INTRODUCTION TO ALGEBRAIC THEORIES

By

A. ADRIAN ALBERT

THE UNIVERSITY OF CHICAGO

THE UNIVERSITY OF CHICAGO PRESS
CHICAGO · ILLINOIS

THE UNIVERSITY OF CHICAGO PRESS, CHICAGO 37
Cambridge University Press, London, N.W.1, England
The University of Toronto Press, Toronto 5, Canada

Published January 1941. Sixth Impression 1958. Composed and printed by THE UNIVERSITY OF CHICAGO PRESS, *Chicago, Illinois, U.S.A.*

PREFACE

During recent years there has been an ever increasing interest in modern algebra not only of students in mathematics but also of those in physics, chemistry, psychology, economics, and statistics. My *Modern Higher Algebra* was intended, of course, to serve primarily the first of these groups, and its rather widespread use has assured me of the propriety of both its contents and its abstract mode of presentation. This assurance has been confirmed by its successful use as a text, the sole prerequisite being the subject matter of L. E. Dickson's *First Course in the Theory of Equations*. However, I am fully aware of the serious gap in mode of thought between the intuitive treatment of algebraic theory of the *First Course* and the rigorous abstract treatment of the *Modern Higher Algebra*, as well as the pedagogical difficulty which is a consequence.

The publication recently of more abstract presentations of the theory of equations gives evidence of attempts to diminish this gap. Another such attempt has resulted in a supposedly less abstract treatise on modern algebra which is about to appear as these pages are being written. However, I have the feeling that neither of these compromises is desirable and that it would be far better to make the transition from the intuitive to the abstract by the addition of a new course in algebra to the undergraduate curriculum in mathematics—a curriculum which contains at most two courses in algebra and these only partly algebraic in content.

This book is a text for such a course. In fact, its only prerequisite material is a knowledge of that part of the theory of equations given as a chapter of the ordinary text in college algebra as well as a reasonably complete knowledge of the theory of determinants. Thus, it would actually be possible for a student with adequate mathematical maturity, whose only training in algebra is a course in college algebra, to grasp the contents. I have used the text in manuscript form in a class composed of third- and fourth-year undergraduate and beginning graduate students, and they all seemed to find the material easy to understand. I trust that it will find such use elsewhere and that it will serve also to satisfy the great interest in the theory of matrices which has been shown me repeatedly by students of the social sciences.

I wish to express my deep appreciation of the fine critical assistance of Dr. Sam Perlis during the course of publication of this book.

A. A. Albert

University of Chicago
September 9, 1940

TABLE OF CONTENTS

CHAPTER I

POLYNOMIALS

1. Polynomials in x. There are certain simple algebraic concepts with which the reader is probably well acquainted but not perhaps in the terminology and form desirable for the study of algebraic theories. We shall thus begin our exposition with a discussion of these concepts.

We shall speak of the familiar operations of *addition*, *subtraction*, and *multiplication* as the *integral operations*. A positive integral power is then best regarded as the result of a finite repetition of the operation of multiplication.

A *polynomial* $f(x)$ in x is any expression obtained as the result of the application of a finite number of integral operations to x and constants. If $g(x)$ is a second such expression and it is possible to carry out the operations indicated in the given formal expressions for $f(x)$ and $g(x)$ so as to obtain two identical expressions, then we shall regard $f(x)$ and $g(x)$ as being the *same* polynomial. This concept is frequently indicated by saying that $f(x)$ and $g(x)$ are *identically equal* and by writing $f(x) \equiv g(x)$. However, we shall usually say merely that $f(x)$ and $g(x)$ are *equal* polynomials and write $f(x) = g(x)$. We shall designate by 0 the polynomial which is the constant zero and shall call this polynomial the *zero polynomial*. Thus, in a discussion of polynomials $f(x) = 0$ will mean that $f(x)$ is the zero polynomial. No confusion will arise from this usage for it will always be clear from the context that, in the consideration of a *conditional* equation $f(x) = 0$ where we seek a constant solution c such that $f(c) = 0$, the polynomial $f(x)$ is *not* the zero polynomial. We observe that the zero polynomial has the properties

$$0 \cdot g(x) = 0\,, \qquad 0 + g(x) = g(x)$$

for every polynomial $g(x)$.

Our definition of a polynomial includes the use of the familiar term *constant*. By this term we shall mean any complex number or function independent of x. Later on in our algebraic study we shall be much more explicit about the meaning of this term. For the present, however, we shall merely make the unprecise assumption that our constants have the usual properties postulated in elementary algebra. In particular, we shall assume the properties that if a and b are constants such that $ab = 0$ then either

a or b is zero; and if a is a nonzero constant then a has a constant inverse a^{-1} such that $aa^{-1} = 1$.

If $f(x)$ is the label we assign to a particular formal expression of a polynomial and we replace x wherever it occurs in $f(x)$ by a constant c, we obtain a corresponding expression in c which is the constant we designate by $f(c)$. Suppose now that $g(x)$ is any different formal expression of a polynomial in x and that $f(x) = g(x)$ in the sense defined above. Then it is evident that $f(c) = g(c)$. Thus, in particular, if $h(x)$, $q(x)$, $r(x)$ are polynomials in x such that $f(x) = h(x)q(x) + r(x)$ then $f(c) = h(c)q(c) + r(c)$ for any c. For example, we have $f(x) = x^3 - 2x^2 + 3x$, $h(x) = x - 1$, $q(x) = x^2 - x$, $r(x) = 2x$, and are stating that for any c we have $c^3 - 2c^2 + 3c = (c - 1)(c^2 - c) + 2c$.

If the indicated integral operations in any given expression of a polynomial $f(x)$ be carried out, we may express $f(x)$ as a sum of a finite number of terms of the form ax^k. Here k is a non-negative integer and a is a constant called the *coefficient* of x^k. The terms with the same exponent k may be combined into a single term whose coefficient is the sum of all their coefficients, and we may then write

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n . \tag{1}$$

The constants a_i are called the coefficients of $f(x)$ and may be zero, but unless $f(x)$ is the zero polynomial, we may always take $a_0 \neq 0$. The expression (1) of $f(x)$ with $a_0 \neq 0$ is most important since, if $g(x)$ is a second polynomial and we write $g(x)$ in the corresponding form

$$g(x) = b_0x^m + b_1x^{m-1} + \ldots + b_m \tag{2}$$

with $b_0 \neq 0$, then $f(x)$ and $g(x)$ are equal if and only if $m = n$, $a_i = b_i$ for $i = 0, \ldots, n$. In other words, we may say that the expression (1) of a polynomial is unique, that is, two polynomials are equal if and only if their expressions (1) are identical.

The integer n of any expression (1) of $f(x)$ is called the *virtual degree* of the expression (1). If $a_0 \neq 0$ we call n the *degree** of $f(x)$. Thus, either any $f(x)$ has a positive integral degree, or $f(x) = a_n$ is a constant and will be called a constant polynomial in x. If, then, $a_n \neq 0$ we say that the constant polynomial $f(x)$ has degree zero. But if $a_n = 0$, so that $f(x)$ is the zero polynomial, we shall assign to it the degree *minus infinity*. This will

* Clearly any polynomial of degree n_0 may be written as an expression of the form (1) of virtual degree any integer $n \geq n_0$. We may thus speak of any such n as a virtual degree of $f(x)$.

be done so as to imply that certain simple theorems on polynomials shall hold without exception.

The coefficient a_0 in (1) will be called the *virtual leading coefficient* of this expression of $f(x)$ and will be called the *leading coefficient* of $f(x)$ if and only if it is not zero. We shall call $f(x)$ a *monic polynomial* if $a_0 = 1$. We then have the elementary results referred to above, whose almost trivial verification we leave to the reader.

