is zero. Let the coordinates of P and Q be respectively; (a,α), (b,β), and the axis along the given line be called s-axis. By using the "disk method" we obtain:

$$V = \left| \pi \int_{(a,\alpha)}^{(b,\beta)} \left[\frac{Ax + Bf(x) + C}{\sqrt{A^2 + B^2}} \right]^2 ds \right|.$$

Since

$$ds = \left(\sqrt{1 + (dy/dx)^2} \right) dx = \sqrt{A^2 + B^2}\, dx/|B|$$

we get

$$V = \left| \frac{\pi}{B\sqrt{A^2 + B^2}} \int_a^b [Ax + Bf(x) + C]^2\, dx \right|$$

Also solved by R. K. Guy, Univeristy of Malaya, Singapore; Louis S. Mann, Los Angeles State College and the Proposer.

Professor Ogilvy listed the following pertinent references:

Math Gazette, Vol 21, 1937, pp 226-8

The American Mathematical Monthly, Vol 55, 1948, p 458, No 5.

The American Mathematical Monthly, Vol 56, 1949, p 708, No 7.

An Orthocentric Locus

258. [January 1956] *Proposed by Huseyin Demir, Zonguldak, Turkey.*

A triangle ABC inscribed in a circle varies such that AB and AC keep fixed directions. Find the locus of the orthocenter H.

1. *Solution by Major H. S. Subba Rao, Defense Science Organization, New Delhi, India.* The vertical angle A and the base BC are fixed in magnitude. Let $A_1B_1C_1$ be the isosceles triangle satisfying the conditions imposed on ABC. Let P be the mid-point of the smaller of the two arcs AC of the circum-circle and similarly Q the mid-point of the arc AB. Let O be the centre of the circle. The points P and Q are fixed.

Take the diameter through A, as the y-axis and the perpendicular diameter as the x-axis. With reference to these axes we can represent any point on the circle ABC by the parametric representation $a \cos t$, $a \sin t$.

Let $B_1 \equiv (t_2)$, $C_1 \equiv (t_3)$, $P \equiv (t_4)$ and $Q \equiv (t_5)$.

Noting that angle $A_1B_1C_1$ angle $A_1C_1B_1 = 90^\circ - A/2$ it can be easily shown that $t_2 = \frac{3\pi}{2} - A$, $t_3 = \frac{3\pi}{2} + A$, $t_4 = \frac{A}{2}$, $t_5 = 2\pi - \frac{A}{2}$.

In any position of the triangle ABC let $t = \measuredangle B_1OB = \measuredangle C_1OC$. Then $B \equiv (t_2 + t)$ and $C \equiv (t_3 + t)$. Further, BH being perpendicular to AC is parallel to OP and similarly CH is parallel to OQ.
The equations to BH and CH are easily found to be

$$x \operatorname{Sin} \frac{A}{2} - y \cos \frac{A}{2} = a \cos \left(t - \frac{3A}{2}\right)$$

and

$$x \operatorname{Sin} \frac{A}{2} + y \cos \frac{A}{2} = a \cos \left(t + \frac{3A}{2}\right).$$

Eliminating t between the two equations, the locus of H is found to be

$$\frac{x^2 \operatorname{Sin}^2 \frac{A}{2}}{a^2 \cos^2 \frac{3A}{2}} + \frac{y^2 \cos^2 \frac{A}{2}}{a^2 \operatorname{Sin}^2 \frac{3A}{2}} = 1.$$

This is an ellipse with its centre at O and semi axes

$$\frac{a \operatorname{Cos} \frac{3A}{2}}{\operatorname{Sin} \frac{A}{2}} \quad \text{and} \quad \frac{a \operatorname{Sin} \frac{3A}{2}}{\operatorname{Cos} \frac{A}{2}}$$

(An interesting corollary to this is that the loci of the nine-point centre and centroid of the triangle ABC are also ellipses).

