CONCERNING CERTAIN LINEAR TRANSFORMATION APPARATUS OF CRYPTOGRAPHY[1]

By LESTER S. HILL, Hunter College

1. *Introductory Note*

Of especial interest in systematic cryptography is the linear transformation:

$$(T)\qquad \begin{array}{l} y_1 = a_{11}x_1 + a_{12}x_2 + \cdots + a_{1f}x_f + a_1, \\ y_2 = a_{21}x_1 + a_{22}x_2 + \cdots + a_{2f}x_f + a_2, \\ \cdot \quad \cdot \quad \cdot \quad \cdots \quad \cdot \quad \cdot \\ \cdot \quad \cdot \quad \cdot \quad \cdots \quad \cdot \quad \cdot \\ y_f = a_{f1}x_1 + a_{f2}x_2 + \cdots + a_{ff}x_f + a_f, \end{array}$$

in which f is any positive integer, and the variables x_i, y_i, as well as the coefficients a_{ij} and a_i are elements of an arbitrary field, finite or infinite. But the linear apparatus which may be profitably employed is much more extensive. To meet the demands of effective cipher construction, we must often operate in sets which do not possess full field character. The necessary operational sets are really special linear associative and commutative algebras. In the present paper, we shall call these sets *scales*. For our purposes, the transformation T must be made available in any scale.

Moreover, it is highly desirable to extend the transformation T in the sense of permitting the x_i, y_i, a_{ij}, a_i to be square matrices of arbitrary order in an arbitrary scale. This enables us to convert a sequence $x_1, x_2, \cdots, x_f$ of f matrices into another sequence $y_1, y_2, \cdots, y_f$ of f matrices. The specification of conditions under which a unique inverse transformation exists will naturally be important.

When the underlying scale is of the type of most immediate cryptographic significance, namely the type $S(n)$ discussed in Section 3, the linear transformations T may be effected with extraordinary speed and accuracy by means of a mechanical device, no calculations of any sort being required. To avoid the expense of preparing machines of different structures, one for encipherment and the other for decipherment, we employ *involutory* transformations of type T(that is to say, transformations of period 2).

It is hoped that these notes will direct attention to a fascinating, although sadly neglected, domain of applied algebra.

2. *Scales*

The word *ring*[2] has been quite generally adopted to describe any finite or infinite set R, over which operations of so-called "addition" and "multiplica-

[1] *A Note by the Editor*: This paper was presented under a different title to the American Mathemathical Society at Boulder, Colorado in August, 1929. It is the second article by Professor Hill on the subject of *Cryptography* to be published in this Monthly. The first one was *Cryptography in an algebraic alphabet*, in vol. 36 (1929), pp. 306–312.

[2] See Hasse, *Höhere Algebra*, Part 1, pp. 7–9.

tion" are in any way uniquely specified, provided that: (1) R contains at least two different elements; (2) multiplication is distributive with respect to addition, and each of these two operations is associative and commutative; and (3) if α and β denote elements of R, not necessarily different, then R contains exactly one element γ such that $\alpha+\gamma=\beta$.[3]

It is readily shown that any ring R contains exactly one zero element, and we shall denote this element by 0. The zero element has the properties, the first of which is definitional and pertains only to this element, that $\alpha+0=\alpha$ and $\alpha\cdot 0=0$, where α denotes any element of R. Concerning the second of these properties, we note that there is an infinity of rings in which every product vanishes (is equal to the zero element). According to the definition given below, such rings are clearly not *scales*.

Each element α of any ring determines uniquely an element δ such that $\alpha+\delta=0$, and δ is called the "negative" of α. We write $\delta=-\alpha$, noting the obvious implication that $\alpha=-\delta$. The element γ of postulate (3) above is denoted by $\beta-\alpha$; and we observe that $\beta-\alpha=\beta+(-\alpha)$.

Let α, β, γ denote elements, not necessarily different, of a ring R. We easily see that $\alpha(-\beta)=(-\alpha)\beta=-\alpha\beta$, $(-\alpha)(-\beta)=\alpha\beta$, $\alpha(\beta-\gamma)=\alpha\beta-\alpha\gamma$; and also that each of the equations $\alpha=\beta$, $\alpha-\beta=0$, implies the other.

An element α of a ring R is a "divisor of zero" if R contains an element β different from zero ($\beta\neq 0$) such that $\alpha\beta=0$. The zero element of a ring is always a divisor of zero.

By reason of the commutativity of multiplication, a ring R can not contain more than one element ϵ such that $\epsilon\alpha=\alpha$ for every element α of R. If one such element ϵ is present, it is called the *unit element* of R, and may be conveniently denoted by 1.

In all that follows, we shall operate exclusively in those rings which we distinguish as *scales*. Hence we emphasize the definition: *A scale is a ring which contains a unit element.* If a ring R is a scale, we shall ordinarily denote it by the letter S.

Let α denote any element of a scale S. It is readily established that S can not contain more than one element β such that $\alpha\beta=1$. If one such element β is present in the scale, we call it the "reciprocal" of α, writing $\beta=1/\alpha$, and noting the implication that $\alpha=1/\beta$. An element of a scale will be classed as *regular* or *singular* according as it has, or has not, a reciprocal.

In any scale, the unit and zero elements are respectively regular and singular; and the product of two elements, not necessarily different, is regular when and only when both elements are regular. The negative and the reciprocal of a regular element are regular. *A field is a scale in which the zero is the only singular element.*

[3] When no misunderstanding can arise, we shall employ without comment the familiar terminology and notations of elementary algebra. Thus, for instance, we shall say that addition and multiplication of the elements α and β of a ring yield respectively the "sum" $\alpha+\beta$ and the "product" $\alpha\beta$.

A regular element of a scale is never a divisor of zero. In some scales, every singular element is a divisor of zero; in other scales, this is not the case.

If α is any element, and β any regular element, of a scale S, then S contains exactly one element, γ, such that $\beta\gamma=\alpha$. We write $\gamma=\alpha/\beta$, observing that, in fact, $\alpha/\beta=\alpha(1/\beta)$.

Exponential notations are easily introduced. If α is any element of a scale S, the meaning of the symbol α^n, for positive integral n, requires no comment. When n is a negative integer or zero, this symbol is defined only for the case in which α is a *regular* element of S, and the specifications in that case are: $\alpha^0=1$ (the unit element of S), $\alpha^n=(1/\alpha)^{-n}$.

It should be noted that every field is a scale, and that every scale is a ring. The following two sections will furnish examples of scales which are fields, and of scales which are not fields. There exist an infinity of rings (finite rings as well as infinite rings) which are not scales; but the present paper completely disregards such rings.

3. *Simple Examples of Scales*

It is evident that the fields of rational, real, and ordinary complex numbers furnish three examples of scales. A subscale of each of these is found in the set of all positive and negative integers and zero. This infinite subscale contains only two regular elements, namely ± 1, and only one divisor of zero, namely 0.

Of exceptional practical interest in cryptography are the finite modular scales which we here designate as of type $S(n)$. For the integer $n \geqq 2$, let $S(n)$ denote any set of n elements associated, one-to-one, with the n integers $0, 1, 2, \cdots, n-1$. If the elements α, β of $S(n)$ are associated with the integers a, b, we define:

$$\alpha+\beta=\gamma, \quad \alpha\beta=\delta$$

where γ and δ are the elements of $S(n)$ associated respectively with the *remainders* obtained upon dividing, by n, the ordinary sum $a+b$, and the ordinary product ab, of integers.

