The following officers were elected: Chairman, Professor C. H. Ashton, Vice-Chairman, Professor Emma Hyde, Secretary-Treasurer, L. T. Dougherty.

The morning session was a joint meeting with the Kansas Association of Mathematics Teachers, Miss M. Bird Weimar, of Wichita, presiding. At this session, Professor J. O. Hassler, of Oklahoma University, spoke on the value of mathematical history to the teacher and to the pupil, and Professor E. B. Stouffer, of the University of Kansas, gave a report of the Mathematical Congress at Bologna in the Summer of 1928. At the joint luncheon of the two Associations, which followed the morning session, Professor U. G. Mitchell, of the University of Kansas, gave a very interesting talk and demonstration of "Mathematics and Poetry." In the afternoon, the Kansas Section met in separate session, the program consisting of two papers:

1. "The Gamma-function," by Professor Ashton.

2. "Some properties of Euler's phi-function," by Professor Richert.

Abstracts of these papers follow:

1. Just two hundred years ago, Euler introduced a new function, which has been the subject of many papers and a few entire volumes. Nearly a hundred years after its introduction by Euler, Legendre named it the Gamma-function. Comparatively little has been written about this function in this country, either in our books or in our journals. In this expository paper, it is defined by an integral, by infinite products, and by its difference equation, and some of its properties are discussed.

2. If m is any given positive integer, the number of integers not greater than m and prime to it, is called Euler's phi-function of m, (or indicator of m), and is denoted by $\phi(m)$. It is well known that this function is of frequent occurence in the theory of numbers. This paper deals with the fundamental properties of the phi-function.

LUCY T. DOUGHERTY, *Secretary*

CRYPTOGRAPHY IN AN ALGEBRAIC ALPHABET

By LESTER S. HILL, Hunter College

1. *The Bi-Operational Alphabet*

Let $a_0, a_1, \ldots, a_{25}$ denote any permutation of the letters of the English alphabet; and let us associate the letter a_i with the integer i. We define operations of modular addition and multiplication (modulo 26) over the alphabet as follows: $a_i+a_j=a_r$, $a_ia_j=a_t$, where r is the remainder obtained upon dividing the integer $i+j$ by the integer 26 and t is the remainder obtained on dividing ij by 26. The integers i and j may be the same or different.

It is easy to verify the following salient propositions concerning the bi-operational alphabet thus set up:

(1) If α, β, γ are any letters of the alphabet, $\alpha+\beta=\beta+\alpha$, $\alpha\beta=\beta\alpha$, $\alpha+(\beta+\gamma)=(\alpha+\beta)+\gamma$, $\alpha(\beta\gamma)=(\alpha\beta)\gamma$, $\alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma$.

(2) There is exactly one "zero" letter, namely a_0, characterized by the fact that the equation $\alpha+a_0=\alpha$ is satisfied whatever be the letter denoted by α. It should be observed that, by our definition of multiplication, if α denotes any letter of the alphabet, we have: $\alpha a_0=a_0\alpha=a_0$.

(3) Given any letter α, we can find exactly one letter β, dependent upon α, such that $\alpha+\beta=a_0$. We call β the "negative" of α, and write: $\beta=-\alpha$. Evidently, if $\beta=-\alpha$, then also $\alpha=-\beta$.

(4) Given any letters α, β we can find exactly one letter γ such that $\alpha+\gamma=\beta$. We write: $\gamma=\beta-\alpha$. It is obvious that $\beta-\alpha=\beta+(-\alpha)$; and also that if $\beta-\alpha=a_0$, then $\beta=\alpha$.

(5) Distinguishing the twelve letters, a_1, a_3, a_5, a_7, a_9, a_{11}, a_{15}, a_{17}, a_{19}, a_{21}, a_{23}, a_{25}, with subscripts prime to 26, as "primary" letters, we make this assertion, easily proved: If α is any primary letter and β is any letter, there is exactly one letter γ for which $\alpha\gamma=\beta$. We write: $\gamma=\beta/\alpha$. Each primary letter α has the "reciprocal" a_1/α, where a_1 is the "unit" letter; and the reciprocal is likewise primary. If α is primary, we shall call the "fraction" β/α "admissible." A table of the letters represented by the twelve particular admissible fractions a_1/α enables us, when used with the formula $\beta/\alpha=\beta(a_1/\alpha)$, to find immediately the letter represented by any admissible fraction.