II. *Solution by the proposer.* Let OX, OY be the lines parallel to external and internal bisectors of A respectively. Let the altitude AH intersect these fixed lines at X, Y. Since AO, AH are equally inclined to the bisectors of A, we have $AX = AO = AY$. Hence $XY = 2R$ = const.

We may think then of XY as a rod of constant length having the ends moving on OX, OY. Now the angle A being constant, BC will envelop, or the mid-point D of BC will describe a circle with center O. Hence $AH = 2\ OD = 2\ R \cos A$ = const. This proves that H is a fixed point of the moving bar XAY. Hence H describes an ellipse.
The semi-diameters of the ellipse are easily determined:

$$a = HY + AY = HA = R(1 + 2\cos A), \qquad b = HX = XA - HA = R(1 - 2\cos A).$$

Also solved by J. W. Clawson, Collegeville, Pennsylvania; R. K. Guy, University of Malaya, Singapore; Sister M. Stephanie, Georgian Court College, New Jersey; Harry D. Ruderman, The Bronx, New York and Chih-yi Wang, University of Minnesota.

Intersection of Perpendiculars

259. [January 1956] *Proposed by N. Shklov, University of Saskatchewan.*

Let A and B be the feet of the perpendicular drawn from the variable point $P(x,y)$ to the lines $15x - 8y = 0$ and $y = 0$ respectively. If the length of $AB = 15$, what is the equation of the locus of P?

I. *Solution by Sister M. Stephanie, Georgian Court College, New Jersey.* Since $OB = X$, $AB = 15$ and $PB = Y$, we have $AP = (15x - 8y)/17$. By the Pythagorean theorem $OP = \sqrt{x^2 + y^2}$; $AO = (8x + 15y)/17$. Since OAP and PBO are right angles, the quadrilateral $AOBP$ is cyclic and Ptolemy's theorem applies. Then: $AB \cdot OP = AP \cdot OB + AO \cdot PB$. (1). Substituting the above values in equation (1) yields an equation which reduces to $x^2 + y^2 = 289$ which is the required locus, and is, of course, a circle with center at the origin and radius 17.

II. *Solution by C. W. Trigg, Los Angeles City College.* Consider the more general problem wherein the lines are $ax = by$ and $y = 0$, and the length of AB is c. Then A is the intersection of $y - y_1 = -(b/a)(x - x_1)$ and $ax = by$. Thus the extremities of AB are $B[x_1, O]$ and

$$A[b(bx_1 + ay_1)/(a^2 + b^2),\ a(bx_1 + ay_1)/(a^2 + b^2)].$$

Then, dropping the subscripts and applying the distance formula, we have

$$\left[\frac{b(bx + ay)}{a^2 + b^2} - x\right]^2 + \left[\frac{a(bx + ay)}{a^2 + b^2}\right]^2 = c^2$$

Hence, the locus of P consists of the arcs of the circle

$$x^2 + y^2 = (a^2 + b^2)c^2/a^2$$

which lie between the two lines. In the specific case of this problem, the circle is $x^2 + y^2 = 289$.

Also solved by Robert Becker, Albright College, Pennsylvania; Huseyin Demir, Zonguldak, Turkey; J. M. Gandhi, Lingraj College, Belgaum, India; R. K. Guy, University of Malaya, Singapore; Edgar H. Grossman, Vancouver, B.C.; R. Huck, Marietta College, Ohio; C. N. Mills, Augustana College, South Dakota; M. Morduchow, Polytechnic Institute of Brooklyn, Maj HS Subba Rao, Defense Science Organization, New Delhi, India; Stewart Robinson, Duke University, North Carolina; Chih-yi Wang, University of Minnesota; Hazel S. Wilson, Jacksonville State College, Alabama and the proposer.

A Student's Error

260. [January 1956] *Proposed by Ben K. Gold, Los Angeles City College.*

A student solved the following problem incorrectly. Problem: In how many ways can five dice be tossed so that at least three aces show? His solution was ${}_5C_3 6^2$, reasoning that three dice must be aces and the other two may or may not be. What is the fallacy in this reasoning and how can the correct solution be obtained from his incorrect answer?