With operations thus defined, modulo n, we see that $S(n)$ is a finite scale. Its regular elements are those associated with integers prime to n. When n is prime, $S(n)$ is a field.

It will be convenient to treat, as the elements of $S(n)$, the n integers $0, 1, 2, \cdots, n-1$ themselves, regarded as mere marks or symbols.

For cipher construction, perhaps the most useful scales of the type $S(n)$ are those which correspond to $n=23$, 25, 26, 27, 36, 100, 101. The first and the last of these seven are, of course, fields.

We shall draw our illustrative material from $S(26)$. We tabulate here, for later reference, the regular elements of this scale, together with their reciprocals:

$S(26)$

Element:	1,	3,	5,	7,	9,	11,	15,	17,	19,	21,	23,	25
Reciprocal:	1,	9,	21,	15,	3,	19,	7,	23,	11,	5,	17,	25

The negative of the reciprocal of an element in any scale is the reciprocal of the negative. Thus we have here:

$$-21=1/(-5)=1/21=5;\quad -17=1/(-23)=1/3=9;\ \text{etc.}$$

Operations in $S(26)$ may be further illustrated as follows:

$3+11=14$; $17+12=3$; $9+17=0$, whence $-9=17$ and $-17=9$; $3(7)=21$, whence $21/3=7$ and[4] $21/7=3$; $7(15)=1$, whence $1/7=15$ and $1/15=7$; etc. The negative of any element is obvious: $-0=0$, $-1=25$, $-2=24$, $-3=23$, etc.

4. *Scales Obtained by Algebraic Extension of Other Scales*

The theory of polynomials in any *field* is so familiar a chapter of modern algebra that not very much needs to be said here concerning polynomials in an arbitrary *scale* S (polynomials with "coefficients" which are elements of S). We note only a few points of special interest. A polynomial in a scale S is conveniently distinguished as *primary* if the coefficient in the term of highest "degree" is a *regular* element of S. Each element α of S is regarded as a polynomial in S, degrees being as follows: (1) when $\alpha\neq 0$, it is a polynomial of degree zero; and (2) when $\alpha=0$, it is a polynomial of degree[5] -1. Regular and singular elements of S, regarded as polynomials in S, are classed respectively as primary and non-primary.

We note that the degree of the product of two polynomials in a scale is equal to the sum of their degrees whenever at least one of the polynomials is primary and the other is not the polynomial 0 (of degree -1). We record also this fundamental *division property*:

Let S be any scale, finite or infinite. Let P denote any polynomial, and D any *primary* polynomial, in S. There are uniquely determined two polynomials Q and R in S, the latter of degree less than the degree of D, such that $P=QD+R$.

It is convenient to designate R as the *residue of P, modulo D*; and to write: $R=\text{Res}\ (P, \text{mod}\ D)$. If the degree of P is less than that of D, we see at once that[6] $\text{Res}\ (P, \text{mod}\ D)=P$.

Let us now select, as a modulus, any polynomial N, in S, which is primary and of degree $n\geqq 2$. It is easy to define addition and multiplication over the set U of all polynomials in S which have degrees less than n, *in such manner that U will be closed under these operations and will constitute a scale.* We need merely specify,[7] as the sum of two polynomials A, B of U, the sum $A+B$ in S;

[4] Similarly since $17(18)=20$ we might expect to have $20/17=18$ and $20/18=17$; but such is not the case, for while $17(18)=20$ implies $20/17=18$, it does not imply $20/18=17$. The element 18 is singular, and $20/18$ is not defined.

[5] Any other negative real number would serve equally well, for our purposes, to mark the degree of the polynomial 0. We wish merely to signalize that the "degree" of this polynomial is to be regarded as less than that of any other polynomial in S.

[6] In this case, Q is the polynomial 0, and $R=P$.

[7] For the case in which the scale S is a field, this procedure is very familiar. In this case, every polynomial in S, except the polynomial 0, is primary. But to obtain a scale U which is a field, we must employ, as modulus N, a primary polynomial *irreducible* in the field S.

and as the product, the polynomial Res (AB, mod N), where AB is the product in S.

The scale U plainly contains a subset V which is a scale simply isomorphic with the scale S. The scale V consists of those polynomials of U each of which is represented by an element of S. In this sense, we may regard U as an *extension* of S.

It is evident that when the scale S is finite, consisting of k elements, the scale U will likewise be finite, consisting of k^n elements, where n is the degree of the modulus N.

For the benefit of those readers who may not be experienced in manipulations of the character here considered, we append two examples.

Example 1: Let $S=S(2)$, of which the elements[8] are 0 and 1. Let $N=x^2+x+1$. The elements of U are the four polynomials 0, 1, x, $x+1$ in $S(2)$. Denoting these elements by a, b, c, d respectively, we find that:

$$c + d = x + (x + 1) = 1 = b; \quad cd = \text{Res}\,(x^2 + x, \ \text{mod}\ N) = 1 = b; \text{ etc.}$$

Since, in this case, S is a field, and N is irreducible in S, the scale U is a field. Its operation tables in full are:

Addition

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Multiplication

	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	d	b
d	a	d	b	c

The zero element is a, and the unit element is b. Every element is its own negative.[9]

For variety, let us select a modulus which is reducible in $S(2)$, say $N'=x^2+1$. We are led to a scale U', the operation tables of which, aside from the four products, $cc=b$, $cd=dc=d$, $dd=a$, are exactly the same as those of U. The zero and unit elements are again a and b, respectively. There is a singular element other than the zero, namely d, and U' is therefore not a field.

Example 2: Let $S=S(6)$, of which the six elements are:

$$0;\ 1 = -5;\ 2 = -4;\ 3 = -3;\ 4 = -2;\ 5 = -1.$$

In this case, S is not a field; it contains the four singular elements, 0, 2, 3, 4.

For adequate illustration, we employ three moduli $N_1=x^2-1$, $N_2=x^2-2$, $N_3=x^2-x-1$, leading to the three scales U_1, U_2, U_3, respectively. The elements of each of these scales are the thirty-six polynomials $\alpha+\beta x$ in $S(6)$, where α and β denote any elements of $S(6)$. Interesting light is thrown upon the structural

[8] See Section 3, above. We shall take, as the elements of $S(n)$, the n integers $0, 1, 2, \cdots, n-1$ themselves, adding and multiplying modulo n.

[9] This is true in $S(2)$, and in every scale obtained from $S(2)$ by algebraic extension.

relations of U_1, U_2, U_3 by the following table, which exhibits the reciprocals of all regular elements. For convenience of tabulation, $\alpha+\beta x$ is compactly indicated by[10] $\alpha\beta$.