LEMMA 1. *The degree of a product of two polynomials* $\mathrm{f(x)}$ *and* $\mathrm{g(x)}$ *is the sum of the degrees of* $\mathrm{f(x)}$ *and* $\mathrm{g(x)}$. *The leading coefficient of* $\mathrm{f(x) \cdot g(x)}$ *is the product of the leading coefficients of* $\mathrm{f(x)}$ *and* $\mathrm{g(x)}$, *and thus, if* $\mathrm{f(x)}$ *and* $\mathrm{g(x)}$ *are monic, so is* $\mathrm{f(x) \cdot g(x)}$.

LEMMA 2. *A product of two nonzero polynomials is nonzero and is a constant if and only if both factors are constants.*

LEMMA 3. *Let* $\mathrm{f(x)}$ *be nonzero and such that* $\mathrm{f(x)g(x) = f(x)h(x)}$. *Then* $\mathrm{g(x) = h(x)}$.

LEMMA 4. *The degree of* $\mathrm{f(x) + g(x)}$ *is at most the larger of the two degrees of* $\mathrm{f(x)}$ *and* $\mathrm{g(x)}$.

EXERCISES*

1. State the condition that the degree of $f(x) + g(x)$ be less than the degree of either $f(x)$ or $g(x)$.

2. What can one say about the degree of $f(x) + g(x)$ if $f(x)$ and $g(x)$ have positive leading coefficients?

3. What can one say about the degree of f^2, of f^3, of f^k for $f = f(x)$ a polynomial, k a positive integer?

4. State a result about the degree and leading coefficient of any polynomial $s(x) = f_1^2 + \ldots + f_t^2$ for $t \geq 1$, $f_i = f_i(x)$ a polynomial in x with *real* coefficients.

5. Make a corresponding statement about $g(x)s(x)$ where $g(x)$ has odd degree and real coefficients, $s(x)$ as in Ex. 4.

6. State the relation between the term of least degree in $f(x)g(x)$ and those of least degree in $f(x)$ and $g(x)$.

7. State why it is true that if x is not a factor of $f(x)$ or $g(x)$ then x is not a factor of $f(x)g(x)$.

8. Use Ex. 7 to prove that if k is a positive integer then x is a factor of $[f(x)]^k$ if and only if x is a factor of $f(x)$.

9. Let f and g be polynomials in x such that the following equations are satisfied (identically). Show, then, that both f and g are zero. Hint: Verify first that other-

* The early exercises in our sets should normally be taken up orally. The author's choice of oral exercises will be indicated by the language employed.

wise *both* f and g are not zero. Express each equation in the form $a(x) = b(x)$ and apply Ex. 3. In parts (*c*) and (*d*) complete the squares.

a) $f^2 + xg^2 = 0$ *c*) $f^4 + 2xf^2g^2 + (x^2 - x)g^4 = 0$
b) $f^3 - x^2g^3 = 0$ *d*) $f^2 + 2xfg - xg^2 = 0$

10. Use Ex. 8 to give another proof of (*a*), (*b*), and (*d*) of Ex. 9. Hint: Show that if f and g are nonzero polynomial solutions of these equations of least possible degrees, then x divides $f = xf_1$ as well as $g = xg_1$. But then f_1 and g_1 are also solutions —a contradiction.

11. Use Ex. 4 to show that if f, g, and h are polynomials in x with real coefficients satisfying the following equations (identically), then they are all zero:

a) $f^2 - xg^2 = xh^2$
b) $f^2 - xg^2 + h^2 = 0$
c) $f^2 + g^2 + (x + 2)h^2 = 0$

12. Find solutions of the equations of Ex. 11 for polynomials f, g, h with complex coefficients and not all zero.

2. The division algorithm. The result of the application of the process ordinarily called long division to polynomials is a theorem which we shall call the *Division Algorithm* for polynomials and shall state as

Theorem 1. *Let* f(x) *and* g(x) *be polynomials of respective degrees* n *and* m, g(x) $\neq 0$. *Then there exist unique polynomials* q(x) *and* r(x) *such that* r(x) *has virtual degree* m $-$ 1, q(x) *is either zero or has degree* n $-$ m, *and*

$$f(x) = q(x)g(x) + r(x) . \tag{3}$$

For let $f(x)$ and $g(x)$ be defined respectively by (1) and (2) with $b_0 \neq 0$. Then, either $n < m$ and we have (3) with $q(x) = 0$, $r(x) = f(x)$, or $a_0 \neq 0$, $n \geq m$. If c_k is the virtual leading coefficient of a polynomial $h(x)$ of virtual degree $m + k \geq m$, a virtual degree of $h(x) - b_0^{-1}c_kx^kg(x)$ is $m + k - 1$. Thus a virtual degree of $f(x) - b_0^{-1}a_0x^{n-m}g(x)$ is $n - 1$, and a finite repetition of this process yields a polynomial $r(x) = f(x) - b_0^{-1}(a_0x^{n-m} + \ldots)g(x)$ of virtual degree $m - 1$, and hence (3) for $q(x)$ of degree $n - m$ and leading coefficient $a_0b_0^{-1} \neq 0$. If also $f(x) = q_0(x)g(x) + r_0(x)$ for $r_0(x)$ of virtual degree $m - 1$, then a virtual degree of $s(x) = r_0(x) - r(x)$ is $m - 1$. But Lemma 1 states that if $t(x) = q(x) - q_0(x) \neq 0$ the degree of $s(x) = t(x)g(x)$ is the sum of m and the degree of $t(x)$. This is impossible; and $t(x) = 0$, $q(x) = q_0(x)$, $r(x) = r_0(x)$.

The *Remainder Theorem of Algebra* states that if we use the *Division Algorithm* to write

$$f(x) = q(x)(x - c) + r(x) ,$$

so that $g(x) = x - c$ has degree one and $r = r(x)$ is necessarily a constant, then $r = f(c)$. The obvious proof of this result is the use of the remark in the fifth paragraph of Section 1 to obtain $f(c) = q(c)(c - c) + r$, $f(c) = r$ as desired. It is for this application that we made the remark.

The *Division Algorithm* and *Remainder Theorem* imply the *Factor Theorem* —a result obtained and used frequently in the study of polynomial equations. We shall leave the statements of that theorem, and the subsequent definitions and theorems on the roots and corresponding factorizations of polynomials* with real or complex coefficients, to the reader.

* If $f(x)$ is a polynomial in x and c is a constant such that $f(c) = 0$ then we shall call c a root not only of the equation $f(x) = 0$ but also of the polynomial $f(x)$.

EXERCISES

1. Show by formal differentiation that if c is a root of multiplicity m of $f(x) = (x - c)^m q(x)$ then c is a root of multiplicity $m - 1$ of the derivative $f'(x)$ of $f(x)$. What then is a necessary and sufficient condition that $f(x)$ have multiple roots?

2. Let c be a root of a polynomial $f(x)$ of degree n and ordinary integral coefficients. Use the *Division Algorithm* to show that any polynomial $h(c)$ with rational coefficients may be expressed in the form $b_0 + b_1 c + \ldots + b_{n-1}c^{n-1}$ for rational numbers $b_0, \ldots, b_{n-1}$. Hint: Write $h(x) = q(x)f(x) + r(x)$ and replace x by c.

3. Let $f(x) = x^3 + 3x^2 + 4$ in Ex. 2. Compute the corresponding b_i for each of the polynomials

a) $c^6 + 10c^4 + 25c^2$ *c)* $c^6 - 2c^4 + c^2$
b) $c^4 + 4c^3 + 6c^2 + 4c + 1$ *d)* $(2c^2 + 3)(c^3 + 3c)$

3. Polynomial divisibility. Let $f(x)$ and $g(x) \neq 0$ be polynomials. Then by the statement that g(x) *divides* f(x) we mean that there exists a polynomial $q(x)$ such that $f(x) = q(x)g(x)$. Thus, $g(x) \neq 0$ divides $f(x)$ if and only if the polynomial $r(x)$ of (3) is the zero polynomial, and we shall say in this case that f(x) *has* g(x) *as a factor*, g(x) *is a factor of* f(x).