Solution by Emil D. Schell, Remington Rand Univac. The student counted the tosses $(1, 1, 1, x, y)$ as each occuring ${}_5C_3 = 10$ times. Actually $(1, 1, 1, 1, 1)$, for example, occurs only once. He may correct his solution by counting the permutations of $(1, 1, 1, x, y)$. Consider these in three categories:

CASE I. $x = y = 1$. There is only one example. This occurs once but his solution counts it as occuring 10 times, giving a surplus of 9.

CASE II. Either x or y is one, and the other not. There are five examples. Each occurs five times, but his solutions counts each as occuring twenty times, giving a surplus of 75.

CASE III. Neither x nor y is one. There are thirty cases. These are counted correctly. Thus ${}_5C_3 6^2 - 9 - 75 = 276$.

Also solved by Charles K. Fendall, Portland, Oregon; R. K. Guy, University of Malaya, Singapore; Elaine Johnson, Carleton College, Minnesota; Chih-yi Wang, University of Minnesota and the proposer. One incorrect solution was received.

A Class of Functions

261 [January 1956] *Proposed by M.S. Klamkin, Polytechnic Institute of Brooklyn.*

Determine the entire class of analytic functions $F(x)$ so that Simpson's Quadrature Formula

$$\int_{-h}^{h} F(x)\, dx = \frac{h}{3}\left[F(-h) + 4\, F(0) + F(h)\right]$$

holds exactly.

Solution by Harry D. Ruderman, Bronx, New York. Let $F(x) = E(x) + O(x)$ the sum of an even and odd function; that is,

$$E(x) = \frac{F(x) + F(-x)}{2}, \text{ and } O(x) = \frac{F(x) - F(-x)}{2}.$$

Assume that each is integrable. The Quadrature Formula is satisfied for any odd function that is integrable. The result is equal to 0. After replacing $F(x)$ by $E(x) + 0(x)$ and using the property $E(-x) = E(x)$, Simpson's Formula becomes

$$(1) \qquad \int_0^x E(x)\, dx = x/3[E(x) + 2E(O)] \qquad O \le x \le h$$

This relation implies that $E(x)$ has a derivative in this interval. Differentiate both members of (1).

$$(2) \qquad E(x) = \frac{x E'(x)}{3} + \frac{E(x) + 2E(O)}{3}.$$

This is a simple differential equation with the solution

$$(3) \qquad E(x) = A + Bx^2 \quad \text{with} \quad A = E(O)$$

If $F(x)$ has two integrable components and satisfies Simpson's Formula in the interval $O \le x \le h$, Then $F(x) = A + Bx^2 + O(x)$. Thus $F(x)$ is the sum of a quadratic and an odd function.

Also solved by Billy J. Boyer, Murphy Army Hospital, Waltham, Massachusetts; Huseyin Demir, Kandilli Bolgesi, Turkey; R. K. Guy, University of Malaya, Singapore; M. Morduchow, Polytechnic Institute of Brooklyn; Elwyn W. Morton, Texas Technological College; Chih-yi Wang, University of Minnesota and the proposer.

Palindromic Partition

262. [January 1956] *Proposed by P. A. Piza, San Juan, Puerto Rico.*

Partition 166,665 = 3(55,555) into the sum of three positive palindromes in eight different ways, with no zeros involved and with all 24 palindromes distinct.

Solution by Charles K. Fendall, Portland, Oregon. Interpreting the term "partition" in its strict algebraic sense, we assume that each palindrome, within a given solution, must contain different digits. Further, the palindrome condition implies that, in each solution, column one equals five and column two equals four, which is possible only if the sum of each column is 15. We further restrict consideration to 5-digit palindromes.

It is sufficient, therefore, to consider only the first 3 columns of each solution and to examine all the sets of three distinct digits, excluding zero, whose sum is 15.