TABLE

Element	00	10	20	30	40	50	01	11	21	31	41	51
Recip. in U_1		10				50	01					
Recip. in U_2		10				50		51				11
Recip. in U_3		10				50	51	25	31	21	55	01

Element	02	12	22	32	42	52	03	13	23	33	43	53
Recip. in U_1				32					23		43	
Recip. in U_2		52		34		12		13				53
Recip. in U_3		32		12		14		43	53		13	23

Element	04	14	24	34	44	54	05	15	25	35	45	55
Recip. in U_1				34								
Recip. in U_2		54		32		14		55				15
Recip. in U_3		52		54		34	15	05	11	45	35	41

The table is easily interpreted. Thus, for example, it shows at a glance that the element $4+2x$ is singular in each of the three scales U_1, U_2, U_3; and that the element $5+2x$ is singular in U_1, but regular in U_2 and U_3 (with the reciprocals $1+2x$ and $1+4x$, respectively). The scales U_1, U_2, U_3, although of the same order,[11] are of very different structures; in fact, they contain respectively *seven, fourteen,* and *twenty-four regular* elements.

From the standpoint of cryptanalysis, it is especially significant that finite scales of the same order r and of widely divergent structures may be so easily specified in this manner.[12] Two finite *fields* of the same order are well known to be algebraically identical. The present section will serve to emphasize that there is an infinity of finite *scales* in which order does not completely determine structure.

5. *Rational Manipulations in a Scale*

It is very readily argued that, with only minor and obvious reservations, all the rational operations and apparatus incidental to the solution, when unique solutions exist, of systems of linear equations in a field are applicable in any scale.

We are especially interested in noting the existence, in any scale, of a full matric algebra of familiar type. The following comments on determinants and matrices in an arbitrary (finite or infinite) scale will not be amiss.

[10] The reader will hardly confuse the symbol $\alpha\beta$, used only in the present example, with the product $\alpha\beta$ of elements of $S(6)$.

[11] By the "order" of a finite scale, we understand the number of elements contained in the scale.

[12] When $r=k^n$, with k and n positive integers each greater than 1.

The determinant

$$L = \begin{vmatrix} a_{11} & a_{12} \cdots a_{1n} \\ \cdot & \cdot \cdot \cdot \cdot \\ \cdot & \cdot \cdot \cdot \cdot \\ \cdot & \cdot \cdot \cdot \cdot \\ a_{n1} & a_{n2} \cdots a_{nn} \end{vmatrix},$$

of order n, in which the a_{ij} denote elements of the scale S, has the same meaning and properties as if S were a field. We define L to be *regular* or *singular* according as its "value" is a regular or a singular element of S, where its "value" is fixed by any one of the $2n$ equal expressions in S,

$$\sum_{i=1}^{n} a_{ij}A_{ij}, \quad \sum_{j=1}^{n} a_{ij}A_{ij}, \qquad i, j = 1, 2, \cdots, n,$$

in which A_{ij} denotes the cofactor (algebraic complement) of a_{ij} in L.

Moreover, L is called the determinant of the square matrix

$$M = \begin{pmatrix} a_{11} & a_{12} \cdots a_{1n} \\ \cdot & \cdot \cdot \cdot \cdot \\ \cdot & \cdot \cdot \cdot \cdot \\ \cdot & \cdot \cdot \cdot \cdot \\ a_{n1} & a_{n2} \cdots a_{nn} \end{pmatrix} = (a_{ij})$$

of order n in S; and M is classed as *regular* or *singular* with L.

Upon occasion, we shall regard each element of the scale S as a matrix of order $n=1$ in S. The set, $SR\{n\}$, of all square matrices of order n in S will be called a *range* of matrices in S. When no misunderstanding can arise concerning the scale S employed, the range of order n in S will be denoted simply by $R\{n\}$. It is clear that $R\{1\}$ consists of all elements of the scale S regarded as matrices of the first order in S.

When $n>1$, a non-commutative algebra may be set up in the range $R\{n\}$ of the scale S. The procedure is a very familiar one,[13] but may be briefly recalled here:

(1) If $A=(a_{ij})$ and $B=(b_{ij})$ are matrices of the range $R\{n\}$ in the scale S, we define $A=B$ when and only when $a_{ij}=b_{ij}$ in S for every pair of indices i, j; and we define addition and multiplication as follows, operations affecting elements a_{ij}, b_{ij}, c_{ij} of S being performed, of course, under the rules of S:

$$A + B = (a_{ij}) + (b_{ij}) = C = (c_{ij}), \text{ with } c_{ij} = a_{ij} + b_{ij}.$$

$$AB = (a_{ij})(b_{ij}) = D = (d_{ij}), \text{ with } d_{ij} = \sum_{q=1}^{n} a_{iq}b_{qj}.$$

[13] The procedure is familiar for the case in which the scale S is a field. When S is not a field, certain precautions must be taken, as will be indicated.

From these definitions it is easy to conclude that, if A, B, C are any matrices of the range $R\{n\}$,

$$A + B = B + A, \quad A + (B + C) = (A + B) + C,$$
$$A(BC) = (AB)C, \quad A(B + C) = AB + AC.$$

But, in general, $AB \neq BA$.

(2) Let β be any element of the scale S. That matrix of the range $R\{n\}$ in S which has the scalar β in each place of the principal diagonal, and the scalar 0 everywhere else, may be called the *scalar matrix* of β, and may conveniently be denoted by β_n.

(3) If A is any matrix of $R\{n\}$ in S, and β is any scalar in S, each of the mixed products βA and $A\beta$ is defined to be the matrix obtained upon multiplying every element of A by β. It is evident that

$$\beta A = \beta_n A = A\beta_n = A\beta.$$

(4) The range $R\{n\}$ in S contains an unique *zero matrix* 0_n, and an unique *unit matrix* 1_n, such that if A is any matrix of the range,

$$A + 0_n = A, \; A0_n = 0_n A = 0_n, \; A1_n = 1_n A = A.$$

These special matrices are merely the scalar matrices of the scalars 0 and 1.

(5) Corresponding to any matrix A of $R\{n\}$ in S, there is exactly one matrix $B = -A$ such that $A + B = 0_n$. The matrix, $-A$, is the mixed product of the matrix A and the scalar -1.

(6) Corresponding to any matrices A and B of the range $R\{n\}$ in S, there is exactly one matrix $C = B - A$ of the range such that $A + C = B$. Clearly, $B - A = B + (-A)$.

(7) If the matrix A of $R\{n\}$ in S is *regular*, there is exactly one matrix B of the range such that $AB = 1_n$; and B also satisfies the equation $BA = 1_n$. We call B the *reciprocal* of A, and write $B = A^{-1}$. If $B = A^{-1}$, then also $A = B^{-1}$.

(8) Let the matrix A of the range $R\{n\}$ in S be *regular*, and let M be any matrix of the range. Then $R\{n\}$ contains exactly one matrix H, and exactly one matrix K, such that $AH = M = KA$. In fact, it is clear that $H = A^{-1}M$ while $K = MA^{-1}$.

(9) The reciprocal of the *regular* matrix $A = (a_{ij})$ of $R\{n\}$ in S is easily written out; it is simply:

$$A^{-1} = \left(\begin{array}{ccc} \frac{A_{11}}{\rho} & \cdots & \frac{A_{n1}}{\rho} \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ \frac{A_{1n}}{\rho} & \cdots & \frac{A_{nn}}{\rho} \end{array} \right) = \frac{1}{\rho} \left(\begin{array}{ccc} A_{11} & \cdots & A_{n1} \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ A_{1n} & \cdots & A_{nn} \end{array} \right),$$

where A_{ij} is the cofactor of a_{ij} in the determinant of A, and ρ is the value of that determinant as worked out in the scale S. A singular matrix has no reciprocal.