(6) In any algebraic sum of terms, we may clearly omit terms of which the letter a_0 is a factor; and we need not write the letter a_1 explicitly as a factor in any product.

For the limited purposes of the present paper it will not be necessary to define exponential notations, etc.

2. *An Illustration*

Let the letters of the alphabet be associated with integers as follows:

a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*
5	23	2	20	10	15	8	4	18	25	0	16	13

n	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*
7	3	1	19	6	12	24	21	17	14	22	11	9

or, in another convenient formulation:

0	1	2	3	4	5	6	7	8	9	10	11	12
k	*p*	*c*	*o*	*h*	*a*	*r*	*n*	*g*	*z*	*e*	*y*	*s*

13	14	15	16	17	18	19	20	21	22	23	24	25
m	*w*	*f*	*l*	*v*	*i*	*q*	*d*	*u*	*x*	*b*	*t*	*j*

It will be seen that

$$c+x=t,\quad j+w=m,\quad f+y=k,\quad -f=y,\quad -y=f,\quad \text{etc.}$$
$$an=z,\quad hm=k,\quad cr=s,\quad \text{etc.}$$

The zero letter is k, and the unit letter is p. The primary letters are: $a\ b\ f\ j\ n\ o\ p\ q\ u\ v\ y\ z$.

Since this particular alphabet will be used several times, in the illustration of further developments, we append the following table of negatives and reciprocals:

Letter	:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Negative	:	u	o	t	r	l	y	i	x	g	p	k	e	m	q	b	j	n	d	w	c	a	z	s	h	f	v
Reciprocal	:	u	v			n			j				f	z	p	y				a	b			q	o		

The solution of the equation $z+\alpha=t$ is $\alpha=t-z$, or $\alpha=t+(-z)=t+v=f$.

The system of two linear equations: $o\alpha+u\beta=x$, $n\alpha+i\beta=q$ has the solution $\alpha=u$, $\beta=o$, which may be obtained by the familiar method of elimination or by formula (see Section 4).

3. *Concerning Determinants in the Bi-Operational Alphabet*

The determinant

$$D=\begin{vmatrix} a_{11} & a_{12}\cdots a_{1n} \\ a_{21} & a_{22}\cdots a_{2n} \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ a_{n1} & a_{n2}\cdots a_{nn} \end{vmatrix}$$

where the a_{ij} denote letters of the bi-operational alphabet defined in Section 1, has the same definition, and the same properties, as the corresponding expression in ordinary algebra—except that additions and multiplications are, of course, effected in the modular sense.

We note explicitly these properties:

I. Let δ denote the value of the n-th order determinant D; let M_{ij} denote the value of the determinant of order $n-1$ obtained from D by striking out the row and column in which the element a_{ij} lies; and let $A_{ij}=\pm M_{ij}$, the positive or negative sign being used according as the integer $i+j$ is even or odd. Then each of the sums

$$\sum_{t=1}^{n} a_{it}A_{jt}, \qquad \sum_{t=1}^{n} a_{ti}A_{tj}$$

has the value δ if $i=j$, and the value a_0 if $i\neq j$.

II. The value of D is not changed: (1) if rows and columns are interchanged; or (2) if to each element of any row (column) is added α times the corresponding element of another row (column), where α denotes any letter of the alphabet.

III. The value of D is changed only in sign (1) if two rows (columns) are interchanged; or (2) if the signs of all elements in any row (column) are changed.

IV. The value of D is not changed if the elements of any row (column) are

multiplied by any primary letter β and the elements of another row (column) by the reciprocal, a_1/β, of β.

We shall call D a "primary determinant" if its value is a primary letter. We shall not have to deal, in this paper, with determinants that are not primary.

LEMMA: *By means of properties II and III*, we may obviously convert the determinant of n-th order;

$$ {}_nI_\alpha = \begin{vmatrix} a_1 & a_0 & a_0 \cdots a_0 \\ a_0 & a_1 & a_0 \cdots a_0 \\ \cdot & \cdot & \cdots \cdot \\ \cdot & \cdot & \cdots \cdot \\ a_0 & a_0 & a_0 \cdots \alpha \end{vmatrix} = \alpha, $$

into a variety of n-th order determinants, all of which have the value α, *where* α *is any assigned letter of the alphabet.*[1] In ${}_nI_\alpha$, all elements, except those of the principal diagonal, are equal to the zero letter a_0; and all elements of that diagonal, except the last, are equal to the unit letter a_1.

We have only to make α a primary letter if we wish to set up with great ease a wide variety of n-th order primary determinants.