By combining two distinct sets, such as $\begin{matrix}9\\5\\1\end{matrix}$ and $\begin{matrix}7\\6\\2\end{matrix}$, and permuting columns and rows, the following twenty solutions, in three column form, were found:

999	777	977	797	779	997	979	799	922	292
555	666	566	656	665	556	565	655	577	757
111	222	122	212	221	112	121	211	166	616
229	992	929	299	966	696	669	996	969	699
775	557	575	755	522	252	225	552	525	255
661	116	161	611	177	717	771	117	171	711

Examination of some other sets and their permutations disclosed the following forty-two additional solutions, totalling sixty-two solutions with all 186 palindromes distinct and with the three palindromes within each solution containing different digits:

955	595	559	995	959	599	933	393	339	993	939	399	944	494
477	747	774	447	474	744	455	545	554	445	454	544	588	858
233	323	332	223	232	322	277	727	772	227	272	722	133	313
449	994	949	499	988	898	889	998	989	899	911	191	119	991
885	558	585	855	411	141	114	441	414	144	288	828	882	228
331	113	131	311	266	626	662	226	262	622	466	646	664	446
919	199	877	787	778	887	878	788	866	686	668	886	868	688
282	822	633	363	336	663	636	366	422	242	224	442	424	244
464	644	155	515	551	115	151	511	377	737	773	337	373	733

Also solved by R. K. Guy, University of Malaya, Singapore; E. D. Schell, Remington Rank Univac, New York; Chih-yi Wang, University of Minnesota and the proposer.

Guy pointed out that many more solutions exist using palindromes of other than 5 digits such as:

143341	111111	119911	and	148841
19991	27172	22922		13831
3333	28382	23832		3993

A Repeated Operator

263. [January 1956] *Proposed by Chih-yi Wang, University of Minnesota.*

Define $g(z) = [(|z|+z)/2]^2$, $g^2(z) = g(g(z)), \dots, g^n(z) = g(g^{n-1}(z))$.

Show that for $z = re^{i\alpha}$, $0 < \alpha \leq \pi$, $0 \leq r \cos^2(\alpha/2) < 1$ we have $\lim_{n\to\infty} g^n(re^{i\alpha}) = 0$.

Solution by Billy J. Boyer, Murphy Army Hospital, Waltham, Massachusetts. From the definition of $g(z)$, for any real constant c,

(1) $$g(cz) = c^2 g(z)$$

Multiplying the quantity within the brackets in the expression for $g(z)$ by $e^{i\alpha/2}\, e^{-i\alpha/2}$, the expression for $g(z)$ becomes:

$$g(z) = r\cos^2(\alpha/2)\cdot re^{i}, \text{ or } g(z) = cre^{i}, \text{ where } c = r\cos^2(\alpha/2).$$

Substituting $g(z)$ for z in the defining equation for $g(z)$, we have

$$g(g(z)) = g^2(z) = [(cr + cre^{i\alpha})/2]^2 = c^2 g(z).$$

Repeated application of (1) to this last equation gives the recursion: $g^n(z) = c^{2^{n-1}} g^{n-1}(z)$, for $n \geq 2$. From this it follows by induction that $g^n(z) = c^{2^{n-2}} g(z)$. Since, by hypothesis, $0 \leq c < 1$, $\lim_{n\to\infty} g^n(z) = 0$. The additional condition, $0 < \alpha \leq \pi$, stated in the problem seems to be unnecessary.

Also solved by Waleed A Al-Salam, Duke University, North Carolina; Huseyin Demir, Dandilli Bolgesi, Turkey; R. K. Guy, University of Malaya, Singapore; Major HS Subba Rao, Defense Science Organization, New Delhi, India; Calvin A. Rogers, Colorado A and M College and the proposer.

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 solution and the source, if known.

Q 177. Prove $\left|\Sigma_1 + \sqrt{\Sigma_1^2 - \Sigma_2^2}\right| + \left|\Sigma_1 - \sqrt{\Sigma_1^2 - \Sigma_2^2}\right| = |\Sigma_1 + \Sigma_2| + |\Sigma_1 - \Sigma_2|$

[*Submitted by M.S. Klamkin*]

Q 178. Show that $\cos x = e^{-\int \tan x\, dx}$ [*Submitted by George T. Forbes*]

Q 179. Is i^i real or complex? [*Submitted by M. S. Klamkin*]

Q 180. Solve $x^4 + 4x - 1 = 0$. [*Submitted by M. S. Klamkin*].