(10) If we agree to interpret the mixed sum $\beta+A=A+\beta$, where β is a scalar in S and A is a matrix of the range $R\{n\}$ in S, as the sum $\beta_n+A=A+\beta_n$ of matrices of $R\{n\}$, then in any expression like

$$c+\sum_{q=1}^{m}a_qx_q,$$

where c, a_q, x_q are matrices of $R\{n\}$, we may replace any scalar matrix by its corresponding scalar.

(11) Exponential notations will be self-explanatory. We note, however, that the symbol A^{-q}, where A is a matrix of the range $R\{n\}$ in the scale S, and q is a positive integer or zero, is not defined unless A is regular. When A is regular, $A^0=1_n$, $A^{-q}=(A^{-1})^q$.

We are now prepared to discuss a novel class of ciphers associated with the general linear transformation in the general range $R\{n\}$ of the general scale S. It will be necessary, of course, to employ only such transformations as have unique inverses. Also it will be very desirable, for practical reasons, to make easily available a large class of *involutory* transformations.

6. *Linear Transformations in the General Range*

Consider the linear transformation T_a:

$$\begin{aligned} y_1 &= a_{11}x_1+a_{12}x_2+\cdots+a_{1f}x_f+a_1,\\ &\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\\ &\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\\ y_f &= a_{f1}x_1+a_{f2}x_2+\cdots+a_{ff}x_f+a_f, \end{aligned}$$

where f is any positive integer, and the x_i, y_i, a_{ij}, a_i are matrices of any range $R\{n\}$ in any scale S. All operations required to effect this transformation are to be performed in the range $R\{n\}$.

If $n>1$, the algebra of $R\{n\}$ is non-commutative, as explained in Section 5. The range $R\{1\}$ coincides with the scale S itself, and the algebra of this range with the (commutative) algebra of S. When $n=1$, it is clear that T_a is merely a scalar transformation, the variables and the coefficients being elements of the scale S.

In all that follows, we shall understand the range $R\{n\}$ to include the underlying scale S as the special range $R\{1\}$. The transformation T_a converts a sequence of f matrices of the general range $R\{n\}$ into another such sequence. But when $n=1$, the matrices are of order 1, and are therefore merely *scalars* (elements of the scale S).

The rectangular array of $f(f+1)$ matrices,

$$P_a = \begin{bmatrix} a_{11} \cdots a_{1f} & a_1 \\ \cdot \quad \cdot \cdot \cdot \cdot & \cdot \\ \cdot \quad \cdot \cdot \cdot \cdot & \cdot \\ a_{f1} \cdots a_{ff} & a_f \end{bmatrix},$$

will be called the *schedule* of T_a, and will be designated as $P_a = [(a_{ij}), a_i]$. The square array of f^2 matrices $M_a = (a_{ij})$ will be called the *basis* of T_a.

We denote by J the set of all transformations which can be obtained in this way, for a fixed integer f, from the range $R\{n\}$ in the scale S. Let T_a, with $P_a = [(a_{ij}), a_i]$, and T_b, with $P_b = [(b_{ij}), b_i]$, be two transformations of the set J. Applying T_a to a sequence of f matrices $x_1, x_2, \cdots, x_f$ of $R\{n\}$ in S, we obtain the sequence $y_1, y_2, \cdots, y_f$ of matrices of the same range; applying T_b to the sequence $y_1, y_2, \cdots, y_f$, we obtain the sequence $z_1, z_2, \cdots, z_f$; compactly: $T_a(x) = y$, $T_b(y) = z$. The set J evidently contains an unique transformation T_c, with $P_c = [(c_{ij}), c_i]$, such that $T_c(x) = z$. We say that T_c is the *product* T_bT_a, distinguishing this product from T_aT_b. It is quickly found that

$$c_{ij} = \sum_{q=1}^{f} b_{iq}a_{qj}, \quad c_i = b_i + \sum_{q=1}^{f} b_{iq}a_q, \tag{1}$$

the operations required for calculation by these formulas being effected according to the algebra of the range $R\{n\}$.

It is readily shown that products of transformations in J are associative; if T_a, T_b, T_c are any transformations in J, then $T_a(T_bT_c) = (T_aT_b)T_c$.

7. *A Fundamental Lemma*

Let T_a, with the schedule $P_a = [(a_{ij}), a_i]$, be a transformation belonging to the set J considered in Section 6. We fix our attention upon the *basis* $M_a = [a_{ij}]$ of T_a. If parentheses are removed from all the f^2 matrices in the square array $[a_{ij}]$, there results a square matrix G_a in the scale S, of order $g = fn$. The matrix G_a will be called the *frame matrix* of T_a. It is evident that G_a belongs to the range $R\{g\}$ in the scale S.

The following lemma is fundamental. It may be established by a straightforward argument which will be omitted here.

Lemma: Let T_a, T_b, T_c be transformations in J; and let their frame matrices be G_a, G_b, G_c respectively. Then $G_c = G_aG_b$ if[14] $T_c = T_aT_b$. In other words, *the frame matrix of a product of transformations is the corresponding product of the frame matrices of the transformations.*

8. *Regular Transformations in J.*

We consider now the set H of all those transformations in the set J which have *regular* frame matrices. We say that H is the set of *regular transformations* in J.

[14] Two transformations of the set J are "equal" when their schedules are exactly the same.

It is clear that H contains the identical transformation, defined by the schedule $Q=[(a_{ij}), a_i]$ in which $a_{ij}=1_n(i=j)$, $a_{ij}=0_n(i\neq j)$, $a_i=0_n$ (every index i). Here, as heretofore, we employ the designations 0_n and 1_n respectively for the zero and unit matrices of the range $R\{n\}$ in S.

By an argument based upon the *lemma*, a significant theorem may now be established:

Theorem 1: If T_a is any transformation in H, there exists, in H, an unique transformation T_b such that the schedule of the product T_aT_b is Q; and Q is likewise the schedule of the product T_bT_a.

This theorem asserts that (1) any *regular* transformation T in J has an unique inverse T^{-1}, and (2) T^{-1} is regular and has T for its inverse.

Proof: We suppose, first, that T_a is any *homogeneous* transformation in H (any transformation in H with the schedule $[(a_{ij}), a_i]$ in which $a_i=0_n$, the zero matrix of the range $R\{n\}$, for every index i). The frame matrix G_a of T_a is regular, and has an unique reciprocal[15] G_a^{-1} in the range $R\{g\}$. Hence that homogeneous transformation T_b of J which has the frame matrix G_a^{-1} is regular, and lies in H. By the *lemma*, T_b is manifestly an unique inverse to T_a in the set H.

Now let T_a be any transformation in H. Let $y_i=z_i+a_i$ $(i=1, 2, \cdots, f)$, these sums being formed, of course, in the range $R\{n\}$ of matrices. Substituting in the equations of T_a, we obtain the equations of a transformation T_c in H—a transformation converting the sequence $x_1, x_2, \cdots, x_f$ into the sequence $z_1, z_2, \cdots, z_f$. Since T_c is of homogeneous type, it has an unique inverse T_c^{-1}. Replacing z_i, in the equations of T_c^{-1}, by y_i-a_i, and simplifying (by operations in the range $R\{n\}$), we determine the equations of a transformation T_a^{-1} which is the unique inverse of T_a in H.