4. *Normal Transformations and Polygraphic Cipher Systems*

The determinant D, of n-th order, which was written out in Section 3, fixes the linear transformation with coefficients a_{ij}:

$$ (T) \qquad \begin{aligned} y_1 &= a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n, \\ y_2 &= a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n, \\ &\cdots \\ y_n &= a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n. \end{aligned} $$

We call D the determinant of the transformation T; and we say that T is a "*normal*" transformation if its determinant is primary.

THEOREM: *A normal transformation T has an unique inverse* T^{-1}, *of which the equations are*:

$$ x_i = D_i/D \,(i = 1, 2, \cdots, n), $$

where D denotes the value of the determinant of T, and D_i *denotes the value of the determinant obtained therefrom by replacing* a_{ji} by $y_j (j = 1, 2, \ldots, n)$. Moreover, T is the inverse of T^{-1}. The values of the determinants of T and T^{-1} are reciprocals (see Section 1), and therefore T^{-1} is a normal transformation.

[1] By means of II, III, IV, any assigned determinant which is of the nth order and whose value is any primary letter α can be obtained from ${}_nI_\alpha$.

Given any pair of inverse normal transformations T and T^{-1} in our bi-operational alphabet, we have a device which may be applied (1) to convert any message sequence of n letters into a corresponding cipher sequence of n letters, and (2) to convert the cipher sequence back into the message sequence from which it came. In other words, we have all the apparatus of an extraordinarily effective *polygraphic* (*n-graphic*) *cipher system*. We may regard $x_1x_2 \cdots x_n$ as the message sequence, and determine the cipher sequence $y_1y_2 \cdots y_n$ by means of T, using T^{-1} for decipherment; or we may encipher with T^{-1} and decipher with T, treating $y_1y_2 \cdots y_n$ as the message sequence and $x_1x_2 \cdots x_n$ as the cipher sequence. In either case, we begin by writing the message in sequences of n letters, as will be illustrated in Section 5.

A polygraphic cipher consisting of the inverse normal transformation of the literal sequences x_i, $y_i (i=1, 2, \ldots, n)$ may suitably be called a *linear cipher of order n*, and designated as a C_n.

5. *Illustration of Linear Ciphers*

Let us employ the particular bi-operational alphabet considered in Section 2.

EXAMPLE 1: To construct and apply a cipher of type C_3.

Selecting any primary letter, say y, we can immediately obtain from

$$ {}_3I_y = \begin{vmatrix} p & k & k \\ k & p & k \\ k & k & y \end{vmatrix} = y $$

a host of different primary determinants all of which have the value y, as pointed out in the LEMMA in Section 3. One of these is the determinant

$$ \begin{vmatrix} y & k & o \\ z & x & k \\ r & n & y \end{vmatrix} $$

of the normal transformation,

$$ (T_1) \qquad \begin{aligned} y_1 &= yx_1 + ox_3, \\ y_2 &= zx_1 + xx_2, \\ y_3 &= rx_1 + nx_2 + yx_3, \end{aligned} $$

of which the inverse,

$$ (T_1^{-1}) \qquad \begin{aligned} x_1 &= xy_1 + zy_2 + dy_3, \\ x_2 &= vy_1 + ny_2 + qy_3, \\ x_3 &= fy_1 + qy_2 + xy_3, \end{aligned} $$

is easily found. It will be observed that the values of the determinants of T_1 and T_1^{-1} are y and q respectively, and that these letters are reciprocals.

Let the message to be enciphered consist of the word *Mississippi*. Writing

this message in 3-letter sequences, and filling the last sequence with any prearranged letter, say k, we have:

$$m\ i\ s \quad s\ i\ s \quad s\ i\ p \quad p\ i\ k.$$

Substituting $m\ i\ s$ for $x_1x_2x_3$ in T_1, we find $b\ q\ t$ for $y_1y_2y_3$, thus converting the message sequence $m\ i\ s$ into the cipher sequence $b\ q\ t$. Proceeding in like manner with the other message sequences, we obtain as the enciphered form of our message: $b\ q\ t \quad s\ e\ i \quad a\ e\ p \quad y\ f\ c$. We should probably send it in the customary five-letter grouping: *bqtse iaepy fc.*

To decipher, we substitute $b\ q\ t$ for $y_1y_2y_3$ in T_1^{-1} obtaining $m\ i\ s$ for $x_1x_2x_3$. Proceeding in the same way with the other cipher sequences, we regain the entire original message.