We shall call two nonzero polynomials $f(x)$ and $g(x)$ *associated polynomials* if $f(x)$ divides $g(x)$ and $g(x)$ divides $f(x)$. Then $f(x) = q(x)g(x)$, $g(x) = h(x)f(x)$, so that $f(x) = q(x)h(x)f(x)$. Applying Lemmas 3 and 2, we have $q(x)h(x) = 1$, $q(x)$ and $h(x)$ are nonzero constants. Thus f(x) *and* g(x) *are associated if and only if each is a nonzero constant multiple of the other.*

It is clear that every nonzero polynomial is associated with a monic polynomial. Observe thus that the familiar process of dividing out the leading coefficient in a conditional equation $f(x) = 0$ is that used to replace this equation by the equation $g(x) = 0$ where $g(x)$ is the monic polynomial associated with $f(x)$.

Two associated monic polynomials are equal. We see from this that if $g(x)$ divides $f(x)$ every polynomial associated with $g(x)$ divides $f(x)$ and that one possible way to distinguish a member of the set of all associates of $g(x)$ is to assume the associate to be monic. We shall use this property ater when we discuss the existence of a *unique* greatest common divisor (abbreviated, g.c.d.) of polynomials in x.

In our discussion of the g.c.d. of polynomials we shall obtain a property which may best be described in terms of the concept of rational function. It will thus be desirable to arrange our exposition so as to precede the study of greatest common divisors by a discussion of the elements of the theory of polynomials and rational functions of several variables, and we shall do so.

EXERCISES

1. Let $f = f(x)$ be a polynomial in x and define $m(f) = x^m f(1/x)$ for every positive integer m. Show that $m(f)$ is a polynomial in x of virtual degree m if and only if m is a virtual degree of $f(x)$.

2. Show that $m(0) = 0$, $m[m(f)] = f$.

3. Define $\bar{f} = 0$ if $f = 0$, and $\bar{f} = n(f)$ if f is any nonzero polynomial of degree n. Show that $m(f) = x^{m-n}\bar{f}$ for every $m \geq n$ and that, if $f \neq 0$, x is not a factor of $\bar{f}$.

4. Let g be a factor of f. Prove that $\bar{g}$ is a factor of $m(f)$ for every m which is at least the degree of f.

4. Polynomials in several variables. Some of our results on polynomials in x may be extended easily to polynomials in several variables. We define a polynomial $f = f(x_1, \ldots, x_q)$ in $x_1, \ldots, x_q$ to be any expression obtained as the result of a finite number of integral operations on $x_1, \ldots, x_q$ and constants. As in Section 1 we may express $f(x_1, \ldots, x_q)$ as the sum of a finite number of terms of the form

$$ax_1^{k_1} x_2^{k_2} \ldots x_q^{k_q}. \tag{4}$$

We call a the *coefficient* of the term (4) and define the *virtual degree* in $x_1, \ldots, x_q$ of such a term to be $k_1 + \ldots + k_q$, the virtual degree of a particular expression of f as a sum of terms of the form (4) to be the largest of the virtual degrees of its terms (4). If two terms of f have the same set of exponents $k_1, \ldots, k_q$, we may combine them by adding their coefficients and thus write f as the unique sum, that is, the sum with unique coefficients,

$$f = f(x_1, \ldots, x_q) = \sum_{k_j = 0, 1, \ldots, n_j} a_{k_1 \ldots k_q} x_1^{k_1} \ldots x_q^{k_q}. \tag{5}$$

Here the coefficients $a_{k_1} \ldots {}_{k_q}$ are constants and n_j is the degree of $f(x_1, \ldots, x_q)$ considered as a polynomial in x_j alone. Also f is the zero polynomial if and only if all its coefficients are zero. If f is a nonzero polynomial, then some $a_{k_1} \ldots {}_{k_q} \neq 0$, and the *degree* of f is defined to be the maximum sum $k_1 + \ldots + k_q$ for $a_{k_1} \ldots {}_{k_q} \neq 0$. As before we assign the degree *minus infinity* to the zero polynomial and have the property that nonzero constant polynomials have degree zero. Note now that a polynomial may have several different terms of the same degree and that consequently the usual definition of leading term and coefficient do not apply. However, some of the most important simple properties of polynomials in x hold also for polynomials in several x_i, and we shall proceed to their derivation.

We observe that a polynomial f in $x_1, \ldots, x_q$ may be regarded as a polynomial (1) of degree $n = n_q$ in $x = x_q$ with its coefficients $a_0, \ldots, a_n$ all polynomials in $x_1, \ldots, x_{q-1}$ and a_0 not zero. If, similarly, g be given by (2) with b_0 not zero, then a virtual degree in x_q of fg is $m + n$, and a virtual leading coefficient of fg is $a_0 b_0$. If $q = 2$, then a_0 and b_0 are nonzero polynomials in x_1 and $a_0 b_0 \neq 0$ by Lemma 2. Then we have proved that the product fg of two nonzero polynomials f and g in x_1, x_2 is not zero. If we prove similarly that the product of two nonzero polynomials in $x_1, \ldots, x_{q-1}$ is not zero, we apply the proof above to obtain $a_0 b_0 \neq 0$ and hence have proved that the product fg of two nonzero polynomials in $x_1, \ldots, x_q$ is not zero. We have thus completed the proof of

Theorem 2. *The product of any two nonzero polynomials in* $x_1, \ldots, x_q$ *is not zero.*

We have the immediate consequence

Theorem 3. *Let* f, g, h *be polynomials in* $x_1, \ldots, x_q$ *and* f *be nonzero,* fg = fh. *Then* g = h.

To continue our discussion we shall need to consider an important special type of polynomial. Thus we shall call $f(x_1, \ldots, x_q)$ a *homogeneous polynomial* or a *form* in $x_1, \ldots, x_q$ if all terms of (5) have the same degree $k = k_1 + \ldots + k_q$. Then, if f is given by (5) and we replace x_i in (5) by yx_i, we see that each power product $x_1^{k_1} \ldots x_q^{k_q}$ is replaced by $y^{k_1 + \cdots + k_q} x_1^{k_1} \ldots x_q^{k_q}$ and thus that the polynomial $f(yx_1, \ldots, yx_q) = y^k f(x_1, \ldots, x_q)$ identically in $y, x_1, \ldots, x_q$ if and only if $f(x_1, \ldots, x_q)$ is a form of degree k in $x_1, \ldots, x_q$.

The product of two forms f and g of respective degrees n and m in the same $x_1, \ldots, x_q$ is clearly a form of degree $m + n$ and, by Theorem 2, is nonzero if and only if f and g are nonzero. We now use this result to obtain the second of the properties we desire. It is a generalization of Lemma 1.

Observe first that all the terms of the same degree in a nonzero polynomial (5) may be grouped together into a form of this degree and then we may express (5) uniquely as the sum

$$f = f(x_1, \ldots, x_q) = f_0 + \ldots + f_n , \tag{6}$$

where f_0 is a nonzero form of the same degree n as the polynomial f and f_i is a form of degree $n - i$. If also

$$g = g(x_1, \ldots, x_q) = g_0 + \ldots + g_m , \tag{7}$$

for forms g_i of degree $m - i$ and such that $g_0 \neq 0$, then clearly

$$fg = h_0 + \ldots + h_{m+n} , \tag{8}$$

where the h_i are forms of degree $m + n - i$ and $h_0 = f_0 g_0$. By Theorem 2 $h_0 \neq 0$. Thus if we call f_0 the leading form of f, we clearly have

Theorem 4. *Let* f *and* g *be polynomials in* $x_1, \ldots, x_q$. *Then the degree of* fg *is the sum of the degrees of* f *and* g *and the leading form of* fg *is the product of the leading forms of* f *and* g.

The result above is evidently fundamental for the study of polynomials in several variables—a study which we shall discuss only briefly in these pages.