The argument is completed by the observation that if G_a, G_b denote any two matrices, of the range $R\{g\}$, such that $G_aG_b=1_g$, the unit matrix of the range, then also $G_bG_a=1_g$ (See 7, Section 5).

We have thus a procedure for the actual determination of the equations of the inverse transformation of which the existence is asserted, the required operations being performed *in the underlying scale S itself.* As will be indicated in examples below, it is frequently possible and convenient to find the inverse transformation by elimination processes carried out *in the range* $R\{n\}$, without descending to the scale S.

The set H obviously constitutes a *group* of transformations, this group being finite if the scale S is finite.

9. *Construction of Transformations of the Group H*

The following modifications of a matrix of any range in any scale will be called *elementary*:

(1) interchanging rows and columns; (2) adding, to every element of any row (column), α times the corresponding element of another row (column),

[15] See (9), Section 5.

where α denotes any scalar (element of the underlying scale S); (3) multiplying every element of any row (column) by a *regular* scalar, and every element of another row (column) by the reciprocal of that scalar; (4) interchanging two rows (columns); (5) changing the sign of every element of a row (column).

The value of the determinant of the matrix is, of course, not changed by (1), (2), or (3); and is changed only in sign by (4) or (5).

Now consider the special matrix ${}_gI_\beta$ of the range $R\{g\}$ in the scale S. This matrix is so defined that it differs from the unit matrix 1_g of the range only at the intersection of the last (g-th) row and last column, where it has the scalar β instead of the scalar 1. Successions of elementary modifications may evidently be applied to ${}_gI_\beta$ in such manner as to alter its appearance completely, while leaving the value, β, of its determinant unchanged. Selecting, as β, any *regular* element of the scale S, we have the means of constructing, quickly and easily, a variety of regular matrices of the range $R\{g\}$. We may, of course, use any one of these as the frame matrix of a transformation in the group H.

10. *Involutory Transformations of the Group H*

Let us call a transformation T, in J, *involutory* if T^2 (that is, TT) is the identical transformation, so that the schedule of T^2 is Q. When T is involutory, the determinant of the frame matrix of T^2 evidently has the value 1 in the scale S. Since the value of the determinant of a product of square matrices is obviously the product of the values of their determinants, we conclude that the value, δ, of the determinant of the matrix of T satisfies the equation $\delta^2=1$ in S. It follows that δ is a *regular*[16] element of S, and therefore that T is regular. Hence any involutory transformation in J is regular, and lies in the group H.

The following theorem is evident:

Theorem 2: If T_1 is an involutory transformation, and T any transformation, in H, then each of the transformations TT_1T^{-1} and $T^{-1}T_1T$ is involutory, and lies[17] in H.

For many cryptanalytic purposes, the following is an involutory transformation of sufficient complexity:

$$y_i = x_i - \lambda_i\tau\left(\sum_{j=1}^{f}\lambda_j x_j + \mu\right), \tag{2}$$

where $i=1, 2, 3, \cdots, f$; and $\lambda_1, \lambda_2, \cdots, \lambda_f, \mu$ is any sequence of $f+1$ matrices selected quite arbitrarily from the range $R\{n\}$ in the scale S; provided that

$$\sigma = \sum_{i=1}^{f}\lambda_i^2$$

is a *regular* matrix, and $\tau=2\sigma^{-1}$, the symbol 2 denoting the element $1+1$ of the

[16] The equation $\delta^2=1$, in an arbitrary scale S, does not imply $\delta=\pm 1$. For example, in the scale $S(100)$, this equation has the four roots 1, 49, 51,99 (that is to say, ±1 and ±49).

[17] We have just noted that every involutory transformation in J lies in the group H.

scale S (so that τ is the sum of two matrices, each equal to the reciprocal of σ).[18]

Operations required for the application of formula (2) are to be performed in the range $R\{n\}$ of matrices in the scale S. We easily verify that the formula gives the equations of a transformation which is involutory. In fact, making two applications of this transformation, we obtain:

$$\begin{aligned} z_i &= y_i - \lambda_i\tau\left(\sum\lambda_j y_j + \mu\right) \\ &= x_i - \lambda_i\tau\left(\sum\lambda_j x_j + \mu\right) - \lambda_i\tau\left\{ \sum\lambda_j\left[x_j - \lambda_j\tau\left(\sum\lambda_q x_q + \mu\right)\right] + \mu\right\} \\ &= x_i - \lambda_i\tau \sum\lambda_j x_j - \lambda_i\tau\mu - \lambda_i\tau\left\{ \sum\lambda_j x_j - \sum\lambda_j^2\tau\left(\sum\lambda_q x_q + \mu\right) + \mu\right\} \\ &= x_i - \lambda_i\tau \sum\lambda_j x_j - \lambda_i\tau\mu - \lambda_i\tau \sum\lambda_j x_j + \lambda_i\tau\sigma\tau \sum\lambda_q x_q + \lambda_i\tau\sigma\tau\mu - \lambda_i\tau\mu \\ &= x_i - 2\lambda_i\tau \sum\lambda_j x_j - 2\lambda_i\tau\mu + 2\lambda_i\tau \sum\lambda_j x_j + 2\lambda_i\tau\mu = x_i. \end{aligned}$$

In other words, if we denote the transformation (2) by T, we have $T(x)=y$ and $T(y)=x$, so that $T^2(x)=x$.

The reductions made in the above verification of the involutory character of the transformation (2) will be easily understood if the reader bears in mind that $\tau\sigma=2_n$, where 2_n denotes the scalar matrix, in $R\{n\}$, of the scalar $2=1+1$ of S, and may be replaced by the scalar 2. It should also be recalled that in a mixed product of matrices and scalars we may, as explained in Section 5, shift the position of a scalar factor.

11. *Notations and Procedure in Examples*

Our illustrations will be based upon the scale $S(26)$. We shall give examples of ciphers based upon linear transformations in ranges of this scale. The extension of the method to other scales will be obvious, and will not require explicit treatment.

The following particular correspondence between $S(26)$ and the letters of the English alphabet will be adopted:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
m	*j*	*d*	*x*	*a*	*h*	*o*	*u*	*c*	*z*	*q*	*e*	*t*	*y*	*f*	*w*	*g*	*i*	*v*	*s*	*k*	*p*	*l*	*r*	*n*	*b*

or, in alphabetical arrangement:

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*
4	25	8	2	11	14	16	5	17	1	20	22	0	24	6	21	10	23	19	12	7	18	15	3	13	9.

Any one of the 26! possible correspondences would serve equally well. But, to be explicit, we shall employ the foregoing.

The symbol ${}_nT_f$ will designate a transformation T which is performed in the range $R\{n\}$ of the scale $S(26)$, and is defined by f equations; such a transformation will convert a sequence of f matrices of $R\{n\}$ into another such sequence.

[18] Sections 13 and 14 present examples of the effective use of this formula.

Let it be desired to encipher a message by means of a transformation of the type ${}_nT_f$. Let the message be: $t_1, t_2, t_3, \cdots$, the t_i denoting simply the successive letters of the message as it is written out. Replacing the t_i by their corresponding elements of $S(26)$, we obtain the scalar sequence $q_1, q_2, q_3, q_4, \cdots$.