Q 181. For $n > 1$ prove $$\sum_{i=1}^{\infty} 1/n^i = \frac{1}{n-1}$$ without the use of Geometric Progression. [*Submitted by J.M. Howell*].

Q 182. Determine a polynomial $F(x)$ of seventh degree such that $F(x) + 1$ is divisible by $(x - 1)^4$ and $F(x) - 1$ is divisible by $(x + 1)^4$. [*Submitted by M.S. Klamkin from Goursat-Hedrick,* MATHEMATICAL ANALYSIS, Vol. 1, p 32.]

ANSWERS

A. 177. Let $\Sigma_1 + \Sigma_2 = w_1^2$ and $\Sigma_1 - \Sigma_2 = w_2^2$. Then $\Sigma_1^2 - \Sigma_2^2 = w_1^2 \cdot w_2^2$

or $|w_1 + w_2|^2 + |w_1 - w_2|^2 = 2|w_1|^2 + 2|w_2|^2$

This is equivalent to the theorem that the sum of the squares of the diagonals of a parallelogram equals the sum of the squares of the sides.

A. 178.

$$d \sec x = \sec x \cdot \tan x$$

$$\frac{d \sec x}{\sec x} = \tan x$$

$$d(\log \sec x) = \tan x$$

$$\log \sec x = \int \tan x \, dx$$

$$\sec x = e^{\int \tan x \cdot dx}$$

$$\cos x = e^{-\int \tan x \, dx}$$

A. 179 Here $i^i = e^{i \log i} = e^{i[i(\pi/2+2k\pi)]} = e^{-(\pi/2+2k\pi)}$, but this is real.

A 180. $x^4 + 4x - 1 = 0$ is equivalent to $x^4 + 2x^2 + 1 - 2(x - 2x + 1) = 0$.

Thus $x^2 + 1 = \pm\sqrt{2}(x-1)$ and $x^2 \mp x\sqrt{2} + 1 \pm \sqrt{2} = 0$

so $x = \dfrac{\pm\sqrt{2} \pm \sqrt{2-4(1 \pm \sqrt{2})}}{2}$

A. 181. Write $\dfrac{1}{n-1} = \dfrac{1}{n} + \dfrac{1}{n(n-1)}$

$$= \frac{1}{n} + \frac{1}{n}\left(\frac{1}{n} + \frac{1}{n(n-1)}\right) = \frac{1}{n} + \frac{1}{n^2} + \frac{1}{n^2}\left(\frac{1}{n-1}\right)$$

$$= \frac{1}{n} + \frac{1}{n^2} + \frac{1}{n^3} + \frac{1}{n^3}\left(\frac{1}{n-1}\right),$$ and so on, each

time using the original as a recursion formula leading to:

$$\frac{1}{n-1} = \sum_{i=1}^{\infty} 1/n^i$$

A. 182. Let $F(x) + 1 = (x-1)^4 P_1$ and $F(x) - 1 = (x+1)^4 P_2$. $F(x)$ not divisible by $(x-1)(x+1)$. Multiplying we have $F(x)^2 - 1 = (x^2-1)^4 P_1 P_2$. Differentiating gives $2FF' = 8x(x^2-1)^3 P_1 P_2 + (x^2-1)^4 (P_1 P_2)'$. Thus F' is divisible by $(x^2-1)^3$ and since it is of sixth degree $F' = k(x^2-1)^3$

So $F(x) = k\left[\dfrac{x^7}{7} - \dfrac{3x^5}{5} + x^3 - x\right] + c$. The constants are determined from $F(1) = -1$, $F(-1) = 1$ so that $F(x) = \dfrac{1}{16}[5x^7 - 21x^5 + 35x^3 - 35x]$.