5. Rational functions. The integral operations together with the operation of division by a nonzero quantity form a set of what are called the *rational operations*. A *rational function* of $x_1, \ldots, x_q$ is now defined to be any function obtained as the result of a finite number of rational operations on $x_1, \ldots, x_q$ and constants. The postulates of elementary algebra were seen by the reader in his earliest algebraic study to imply that every rational function of $x_1, \ldots, x_q$ may be expressed as a quotient

$$f = \frac{a(x_1, \ldots, x_q)}{b(x_1, \ldots, x_q)} , \tag{9}$$

for polynomials $a(x_1, \ldots, x_q)$ and $b(x_1, \ldots, x_q) \neq 0$. The coefficients of $a(x_1, \ldots, x_q)$ and $b(x_1, \ldots, x_q)$ are then called *coefficients* of f. Let us observe then that the set of all rational functions in $x_1, \ldots, x_q$ with complex coefficients has a property which we describe by saying that the set is *closed with respect to rational operations*. By this we mean that every rational function of the elements in this set is in the set. This may be seen to be due to the definitions $a/b + c/d = (ad + bc)/bd$, $(a/b) \cdot (c/d) = (ac)/(bd)$. Here b and d are necessarily not zero, and we may use Theorem 2 to obtain

$bd \neq 0$. Observe, then, that the set of rational functions satisfies the properties we assumed in Section 1 for our constants, that is, $fg = 0$ if and only if $f = 0$ or $g = 0$, while if $f \neq 0$ then f^{-1} exists such that $f \cdot f^{-1} = 1$.

6. A greatest common divisor process. The existence of a g.c.d. of two polynomials and the method of its computation are essential in the study of what are called *Sturm's functions* and so are well known to the reader who has studied the *Theory of Equations*. We shall repeat this material here because of its importance for algebraic theories.

We define the *g.c.d.* of polynomials $f_1(x), \ldots, f_t(x)$ not all zero *to be any monic polynomial* $\mathrm{d(x)}$ *which divides all the* $\mathrm{f_i(x)}$, *and is such that if* $\mathrm{g(x)}$ *divides every* $\mathrm{f_i(x)}$ *then* $\mathrm{g(x)}$ *divides* $\mathrm{d(x)}$. If $d_0(x)$ is a second such polynomial, then $d(x)$ and $d_0(x)$ divide each other, $d(x)$ and $d_0(x)$ are associated monic polynomials and are equal. Hence, according to our definition, the g.c.d. of $f_1(x), \ldots, f_t(x)$ is a unique polynomial.

If $g(x)$ divides all the $f_i(x)$, then $g(x)$ divides $d(x)$, and hence the degree of $d(x)$ is at least that of $g(x)$. Thus the g.c.d. $d(x)$ is a common divisor of the $f_i(x)$ of largest possible degree and is clearly the unique monic common divisor of this degree.

If $d_j(x)$ is the g.c.d. of $f_1(x), \ldots, f_j(x)$ and $d_0(x)$ is the g.c.d. of $d_j(x)$ and $f_{j+1}(x)$, then $d_0(x)$ is the g.c.d. of $f_1(x), \ldots, f_{j+1}(x)$. For every common divisor $h(x)$ of $f_1(x), \ldots, f_{j+1}(x)$ divides $f_1(x), \ldots, f_j(x)$, and hence both $d_j(x)$ and $f_{j+1}(x)$, $h(x)$ divides $d_0(x)$. Moreover, $d_0(x)$ divides $f_{j+1}(x)$ and the divisor $d_j(x)$ of $f_1(x), \ldots, f_j(x)$, $d_0(x)$ divides $f_1(x), \ldots, f_{j+1}(x)$.

The result above evidently reduces the problems of the existence and construction of a g.c.d. of any number of polynomials in x not all zero to the case of two nonzero polynomials. We shall now study this latter problem and state the result we shall prove as

Theorem 5. *Let* $\mathrm{f(x)}$ *and* $\mathrm{g(x)}$ *be polynomials not both zero. Then there exist polynomials* $\mathrm{a(x)}$ *and* $\mathrm{b(x)}$ *such that*

$$\mathrm{d(x) = a(x)f(x) + b(x)g(x)} \tag{10}$$

is a monic common divisor of $\mathrm{f(x)}$ *and* $\mathrm{g(x)}$. *Moreover,* $\mathrm{d(x)}$ *is then the unique g.c.d. of* $\mathrm{f(x)}$ *and* $\mathrm{g(x)}$.

For if $f(x) = 0$, then $d(x)$ is associated with $g(x)$, $a(x) = 1$ and $b(x) = b_0^{-1}$ is a solution of (10) if $g(x)$ is given by (2). Hence, there is no loss of generality if we assume that both $f(x)$ and $g(x)$ are nonzero and that the degree of $g(x)$ is not greater than the degree of $f(x)$. For consistency of notation we put

$$h_0(x) = f(x), \qquad h_1(x) = g(x). \tag{11}$$

By Theorem 1

$$h_0(x) = q_1(x)h_1(x) + h_2(x)\,, \tag{12}$$

where the degree of $h_2(x)$ is less than the degree of $h_1(x)$. If $h_2(x) \neq 0$, we may apply Theorem 1 to obtain

$$h_1(x) = q_2(x)h_2(x) + h_3(x)\,, \tag{13}$$

where the degree of $h_3(x)$ is less than that of $h_2(x)$. Thus our division process yields a sequence of equations of the form

$$h_{i-2}(x) = q_{i-1}(x)h_{i-1}(x) + h_i(x)\,, \tag{14}$$

where if n_i is the degree of $h_i(x)$ then $n_1 > n_2 > \ldots$, while $n_i \geq 0$ unless $h_i(x) = 0$. We conclude that our sequence must terminate with

$$h_{r-2}(x) = q_{r-1}(x)h_{r-1}(x) + h_r(x) \tag{15}$$

and

$$h_r(x) \neq 0\,, \qquad h_{r-1}(x) = q_r(x)h_r(x) \tag{16}$$

for $r \geq 1$.

Equation (16) implies that (15) may be replaced by $h_{r-2}(x) = [q_{r-1}(x)q_r(x) + 1]h_r(x)$. Thus $h_r(x)$ divides both $h_{r-2}(x)$ and $h_{r-1}(x)$. If we assume that $h_r(x)$ divides $h_i(x)$ and $h_{i-1}(x)$, then (14) implies that $h_r(x)$ divides $h_{i-2}(x)$. An evident proof by induction shows that $h_r(x)$ divides both $h_0(x) = f(x)$ and $h_1(x) = g(x)$.

Equation (12) implies that $h_2(x) = a_2(x)f(x) + b_2(x)g(x)$ with $a_2(x) = 1$, $b_2(x) = -q_1(x)$. Clearly also $h_1(x) = a_1(x)f(x) + b_1(x)g(x)$ with $a_1(x) = 0$, $b_1(x) = 1$. If, now, $h_{i-2}(x) = a_{i-2}(x)f(x) + b_{i-2}(x)g(x)$ and $h_{i-1}(x) = a_{i-1}(x)f(x) + b_{i-1}(x)g(x)$ then (14) implies that $h_i(x) = [a_{i-2}(x) - q_{i-1}(x)a_{i-1}(x)]f(x) + [b_{i-2}(x) - q_{i-1}(x)b_{i-1}(x)]g(x) = a_i(x)f(x) + b_i(x)g(x)$. Thus we obtain $h_r(x) = a_r(x)f(x) + b_r(x)g(x)$. The polynomial $h_r(x)$ is a common divisor of $f(x)$ and $g(x)$ and is associated with a monic common divisor $d(x) = ch_r(x)$. Then $d(x)$ has the form (10) for $a(x) = ca_r(x)$, $b(x) = cb_r(x)$. We have already shown that $d(x)$ is unique.

The process used above was first discovered by Euclid, who utilized it in his geometric formulation of the analogous result on the g.c.d. of integers. It is therefore usually called *Euclid's process*. We observe that it not only enables us to prove the existence of $d(x)$ but gives us a finite process by

means of which $d(x)$ may be computed. Notice finally that $d(x)$ is computed by a repetition of the *Division Algorithm* on $f(x)$, $g(x)$ and polynomials secured from $f(x)$ and $g(x)$ as remainders in the application of the *Division Algorithm*. But this implies the result we state as

Theorem 6. *The polynomials* a(x), b(x), *and hence the greatest common divisor* d(x) *of Theorem 5 all have coefficients which are rational functions with rational number coefficients of the coefficients of* f(x) *and* g(x).