We now partition the q-sequence into subsequences of $k=n^2f$ elements each, writing $q_1q_2, \cdots, q_{k+1}\, q_{k+2}, \cdots, q_{2k+1}\, q_{2k+2}, \cdots$. If the last subsequence is incomplete, we fill it out, in any prearranged manner, to k elements.

Each subsequence is enciphered in the same way. The encipherment is accomplished by writing the subsequence, according to any convention, as a sequence of f square matrices, each of order n, in the scale $S(26)$, and subsequently transforming this sequence $x_1, x_2, \cdots, x_f$ of matrices, through a transformation of type ${}_nT_f$, into the sequence $y_1, y_2, \cdots, y_f$ of matrices. To decipher, we apply to the sequence $y_1, y_2, \cdots, y_f$ the transformation inverse to that used in encipherment.

The cipher subsequence actually transmitted is, of course, not the sequence $y_1, y_2, \cdots, y_f$ of matrices in $S(26)$, but the corresponding sequence of n^2f letters of the alphabet.

12. *Example 1*

The determinant of the matrix

$$\begin{pmatrix} 5 & 0 & 0 & 4 \\ 1 & 1 & 0 & 0 \\ 3 & 2 & 1 & 0 \\ 9 & 0 & 0 & 3 \end{pmatrix}$$

has the value[19] 5 in $S(26)$. Hence this matrix is regular; and the transformation

$$y_1 = \begin{pmatrix} 5 & 0 \\ 1 & 1 \end{pmatrix} x_1 + \begin{pmatrix} 0 & 4 \\ 0 & 0 \end{pmatrix} x_2 + \begin{pmatrix} 1 & 5 \\ 4 & 3 \end{pmatrix}, \tag{1}$$

$$y_2 = \begin{pmatrix} 3 & 2 \\ 9 & 0 \end{pmatrix} x_1 + \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} x_2 + \begin{pmatrix} 2 & 0 \\ 1 & 6 \end{pmatrix}, \tag{2}$$

of which it is the frame matrix, is regular. In this transformation, which we shall denote by T_1, the terms

$$\begin{pmatrix} 1 & 5 \\ 4 & 3 \end{pmatrix} \text{ and } \begin{pmatrix} 2 & 0 \\ 1 & 6 \end{pmatrix}$$

are, of course, chosen quite arbitrarily from the matrices of the range $R\{2\}$ in $S(26)$.

We readily find that the inverse transformation, T_1^{-1}, has these equations:

[19] See Section 9.

$$x_1 = \begin{pmatrix} 11 & 0 \\ 15 & 1 \end{pmatrix} y_1 + \begin{pmatrix} 0 & -6 \\ 0 & 6 \end{pmatrix} y_2 + \begin{pmatrix} -5 & 7 \\ 1 & 16 \end{pmatrix}, \tag{3}$$

$$x_2 = \begin{pmatrix} 15 & -2 \\ -7 & 0 \end{pmatrix} y_1 + \begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix} y_2 + \begin{pmatrix} 11 & -1 \\ 6 & 3 \end{pmatrix}, \tag{4}$$

there being, throughout the work in $S(26)$, two alternative expressions for each element of the scale $(21 = -5,\ 19 = -7$, etc.).

The equations (3) and (4) may be found by a simple elimination process in the range $R\{2\}$. The coefficient of x_2 in (2) is regular, and has the reciprocal[20]

$$\frac{1}{3}\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} = 9\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 9 \end{pmatrix}.$$

Left-hand multiplication of each term of (2) by the product,

$$\begin{pmatrix} 0 & 4 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 9 \end{pmatrix} = \begin{pmatrix} 0 & 10 \\ 0 & 0 \end{pmatrix},$$

yields an equation which we subtract from (1), obtaining

$$y_1 - \begin{pmatrix} 0 & 10 \\ 0 & 0 \end{pmatrix} y_2 = \begin{pmatrix} -7 & 0 \\ 1 & 1 \end{pmatrix} x_1 + \begin{pmatrix} -9 & -3 \\ 4 & 3 \end{pmatrix}. \tag{5}$$

The coefficient of x_1 in (5) being regular, we easily solve for x_1 in terms of y_1 and y_2. Then (4) is deduced in obvious manner.

In this example, $n = f = 2$. Given a message for encipherment, we first arrange it in subsequences of $n^2 f = 8$ letters each, filling out the last subsequence, if necessary, by the adjunction of further letters according to the conventions of the cipher. Let the message be, for instance, SUSPEND ATTACK, so that the initial subsequence is SUSPENDA. Let it be agreed, as a cipher prearrangement, to write:

$$\begin{pmatrix} S & U \\ S & P \end{pmatrix}, \quad \begin{pmatrix} E & N \\ D & A \end{pmatrix},$$

thus determining the two matrices in $S(26)$,

$$x_1 = \begin{pmatrix} 19 & 7 \\ 19 & 21 \end{pmatrix}, \quad x_2 = \begin{pmatrix} 11 & 24 \\ 2 & 4 \end{pmatrix},$$

by means of the correspondence adopted in Section 11. Applying the transformation T_1 to the sequence x_1, x_2 of matrices, we obtain the sequence y_1, y_2:

$$y_1 = \begin{pmatrix} 17 & 9 \\ 12 & 2 \end{pmatrix} + \begin{pmatrix} 8 & 16 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 5 \\ 4 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 4 \\ 16 & 5 \end{pmatrix},$$

$$y_2 = \begin{pmatrix} 17 & 11 \\ 15 & 11 \end{pmatrix} + \begin{pmatrix} 11 & 24 \\ 6 & 12 \end{pmatrix} + \begin{pmatrix} 2 & 0 \\ 1 & 6 \end{pmatrix} = \begin{pmatrix} 4 & 9 \\ 22 & 3 \end{pmatrix}.$$

[20] See (9), Section 5.

Returning to the alphabet, we replace the sequence y_1, y_2 of matrices by

$$\begin{pmatrix} M & A \\ G & H \end{pmatrix}, \quad \begin{pmatrix} A & Z \\ L & X \end{pmatrix};$$

and the enciphered form of the initial message subsequence is *M A G H A Z L X*. In decipherment, we apply the transformation T_1^{-1} to the sequence y_1, y_2 of matrices, obtaining again the original matrix sequence x_1, x_2, and therewith also the original message subsequence *SUSPENDA*. The same procedure is followed with each message subsequence.