EXAMPLE 2: To construct and apply a cipher of type C_4.

Choosing any primary letter, say j, we may construct from

$${}_4I_j = \begin{vmatrix} p & k & k & k \\ k & p & k & k \\ k & k & p & k \\ k & k & k & j \end{vmatrix} = j$$

an enormous number of different primary determinants all of which have the value j. One of these is the determinant of the normal transformation:

$$(T_2) \qquad \begin{aligned} y_1 &= gx_1 + rx_2 + zx_3 + ax_4, \\ y_2 &= rx_1 + zx_2 + ax_3 + ex_4, \\ y_3 &= ax_1 + gx_2 + hx_3 + zx_4, \\ y_4 &= ex_1 + rx_2 + yx_3 + hx_4, \end{aligned}$$

the inverse of which is easily found to be:

$$(T_2^{-1}) \qquad \begin{aligned} x_1 &= by_1 + dy_2 + ay_3 + py_4, \\ x_2 &= cy_1 + yy_2 + iy_3 + py_4, \\ x_3 &= cy_1 + dy_2 + ry_3 + jy_4, \\ x_4 &= jy_1 + cy_2 + xy_3 + jy_4. \end{aligned}$$

We note that the determinants of T_2 and T_2^{-1} have the reciprocal values j and j, the letter j being its own reciprocal.

Let the message to be enciphered be *Delay operations.* Write it in the form:

$$d\ e\ l\ a \quad y\ o\ p\ e \quad r\ a\ t\ i \quad o\ n\ s\ u,$$

filling the last sequence with any prearranged letter, say u. Substituting $d\ e\ l\ a$ for $x_1x_2x_3x_4$ in T_2, we find $j\ c\ o\ w$ as the corresponding cipher sequence $y_1y_2y_3y_4$. Proceeding in this manner, we find the enciphered form of our message to be:

$$j\ c\ o\ w \quad z\ l\ v\ b \quad d\ v\ l\ e \quad q\ m\ x\ c.$$

To decipher, we substitute $j\ c\ o\ w$ for $y_1y_2y_3y_4$ in T_2^{-1}, etc.

6. *Concluding Remarks*

A great many other cryptographic constructions can, of course, be derived from the algebra, by no means fully developed in this paper, of the bi-operational alphabet. The purpose of the paper, however, will have been accomplished if the single construction described serves to emphasize sufficiently the circumstance that sets which fail to possess in full the character of algebraic fields may still admit a large measure of amusing, and possibly useful, algebraic manipulation. It need hardly be said that if full-fledged finite algebraic fields are employed, the opportunities of the cryptographer are greatly extended; he then has at his disposal a perfectly smooth algebra and its associated geometries. The writer hopes to submit a further communication on this subject. But the number of marks in a finite field is necessarily either a prime or a power of a prime. If our alphabet is to be converted into a finite field, the best that can be done is to omit one letter, say j, to obtain a field of twenty-five marks; or to adjoin an additional symbol so that a field of twenty-seven marks is available. The bi-operational alphabet[1] of twenty-six letters, and the further development of its algebra, should therefore be of some importance in cryptography.

If polygraphic ciphers based upon normal transformations (linear ciphers) prove to be of real interest, we shall indicate a surprising way in which these ciphers may be manipulated easily and quickly, even for fairly large values of n(say $n=8$, 9, or 10), and thus made effective in a distinctly practical sense. It should be remarked that a cipher of type C_n in which $n>4$, although easy to use, is extraordinarily difficult to "break," offering very high resistance to the methods of cryptanalysis.

THE LIFE INSURANCE ACTUARY AND HIS MATHEMATICS[2]

By RAYMOND V. CARPENTER, Metropolitan Life Insurance Co.

It is estimated that the amount of life insurance in force in United States companies at the end of 1928 is about $95,000,000,000. The assets are about $16,000,000,000 and the premium collections in 1928 were over $3,000,000,000.

The employed personnel of a life insurance company consist of the field or agency force and the home office force. An important part of the home office force is the actuarial department.

The actuary has a wide range of duties. He must be reasonably familiar with the work of all departments of the company, and is sometimes called its "technical" man. His two main duties are, first, the calculation of the premiums

[1] The bi-operational alphabet employed in this paper is an example of a "ring." See the Bulletin of the National Research Council, *Report on Algebraic Numbers*, p. 59.

[2] This paper was read by invitation before the Mathematical Association of America at New York City on Dec. 29, 1928.