We thus have the

COROLLARY. *Let the coefficients of* f(x) *and* g(x) *be rational numbers. Then the coefficients of their g.c.d. are rational numbers.*

If the only common divisors of $f(x)$ and $g(x)$ are constants, then $d(x) = 1$ and we shall call $f(x)$ and $g(x)$ *relatively prime polynomials*. We shall also indicate this at times by saying that $f(x)$ is prime to $g(x)$ and hence also that $g(x)$ is prime to $f(x)$. When $f(x)$ and $g(x)$ are relatively prime, we use (10) to obtain polynomials $a(x)$ and $b(x)$ such that

$$a(x)f(x) + g(x)b(x) = 1 . \tag{17}$$

It is interesting to observe that the polynomials $a(x)$ and $b(x)$ in (17) are not unique and that it is possible to define a certain unique pair and then determine all others in terms of this pair. To do this we first prove the

LEMMA 5. *Let* f(x), g(x), *and* h(x) *be nonzero polynomials such that* f(x) *is prime to* g(x) *and divides* g(x)h(x). *Then* f(x) *divides* h(x).

For we may write $g(x)h(x) = f(x)q(x)$ and use (17) to obtain $[a(x)f(x) + b(x)g(x)]h(x) = [a(x)h(x) + b(x)q(x)]f(x) = h(x)$ as desired.

We now obtain

Theorem 7. *Let* f(x) *of degree* n *and* g(x) *of degree* m *be relatively prime. Then there exist unique polynomials* a_0(x) *of degree at most* m − 1 *and* b_0(x) *of degree at most* n − 1 *such that* a_0(x)f(x) + b_0(x)g(x) = 1. *Every pair of polynomials* a(x) *and* b(x) *satisfying* (17) *has the form*

$$a(x) = a_0(x) + c(x)g(x) , \qquad b(x) = b_0(x) - c(x)f(x) \tag{18}$$

for a polynomial c(x).

For, if $a(x)$ is any solution of (17), we apply Theorem 1 to obtain the first equation of (18) with $a_0(x)$ the remainder on division of $a(x)$ by $g(x)$. Then $a_0(x)$ has degree at most $m - 1$, $a(x)f(x) + b(x)g(x) = a_0(x)f(x) + [b(x) + c(x)f(x)]g(x) = 1$. We define $b_0(x) = b(x) + c(x)f(x)$ and see that $b_0(x)g(x) = -a_0(x)f(x) + 1$ has degree at most $m + n - 1$. By Lemma 1 the degree of $b_0(x)$ is at most $n - 1$, $a_0(x)f(x) + b_0(x)g(x) = 1$ as desired. If now $a_1(x)$ has virtual degree $m - 1$, $b_1(x)$ virtual degree $n - 1$ and

$a_1(x)f(x) + b_1(x)g(x) = a_0(x)f(x) + b_0(x)g(x)$, then $f(x)$ clearly divides $[b_0(x) - b_1(x)]g(x)$. By Lemma 5 the polynomial $b_0(x) - b_1(x)$ of virtual degree $n - 1$ is divisible by $f(x)$ of degree n and must be zero. Hence, $b_0(x) = b_1(x)$, so that $a_1(x)f(x) = a_0(x)f(x)$, $a_1(x) = a_0(x)$. This proves $a_0(x)$ and $b_0(x)$ unique. But the definition above of $a_0(x)$ as the remainder on division of $a(x)$ by $g(x)$ shows that then (18) holds.

There is also a result which is somewhat analogous to Theorem 7 for the case where $f(x)$ and $g(x)$ are not relatively prime. We state it as

Theorem 8. *Let* $\mathrm{f(x)} \neq 0$ *and* $\mathbf{g(x)} \neq 0$ *have respective degrees* n *and* m. *Then polynomials* $\mathrm{a(x)} \neq 0$ *of degree at most* $\mathrm{m} - 1$ *and* $\mathrm{b(x)} \neq 0$ *of degree at most* $\mathrm{n} - 1$ *such that*

$$\mathrm{a(x)f(x) + b(x)g(x) = 0} \tag{19}$$

exist if and only if f(x) *and* g(x) *are not relatively prime.*

For if the g.c.d. of $f(x)$ and $g(x)$ is a nonconstant polynomial $d(x)$, we have $f(x) = f_1(x)d(x)$, $g(x) = g_1(x)d(x)$, $g_1(x)f(x) + [-f_1(x)g(x)] = 0$ where $g_1(x)$ has degree less than m and $f_1(x)$ has degree less than n. Conversely, let (19) hold. If $f(x)$ and $g(x)$ are relatively prime, we have $a_0(x)f(x) + b_0(x)g(x) = 1$, $a(x) = a_0(x)a(x)f(x) + a(x)b_0(x)g(x) = g(x)[a(x)b_0(x) - a_0(x)b(x)]$. But then $g(x)$ of degree m divides $a(x) \neq 0$ of degree at most $m - 1$ which is impossible.

EXERCISES

1. Extend Theorems 5, 6, and the corollary to a set of polynomials $f_1(x), \ldots, f_t(x)$.

2. Let $f_1(x), \ldots, f_t(x)$ be all polynomials of the first degree. State their possible g.c.d.'s and the conditions on the $f_i(x)$ for each such possible g.c.d.

3. State the results corresponding to those *above* for polynomials of virtual degree two.

4. Prove that the g.c.d. of $f(x)$ and $g(x)$ is the monic polynomial of least possible degree of the form (10). Hint: Show that if $d(x)$ is this polynomial then $f(x) = q(x)d(x) + r(x)$, $r(x)$ has the form (10) as well as degree less than that of $d(x)$ and so must be zero.

5. A polynomial $f(x)$ is called *rationally irreducible* if $f(x)$ has rational coefficients and is not the product of two nonconstant polynomials with rational coefficients. What are the possible g.c.d.'s of a set of rationally irreducible $f_i(x)$ of Ex. 1?

6. Let $f(x) = 0$ be rationally irreducible, $g(x)$ have rational coefficients. Show that $f(x)$ either divides $g(x)$ or is prime to $g(x)$. Thus, $f(x)$ is prime to $g(x)$ if the degree of $g(x)$ is less than that of $f(x)$.

7. Use Ex. 1 of Section 2 together with the results above to show that a rationally irreducible polynomial has no multiple roots.

8. Find the g.c.d. of each of the following sets of polynomials as well as of all possible pairs of polynomials in each case:

a) $f_1 = 2x^5 - x^3 - 2x^2 - 6x + 4$
$f_2 = x^4 + x^3 - x^2 - 2x - 2$

b) $f_1 = 3x^4 + 8x^2 - 3$
$f_2 = x^3 + 2x^2 + 3x + 6$

c) $f_1 = x^4 - 2x^3 - 2x^2 - 2x - 3$
$f_2 = x^3 + 6x^2 + 11x + 6$
$f_3 = x^4 - 8x^2 - 5x + 6$

d) $f_1 = x^3 + 4x^2 + x - 6$
$f_2 = x^2 - 3x + 2$
$f_3 = x^5 - 3x^3 + x^2 - 4x - 4$

e) $f_1 = x^5 + 2x^4 - x^3 - 5x^2 - 6x - 3$
$f_2 = x^3 + x^2 + 3x + 3$
$f_3 = x^4 + x^3 - x - 1$

f) $f_1 = x^3 + 2x^2 - 3x - 6$
$f_2 = x^2 + x - 2$
$f_3 = x^4 + 2x^3 + x + 2$

9. Let $f(x)$ be a rationally irreducible polynomial and c be a complex root of $f(x) = 0$. Show that, if $g(x)$ is a polynomial in x with rational coefficients and $g(c) \neq 0$, there then exists a polynomial $h(x)$ of degree less than that of $f(x)$ and with rational coefficients such that $g(c)h(c) = 1$.