13. *Example 2*

If a cipher transformation can be made involutory without an appreciable weakening of the resistance offered to cryptanalysis, it is desirable, for many reasons, that this be done. Let us construct an involutory transformation of type ${}_2T_2$, employing formula (2), Section 10. Taking

$$\lambda_1 = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, \quad \lambda_2 = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}, \text{ and } \mu = \begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix},$$

we find that

$$\sigma = \lambda_1^2 + \lambda_2^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 9 & -1 \\ 5 & 14 \end{pmatrix} = \begin{pmatrix} 10 & -1 \\ 5 & 15 \end{pmatrix}$$

is regular. Thus we have:

$$\sigma^{-1} = \begin{pmatrix} 11 & -1 \\ 5 & 16 \end{pmatrix} \text{ and } \tau = 2\sigma^{-1} = \begin{pmatrix} 22 & -2 \\ 10 & 6 \end{pmatrix}.$$

It follows that:

$$-\lambda_1\tau = \lambda_1(-\tau) = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 4 & 2 \\ 16 & 20 \end{pmatrix} = \begin{pmatrix} 4 & 2 \\ 14 & 8 \end{pmatrix}$$

$$-\lambda_2\tau = \lambda_2(-\tau) = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 4 & 2 \\ 16 & 20 \end{pmatrix} = \begin{pmatrix} 10 & 0 \\ 0 & 10 \end{pmatrix}.$$

Therefore, by formula (2) of Section 10, the following transformation, which we shall call T_2, is involutory:

$$y_1 = x_1 + \begin{pmatrix} 4 & 2 \\ 14 & 8 \end{pmatrix} \left[\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} x_1 + \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} x_2 + \begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix} \right],$$

$$y_2 = x_2 + \begin{pmatrix} 10 & 0 \\ 0 & 10 \end{pmatrix} \left[\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} x_1 + \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} x_2 + \begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix} \right].$$

Its equations may be expressed:

$$(1)\qquad y_1 = \begin{pmatrix} 7 & -2 \\ -4 & -7 \end{pmatrix} x_1 + \begin{pmatrix} 10 & 0 \\ 10 & 16 \end{pmatrix} x_2 + \begin{pmatrix} -4 & 10 \\ 12 & 10 \end{pmatrix}$$

$$(2)\qquad y_2 = \begin{pmatrix} 10 & 0 \\ 10 & 16 \end{pmatrix} x_1 + \begin{pmatrix} -5 & -2 \\ 10 & 5 \end{pmatrix} x_2 + \begin{pmatrix} 16 & -6 \\ 0 & 10 \end{pmatrix}$$

the use of negatives being avoidable if only positive signs are desired.

The equations of T_2^{-1} are exactly the same as (1), (2) except that an interchange is made of x_1 and y_1, and of x_2 and y_2.

From T_2, we easily obtain, by Theorem 2, Section 10, further involutory transformations. Thus, denoting again by T_1 the transformation given in equations (1), (2) of Section 12, we know that each of the transformations $T_1^{-1}T_2T_1$ and $T_1T_2T_1^{-1}$ is involutory. These products may be determined from formulas (1) of Section 6, or by successive applications of the factor transformations. Following the latter method, we find that the product T_2T_1 is:

$$z_1 = \begin{pmatrix} 11 & 18 \\ 17 & 13 \end{pmatrix} x_1 + \begin{pmatrix} 10 & 2 \\ 10 & 6 \end{pmatrix} x_2 + \begin{pmatrix} 15 & 13 \\ 16 & 13 \end{pmatrix},$$

$$z_2 = \begin{pmatrix} 17 & 16 \\ 11 & 10 \end{pmatrix} x_1 + \begin{pmatrix} 21 & 8 \\ 10 & 3 \end{pmatrix} x_2 + \begin{pmatrix} 14 & 6 \\ 21 & 8 \end{pmatrix};$$

and that the (involutory) product $T_1^{-1}T_2T_1$ is:

$$(3)\qquad y_1 = \begin{pmatrix} 3 & 8 \\ 14 & 5 \end{pmatrix} x_1 + \begin{pmatrix} 24 & 4 \\ 12 & 2 \end{pmatrix} x_2 + \begin{pmatrix} 8 & 24 \\ 4 & 12 \end{pmatrix},$$

$$(4)\qquad y_2 = \begin{pmatrix} 6 & 8 \\ 12 & 14 \end{pmatrix} x_1 + \begin{pmatrix} 3 & 18 \\ 18 & 15 \end{pmatrix} x_2 + \begin{pmatrix} 6 & 14 \\ 0 & 24 \end{pmatrix}.$$

The cryptographic application of each of the two involutory transformations developed in this section is essentially the same as that of the non-involutory T_1 of the preceding section, and requires no separate discussion. The only difference—an important one, from the practical standpoint—is that the same transformation, with interchange of x_i and y_i, of course, is here employed for encipherment and decipherment.

14. *Example 3*

Let us determine an involutory transformation of type ${}_3T_2$. If we set:

$$\lambda_1 = \begin{pmatrix} 3 & 8 & 14 \\ 8 & 7 & 4 \\ 14 & 4 & 21 \end{pmatrix}, \quad \lambda_2 = \begin{pmatrix} 6 & 18 & 16 \\ 24 & 20 & 12 \\ 16 & 22 & 8 \end{pmatrix}, \quad \mu = \begin{pmatrix} 11 & 2 & 8 \\ 3 & 10 & 7 \\ 9 & 21 & 4 \end{pmatrix},$$

where

$$\sigma = \lambda_1^2 + \lambda_2^2 = \begin{pmatrix} 9 & 6 & 4 \\ 6 & 25 & 16 \\ 4 & 16 & 3 \end{pmatrix} + \begin{pmatrix} 22 & 14 & 24 \\ 10 & 4 & 18 \\ 24 & 20 & 12 \end{pmatrix} = \begin{pmatrix} 5 & 20 & 2 \\ 16 & 3 & 8 \\ 2 & 10 & 15 \end{pmatrix}$$

is regular, and μ is arbitrary, we find, by (9) of Section 5,

$$\sigma^{-1} = \frac{1}{21}\begin{pmatrix} 17 & 6 & 24 \\ 10 & 19 & 18 \\ 24 & 16 & 7 \end{pmatrix} = 5\begin{pmatrix} 17 & 6 & 24 \\ 10 & 19 & 18 \\ 24 & 16 & 7 \end{pmatrix} = \begin{pmatrix} 7 & 4 & 16 \\ 24 & 17 & 12 \\ 16 & 2 & 9 \end{pmatrix},$$

whence

$$\tau = 2\sigma^{-1} = \begin{pmatrix} 14 & 8 & 6 \\ 22 & 8 & 24 \\ 6 & 4 & 18 \end{pmatrix}, \quad \lambda_1\tau = \begin{pmatrix} 16 & 14 & 20 \\ 4 & 6 & 2 \\ 20 & 20 & 12 \end{pmatrix}, \quad \lambda_2\tau = \begin{pmatrix} 4 & 22 & 2 \\ 16 & 10 & 8 \\ 2 & 24 & 14 \end{pmatrix}.$$

By formula (2), Section 10, the transformation

$$y_1 = x_1 - \begin{pmatrix} 16 & 14 & 20 \\ 4 & 6 & 2 \\ 20 & 20 & 12 \end{pmatrix}(\lambda_1 x_1 + \lambda_2 x_2 + \mu),$$

$$y_2 = x_2 - \begin{pmatrix} 4 & 22 & 2 \\ 16 & 10 & 8 \\ 2 & 24 & 14 \end{pmatrix}(\lambda_1 x_1 + \lambda_2 x_2 + \mu)$$

is involutory. Its equations may be simplified to be

$$(1) \qquad y_1 = \begin{pmatrix} 3 & 6 & 2 \\ 16 & 23 & 8 \\ 2 & 16 & 13 \end{pmatrix} x_1 + \begin{pmatrix} 2 & 6 & 14 \\ 8 & 24 & 4 \\ 14 & 16 & 20 \end{pmatrix} x_2 + \begin{pmatrix} 18 & 6 & 6 \\ 24 & 20 & 22 \\ 2 & 2 & 16 \end{pmatrix}$$

$$(2) \qquad y_2 = \begin{pmatrix} 18 & 14 & 22 \\ 20 & 4 & 10 \\ 22 & 20 & 24 \end{pmatrix} x_1 + \begin{pmatrix} 15 & 16 & 20 \\ 4 & 13 & 2 \\ 20 & 8 & 11 \end{pmatrix} x_2 + \begin{pmatrix} 2 & 16 & 14 \\ 8 & 12 & 4 \\ 14 & 8 & 20 \end{pmatrix}.$$

Further involutory transformations of the type ${}_3T_2$ may, of course, be obtained from this by applying Theorem 2 of Section 10 and formulas (1) of Section 6; or by applying Theorem 2 of Section 10 and the procedure outlined at the close of Section 13.

In using the involutory transformation given by the equations (1) and (2) above, we first partition our message into subsequences of eighteen letters each, since $n^2 f = 18$. We fill out the last subsequence, if it is incomplete, with any prearranged letters.

Consider, for instance, the message: *HOLD OUT. SUPPORTING AIR SQUADRONS EN ROUTE.* It contains two full subsequences. Let us treat the first of these: *HOLDOUTSUPPORTINGA*. We suppose that the convention adopted in the cipher is to write:

$$x_1 = \begin{pmatrix} H & 0 & L \\ D & 0 & U \\ T & S & U \end{pmatrix} = \begin{pmatrix} 5 & 6 & 22 \\ 2 & 6 & 7 \\ 12 & 19 & 7 \end{pmatrix}$$

$$x_2 = \begin{pmatrix} P & P & 0 \\ R & T & I \\ N & G & A \end{pmatrix} = \begin{pmatrix} 21 & 21 & 6 \\ 23 & 12 & 17 \\ 24 & 16 & 4 \end{pmatrix}$$

by means of the correspondence specified in Section 11. Substituting these matrices for x_1 and x_2 in the equations (1), (2) of the present section, we obtain:

$$y_1 = \begin{pmatrix} 25 & 14 & 18 \\ 14 & 22 & 23 \\ 16 & 17 & 13 \end{pmatrix} + \begin{pmatrix} 22 & 0 & 14 \\ 10 & 0 & 4 \\ 24 & 0 & 20 \end{pmatrix} + \begin{pmatrix} 18 & 6 & 6 \\ 24 & 20 & 22 \\ 2 & 2 & 16 \end{pmatrix} = \begin{pmatrix} 13 & 20 & 12 \\ 22 & 16 & 23 \\ 16 & 19 & 23 \end{pmatrix},$$

$$y_2 = \begin{pmatrix} 18 & 12 & 24 \\ 20 & 22 & 18 \\ 22 & 6 & 12 \end{pmatrix} + \begin{pmatrix} 19 & 21 & 0 \\ 15 & 12 & 19 \\ 10 & 16 & 14 \end{pmatrix} + \begin{pmatrix} 2 & 16 & 14 \\ 8 & 12 & 4 \\ 14 & 8 & 20 \end{pmatrix} = \begin{pmatrix} 13 & 23 & 12 \\ 17 & 20 & 15 \\ 20 & 4 & 20 \end{pmatrix}.$$

Hence the enciphered form of the subsequence is

$$\begin{pmatrix} Y & K & T \\ L & G & R \\ G & S & R \end{pmatrix}, \begin{pmatrix} Y & R & T \\ I & K & W \\ K & A & K \end{pmatrix};$$

or, as it would be transmitted,[21] *Y K T L G R G S R Y R T I K W K A K.*

Substitution of the matrices y_1, y_2 in the same equations (1) and (2) above yields again the original matrices x_1, x_2, the equations having first been written, of course, with x_i and y_i interchanged ($i = 1, 2$).

Each message subsequence is enciphered and deciphered in the same manner.

15. *Concluding Notes*

All the transformations discussed in the foregoing pages are obviously applicable in any range $R\{n\}$ of any scale S, the special range $R\{1\}$ coinciding with S and yielding ordinary scalar transformations. Of interest in cryptography are not only the scales $S(n)$, and their various algebraic extensions, but also certain non-modular and infinite scales. In this connection, we note especially the scale S consisting of all positive and negative integers and zero in the field of rational numbers; any *regular* transformation in a range of this scale will have a frame matrix with determinant of value ±1.

Plans have been completed for a novel type of computing machine capable of effecting the simultaneous and speedy evaluation of any desired number of

[21] When the entire message has been enciphered, it will normally be transmitted in the conventional five-letter groups: *YKTLG RGSRY* · · · ·

linear functions of any assigned sequences of elements in any scale of type $S(n)$, the linear functions having any arbitrarily selected scheme of coefficients. The machine, although originally designed for other purposes, may be used to apply very rapidly, without calculations of any sort, all transformations proposed in this paper for which the underlying scale is an $S(n)$, and even products of such transformations with widely variable ciphers of different type. From the point of view of cryptography, this circumstance lends exceptional interest to the scales $S(n)$.

Formula (2), Section 10, demands a sequence $\lambda_1, \lambda_2, \cdots, \lambda_f$ of f square matrices such that $\lambda_1^2+\lambda_2^2+\cdots+\lambda_f^2$ is a *regular* matrix. A great variety of sequences with this property can be determined very quickly, in any range of any scale, and for any positive integer f, by means of an interesting formula which will be the subject of special discussion elsewhere.

In any scale S, it is easy to set up an algebra for ranges of matrices whose elements are in turn matrices, the elements of these latter being again matrices, etc. But no important cryptographic advantages seem to arise from these further complications.

TWO FUNCTIONAL EQUATIONS WITH INTEGRAL ARGUMENTS

By PHILIP FRANKLIN, Massachusetts Institute of Technology

Professor E. T. Bell has recently indicated[1] that the general solution of the functional equations

$$(1) \qquad f(x, n_1)f(x, n_2) = f(x, n_1 + n_2 + c),$$

$$(2) \qquad f(x, n_1)f(x, n_2) = f(x, cn_1n_2),$$

in which the argument n is an integer $\geqq 0$, and the constant c is an integer $\geqq 0$, while x is a parameter, had a connection with the question of possible types of arithmetic; and asked what were the general solutions of these equations. We here obtain these general solutions, showing that the solution of the first involves a single function of x, while that of the second involves an enumerable number of such functions.

Theorem 1. *The general solution of* (1) *is* $[F(x)]^{n+c}$. We prove this by noting that, in consequence of (1), we have:

$$(3) \quad f(x, n-1)f(x, n+1) = f(x, 2n+c) = [f(x, n)]^2 \qquad (n = 1, 2, \ldots).$$

This shows that if $f(x, 0)=0, f(x, n)=0$ for all n; and also that if $f(x,0)\neq 0$, no $f(x, n)$ can vanish. In this latter case, we may rewrite (3) in the form:

$$(4) \qquad \frac{f(x, n+1)}{f(x, n)} = \frac{f(x, n)}{f(x, n-1)} \cdots = \frac{f(x, 1)}{f(x, 0)} = F(x).$$

[1] This Monthly, vol. 37 (1930), p. 484.