10. Let $f(x)$ be a rationally irreducible quadratic polynomial and c be a complex root of $f(x) = 0$. Show that every rational function of c with rational coefficients is uniquely expressible in the form $a + bc$ with a and b rational numbers.

11. Let $f_1, \ldots, f_t$ be polynomials in x of virtual degree n and $f_1 \neq 0$. Use Ex. 4 of Section 3 to show that if $d(x)$ is the g.c.d. of $f_1, \ldots, f_t$ then the g.c.d. of $\bar{f}_1, \ldots, \bar{f}_t$ is $\bar{d}$. Thus, show that the g.c.d. of $n(f_1), \ldots, n(f_t)$ has the form $x^k\bar{d}$ for an integer $k \geq 0$.

7. Forms. A polynomial of degree n is frequently spoken of as an *n-ic polynomial*. The reader is already familiar with the terms *linear*, *quadratic*, *cubic*, *quartic*, and *quintic* polynomial in the respective cases $n = 1, 2, 3, 4, 5$.

In a similar fashion a polynomial in $x_1, \ldots, x_q$ is called a *q-ary polynomial*. As above, we specialize the terminology in the cases $q = 1, 2, 3, 4, 5$ to be *unary*, *binary*, *ternary*, *quaternary*, and *quinary*.

The terminology just described is used much more frequently in connection with theorems on forms than in the study of arbitrary polynomials. In particular, we shall find that our principal interest is in n-ary *quadratic* forms.

There are certain special forms which are quadratic in a set of variables $x_1, \ldots, x_m, y_1, \ldots, y_n$ and which have special importance because they

are linear in both $x_1, \ldots, x_m$ and $y_1, \ldots, y_n$, separately. We shall call such forms *bilinear forms*. They may be expressed as forms

$$f = \sum_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}} x_i a_{ij} y_j , \tag{20}$$

so that we may thus write

$$f = \sum_{j=1}^{n} a_j y_j , \qquad a_j = \sum_{i=1}^{m} x_i a_{ij} , \tag{21}$$

and see that f may be regarded as a linear form in $y_1, \ldots, y_n$ whose coefficients are linear forms in $x_1, \ldots, x_m$.

A bilinear form f is called *symmetric* if it is unaltered by the interchange of correspondingly labeled members of its two sets of variables. This statement clearly has meaning only if $m = n$; and f is symmetric if and only if $f = \Sigma x_i a_{ij} y_j = \Sigma y_i a_{ij} x_j$. But $f = \Sigma y_j a_{ji} x_i$, and hence f is symmetric if and only if $m = n$,

$$a_{ij} = a_{ji} \qquad (i, j = 1, \ldots, n) . \tag{22}$$

A *quadratic* form f is evidently a sum of terms of the type $a_i x_i^2$ as well as the type $c_{ij} x_i x_j$ for $i \neq j$. We may write $a_{ii} = a_i$, $a_{ij} = a_{ji} = \frac{1}{2} c_{ij}$ for $i \neq j$ and have $c_{ij} x_i x_j = a_{ij} x_i x_j + a_{ji} x_j x_i$, so that

$$f = \sum_{i,j=1}^{n} x_i a_{ij} x_j \qquad (a_{ij} = a_{ji};\ i, j = 1, \ldots, n) . \tag{23}$$

We compare this with (22) and conclude that a quadratic form may be regarded as the result of replacing the variables $y_1, \ldots, y_n$ in a symmetric bilinear form in $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ by $x_1, \ldots, x_n$, respectively. Later we shall obtain a theory of equivalence of quadratic forms and shall use the result just derived to obtain a parallel theory of symmetric bilinear forms.

A final type of form of considerable interest is the *skew bilinear form*. Here again $m = n$, and we call a bilinear form f *skew* if $f = f(x_1, \ldots, x_n; y_1, \ldots, y_n) = -f(y_1, \ldots, y_n; x_1, \ldots, x_n)$. Thus skew bilinear forms are forms of the type

$$f = \sum_{i,j=1}^{n} x_i a_{ij} y_j , \tag{24}$$

where

$$a_{ji} = -a_{ij} \qquad (i, j = 1, \ldots, n). \tag{25}$$

It follows that $a_{ii} + a_{ii} = 0$, that is

$$a_{ii} = 0 \qquad (i = 1, \ldots, n). \tag{26}$$

Hence f is a sum of terms $a_{ij}(x_iy_j - x_jy_i)$ for $i \neq j$, $i = 1, \ldots, n-1$, $j = 2, \ldots, n$. It is also evident that if we replace the y_j by corresponding x_j, then the new quadratic form $f(x_1, \ldots, x_n; x_1, \ldots, x_n)$ is the zero polynomial. It is important for the reader to observe thus that while (22) may be associated with both quadratic and symmetric bilinear forms we must associate (25) only with skew *bilinear* forms.

ORAL EXERCISES

1. Use the language above to describe the following forms:

a) $x^3 + 3xy^2 + z^3$
b) $x_1^3 + y_1^3$
c) $2x_1y_1 + x_2y_1 + x_1y_2$
d) $x_1^2 + 2x_1y_1$
e) $x_1y_2 - x_2y_1$

2. Express the following quadratic forms as sums of the kind given by (23):

a) $2x_1^2 + 3x_1x_2$
b) $x_1^2 - x_2^2 + 2x_1x_3 + 2x_2^2 - 4x_2x_3$

8. Linear forms. A linear form is expressible as a sum

$$f = a_1x_1 + \ldots + a_nx_n. \tag{27}$$

We shall call (27) a *linear combination* of $x_1, \ldots, x_n$ with coefficients $a_1, \ldots, a_n$. The concept of linear combination has already been used without the name in several instances. Thus any polynomial in x is a linear combination of a finite number of non-negative integral powers of x with constant coefficients, a polynomial in $x_1, \ldots, x_q$ is a linear combination of a finite number of power products $x_1^{k_1} \ldots x_q^{k_q}$ with constant coefficients, the g.c.d. of $f(x)$ and $g(x)$ is a linear combination (10) of $f(x)$ and $g(x)$ with polynomials in x as coefficients.

The form (27) with $a_1 = a_2 = \ldots = a_n = 0$ is the zero form. If g is a second form,

$$g = b_1x_1 + \ldots + b_nx_n, \tag{28}$$

with constant coefficients $b_1, \ldots, b_n$, we see that

$$f + g = (a_1 + b_1)x_1 + \ldots + (a_n + b_n)x_n. \tag{29}$$

Also if c is any constant, we have

$$cf = (ca_1)x_1 + \ldots + (ca_n)x_n . \tag{30}$$

We define $-f$ to be the form such that $f + (-f) = 0$ and see that

$$-f = -1 \cdot f = (-a_1)x_1 + \ldots + (-a_n)x_n . \tag{31}$$

Then $f = g$ if and only if $f - g = f + (-g) = 0$, that is $a_i = b_i$ $(i = 1, \ldots, n)$.

The properties just set down are only trivial consequences of the usual properties of polynomials and, as such, may seem to be relatively unimportant. They may be formulated abstractly, however, as properties of *sequences of constants* (which may be thought of, if we so desire, as the coefficients of linear forms) and in this formulation in Chapter IV will be very important for all algebraic theory. The reader is already familiar with these properties which he has used in the computation of determinants by operations on its rows and columns.

Let, then, u be a sequence

$$u = (a_1, \ldots, a_n) \tag{32}$$

of n constants a_i called the *elements* of the sequence u. If a is any constant, we define

$$au = ua = (aa_1, \ldots, aa_n) \tag{33}$$

and call au the *scalar product* of u by a. We now consider a second sequence,

$$v = (b_1, \ldots, b_n) , \tag{34}$$

and define the sum of u and v by

$$u + v = (a_1 + b_1, \ldots, a_n + b_n) . \tag{35}$$

Then the linear combination

$$au + bv = (aa_1 + bb_1, \ldots, aa_n + bb_n) \tag{36}$$

has been uniquely defined for all constants a and b and all sequences u and v.

The sequence all of whose elements are zero will be called the *zero sequence* and designated by 0. It is clearly the unique sequence z with the

property that $u + z = u$ for every sequence u. Evidently if a is the zero constant $au = 0$ for every u.

We define the negative $-u$ of a sequence u to be the sequence v such that $u + v = 0$. Evidently, then, $-u$ is the unique sequence

$$-u = -1 \cdot u = (-a_1, \ldots, -a_n), \tag{37}$$

and we see that the unique solution of the equation $u + x = v$ is the sequence $v + (-u)$. We evidently call this sequence

$$v - u = (b_1 - a_1, \ldots, b_n - a_n). \tag{38}$$

The reader should observe now that the definitions and properties derived for linear combinations of sequences are precisely those which hold for the sequences of coefficients of corresponding linear combinations of linear forms and that the usual laws of algebra for addition and multiplication hold for addition of sequences and multiplication of sequences by constants.

9. Equivalence of forms. If $f = f(x_1, \ldots, x_q)$ is a form of degree n in $x_1, \ldots, x_q$ and we replace every x_i in f by a corresponding linear form

$$x_i = a_{i1}y_1 + \ldots + a_{ir}y_r \quad (i = 1, \ldots, q), \tag{39}$$

we obtain a form $g = g(y_1, \ldots, y_r)$ of the same degree n in $y_1, \ldots, y_r$. Then we shall say that f is carried into g (or that g is obtained from f) by the *linear mapping* (39). If $q = r$ and the determinant

$$\begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1q} \\ . & . & \ldots & . \\ a_{q1} & a_{q2} & \ldots & a_{qq} \end{vmatrix} \tag{40}$$

is not zero, we shall say that (39) is nonsingular. In this case it is easily seen that we may solve (39) for $y_1, \ldots, y_q$ as linear forms in $x_1, \ldots, x_q$ and obtain a linear mapping which we may call the *inverse* of (39). This terminology is justified by the fact that the equation $f(x_1, \ldots, x_q) = g(y_1, \ldots, y_q)$ is an identity, and thus if we replace $y_1, \ldots, y_q$ in $g(y_1, \ldots, y_q)$ by the corresponding linear forms in $x_1, \ldots, x_q$ we obtain the *original form* $f(x_1, \ldots, x_q)$.

We now consider two forms $f = f(x_1, \ldots, x_q)$ and $g = g(x_1, \ldots, x_q)$ of the same degree n. Then we shall say that f is *equivalent* to g if f is carried into $g(y_1, \ldots, y_q)$ by a nonsingular linear mapping. The statements above imply that if f is equivalent to g then g is also equivalent to f. Thus, we

shall usually say simply that f and g are *equivalent*. We shall not study the equivalence of forms of arbitrary degree but only of the special kinds of forms described in Section 7, and even of those forms only under restricted types of linear mappings.

We have now obtained the background needed for a clear understanding of matrix theory and shall proceed to its development.

EXERCISES

1. The linear mapping (39) of the form $x_i = y_i$ for $i = 1, \ldots, q$ is called the identical mapping. What is its effect on any form f?

2. Apply a nonsingular linear mapping to carry each of the following forms to an expression of the type $a_1y_1^2 + a_2y_2^2$. Hint: Write $f = a_1(x_1 + cx_2)^2 + \ldots$ by completing the square on the term in x_1^2 and put $x_1 + cx_2 = y_1$, $x_2 = y_2$.

a) $2x_1^2 - 4x_1x_2 + 3x_2^2$
b) $x_1^2 + 14x_1x_2 + 9x_2^2$
c) $3x_1^2 + 18x_1x_2 + 24x_2^2$
d) $2x_1^2 - x_1x_2$
e) $3x_1^2 + 2x_1x_2 - x_2^2$

3. Find the inverses of the following linear mappings:

a) $\begin{cases} 2x_1 + x_2 = y_1 \\ 3x_1 + 2x_2 = y_2 \end{cases}$ *b*) $\begin{cases} x_1 + x_2 = y_1 \\ -2x_1 + x_2 = y_2 \end{cases}$

4. Apply the linear mappings of Ex. 3 to the following forms f to obtain equivalent forms g and their inverses to g to obtain f.

a) $f = x_1^2 + x_2^2$ *b*) $f = 4x_1^2 - 4x_1x_2 + 3x_2^2$

CHAPTER II

RECTANGULAR MATRICES AND ELEMENTARY TRANSFORMATIONS

1. The matrix of a system of linear equations. The concept of a *rectangular matrix* may be thought of as arising first in connection with the study of the solution of a system

$$(1)\qquad \begin{cases} a_{11}y_1 + a_{12}y_2 + \ldots + a_{1n}y_n = k_1, \\ a_{21}y_1 + a_{22}y_2 + \ldots + a_{2n}y_n = k_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ a_{m1}y_1 + a_{m2}y_2 + \ldots + a_{mn}y_n = k_m \end{cases}$$

of m linear equations in n unknowns $y_1, \ldots, y_n$, with constant coefficients a_{ij}. The array of coefficients arranged as they occur in (1) has the form

$$(2)\qquad A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}$$

and is called the *coefficient matrix* of the system (1). We shall henceforth speak of the coefficients a_{ij} and k_i in (1) as *scalars* and shall derive our theorems with the understanding that they are constants (with respect to the variables $y_1, \ldots, y_n$) according to the usual definitions and hence satisfy the properties usually assumed in algebra for rational operations. In a later chapter we shall make a completely explicit statement about the nature of these quantities.

It is not only true that the concept of a matrix arises as above in the study of systems of linear equations, but many matrix properties are obtainable by observing the effect, on the matrix of a system, of certain natural manipulations on the equations themselves with which the reader is very familiar. We shall devote this beginning chapter on matrices to that study.

Let us now recall some terminology with which the reader is undoubtedly familiar. The line

$$(3)\qquad u_i = (a_{i1}, \ldots, a_{in})$$

of coefficients in the ith equation of (1) occurs in (2) as its ith horizontal line. Thus, it is natural to call u_i the ith *row* of the matrix A. Similarly, the coefficients of the unknowns y_j in (1) form a vertical line

$$u^{(j)} = \begin{pmatrix} a_{1j} \\ \cdot \\ \cdot \\ \cdot \\ a_{mj} \end{pmatrix} \tag{4}$$

which we call the jth *column* of A.

We may now speak of A as a matrix of m rows and n columns, as an m-rowed and n-columned matrix or, briefly, as an m by n matrix. Then the rows of A are 1 by n matrices and its columns are m by 1 matrices. We shall speak of the scalars a_{ij} as the *elements* of A, and they may be regarded as one by one matrices. The notation a_{ij} which we adopt for the element of A in its ith row and jth column will be used consistently, and this usage will be of some importance in the clarity of our exposition. To avoid bulky displayed equations we shall usually not use the notation (2) for a matrix but shall write instead

$$A = (a_{ij}) \quad (i = 1, \ldots, m; j = 1, \ldots, n). \tag{5}$$

If $m = n$ then A is a *square matrix*, and we shall speak of A simply as an m-rowed square matrix. This, too, is a concept and terminology which we shall use very frequently.

ORAL EXERCISES

1. Read off the elements a_{11}, a_{12}, a_{24}, a_{23} in the following matrices

$$a) \begin{pmatrix} 1 & -2 & 0 & 3 \\ 3 & 4 & -1 & 0 \\ -1 & 2 & 3 & 1 \\ 3 & 4 & 1 & 2 \end{pmatrix} \qquad b) \begin{pmatrix} 1 & 0 & -2 & 3 \\ 2 & 0 & 1 & 2 \\ -1 & 3 & 4 & 1 \\ 5 & 1 & 6 & 7 \end{pmatrix}$$

$$c) \begin{pmatrix} 4 & 0 & 5 & 0 \\ 0 & -1 & -2 & -3 \\ 3 & 1 & 4 & 7 \\ 6 & 0 & -1 & 8 \end{pmatrix} \qquad d) \begin{pmatrix} 3 & 2 & 4 & 5 \\ -1 & 1 & 6 & -6 \end{pmatrix}$$

2. Read off the second row and the third column in each of the matrices of Ex. 1.

3. Read off the systems of equations (1) with constants k_i all zero and matrices of coefficients as in Ex. 1.

2. Submatrices. In solving the system (1) by the usual methods the reader is led to study subsystems of $s \leq m$ equations in certain $t \leq n$ of the unknowns. The corresponding coefficient matrix has s rows and t columns, and its elements lie in certain s of the rows and t of the columns of A. We call such a matrix an s by t *submatrix* B of A. If $s < m$ and $t < n$, the elements in the remaining $m - s$ rows and $n - t$ columns form an $m - s$ by $n - t$ submatrix C of A and we shall call C the *complementary submatrix* of B. Clearly, then, B is the complementary submatrix of C.

It will be desirable from time to time to regard a matrix as being made up of certain of its submatrices. Thus we write

$$A = (A_{ij}) \qquad (i = 1, \ldots, s; j = 1, \ldots, t), \tag{6}$$

where now the symbols A_{ij} themselves represent rectangular matrices. We assume that for any fixed i the matrices $A_{i1}, A_{i2}, \ldots, A_{it}$ all have the same number of rows, and for fixed k the matrices $A_{1k}, A_{2k}, \ldots, A_{sk}$ have the same number of columns. It is then clear how each row of A is a 1 by t matrix whose elements are rows of $A_{i1}, \ldots, A_{it}$ in adjacent positions and similarly for columns. We have thus accomplished what we shall call the *partitioning* (6) of A by what amounts to drawing lines mentally parallel to the rows and columns of A and between them and designating the arrays of elements in the smallest rectangles so formed by A_{ij}. Our principal use of (6) will be the use of the case where we shall regard A as a two by two matrix

$$A = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix} \tag{7}$$

whose elements A_1, A_2, A_3, A_4 are themselves rectangular matrices. Then A_1 and A_2 have the same number of rows, A_3 and A_4 have the same number of rows, and every row of A consists partially of a row of A_1 and of a corresponding row of A_2 or of a row of A_3 and a corresponding row of A_4.

Note our usage in (2), (5), (6), (7) of the symbol of *equality* for matrices. We shall always mean that two matrices are equal if and only if they are identical, that is, have the same size and equal corresponding elements.

EXERCISES

1. State how the columns of A of (7) are connected with the columns of A_1, A_2, A_3, and A_4.

2. Introduce a notation of an arbitrary six-rowed square matrix A and partition A into a three-rowed square matrix whose elements are two-rowed square matrices.

Also partition A into a two-rowed square matrix whose elements are three-rowed square matrices.

3. Write out *all* submatrices of the matrix

$$\begin{pmatrix} 2 & -1 & 3 & 4 & 5 \\ 1 & 0 & 2 & -1 & -2 \\ 0 & 1 & 2 & 3 & 6 \\ 7 & 3 & 2 & 1 & 0 \end{pmatrix}$$

and, if they exist, the complementary submatrices.

4. Which of the submatrices in Ex. 3 occur in some partitioning of A as a matrix of submatrices?

5. Partition the following matrices so that they become three-rowed square matrices whose elements are two-rowed square matrices and state the results in the notation (6).

$$a)\ \begin{pmatrix} 2 & -1 & 3 & 4 & 1 & 2 \\ 0 & 1 & 1 & -1 & 2 & 1 \\ 1 & -2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & -1 & 3 \\ 0 & 0 & 4 & 2 & 1 & 0 \\ 0 & 0 & -1 & 3 & 0 & 1 \end{pmatrix} \qquad b)\ \begin{pmatrix} 1 & -1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ -2 & 0 & 2 & 0 & 3 & 1 \\ 0 & 2 & 0 & 2 & -1 & 2 \\ 0 & 0 & -1 & 1 & -4 & 0 \\ 0 & 0 & -1 & -1 & 0 & -4 \end{pmatrix}$$

6. Partition the matrices of Ex. 5 into two-rowed square matrices whose elements are three-rowed square matrices.

7. Partition the matrices of Ex. 5 into the form (7) such that A_1 is a two by three matrix; a one by six matrix; a two by two matrix. Read off A_2, A_3, and A_4 and state their sizes.

3. Transposition. The theory of determinants arose in connection with the solution of the system (1). The reader will recall that many of the properties of determinants were only proved as properties of the rows of a determinant, and then the corresponding column properties were merely stated as results obtained by the process of interchanging rows and columns. We call the induced process *transposition* and define it as follows for matrices. Let A be an m by n matrix, a notation for which is given by (5), and define the matrix

$$A' = (g_{ji}) \qquad (g_{ji} = a_{ij};\ j = 1, \ldots, n;\ i = 1, \ldots, m), \tag{8}$$

which we shall call the *transpose* of A. It is an n by m matrix obtained from A by interchanging its rows and columns. Thus, the element a_{ij} in the ith row and jth column of A occurs in A' as the element in its jth row and ith

column. Note then that in accordance with our conventions (8) could have been written as

$$A' = \left((a_{ij})_{ji}\right) \qquad (j = 1, \ldots, n; i = 1, \ldots, m). \tag{9}$$

We also observe the evident theorem which we state simply as

$$(A')' = A. \tag{10}$$

The operation of transposition may be regarded as the result of a certain rigid motion of the matrix which we shall now describe. If A is our m by n matrix and $m \leq n$ we put $q = m$ and write

$$A = (A_1, A_2), \tag{11}$$

where A_1 is a q-rowed *square* matrix. On the other hand, if $n \leq m$, we put $q = n$ and have

$$A = \begin{pmatrix} A_1 \\ B_2 \end{pmatrix}, \tag{12}$$

where the matrix A_1 is again a q-rowed square matrix. The line of elements $a_{11}, a_{22}, \ldots, a_{qq}$ of A and hence of A_1 is called the *principal diagonal* of A or, simply, the *diagonal* of A. It is a diagonal of the square matrix A_1 and is its principal diagonal. We shall call the a_{ii} the *diagonal elements* of A. Notice now that A' is obtained from A by using the diagonal of A as an axis for a *rigid rotation* of A so that each row of A becomes a column of A'. We should also observe that if A has been partitioned so that it has the form (6) then A' is the t by s matrix of matrices given by

$$A' = (G_{ji}) \qquad (G_{ji} = A'_{ij}; j = 1, \ldots, t; i = 1, \ldots, s). \tag{13}$$

We have now given some simple concepts in the theory of matrices and shall pass on to a study of certain fundamental operations.

EXERCISES

1. Let A have the form (7). Give the corresponding notation for A'. Give also A' if A is any matrix of Ex. 1 of Section 1.

2. In Ex. 1 assume that $A = A'$. What then is the form (7) of A? Obtain the analogous result if $A = -A'$, where $-A$ is the matrix whose elements are the negatives of those of A.

3. Let A be a three-rowed square matrix. Find the form (2) of A if $A = A'$ and also if $A = -A'$.

4. Prove that the determinant of every three-rowed square matrix A with the property that $A' = -A$ is zero.

5. Solve the system (1) with matrix

$$A = \begin{pmatrix} 1 & -2 & 1 \\ -1 & 3 & -2 \\ 2 & -4 & 3 \end{pmatrix}$$

for y_1, y_2, y_3 in terms of k_1, k_2, k_3. Write the results as $y_i = \sum_{j=1}^{3} b_{ij}k_j$ and thus compute the matrix $B = (b_{ij})$. Do this also for the system (1) with matrix A' and compare the results.

4. Elementary transformations. The system (1) may be solved by the method of *elimination*, and the reader is familiar with the operations on equations which are permitted in this method and which yield systems said to be equivalent to (1). The resulting operations on the rows of the matrix A of the system and corresponding operations on the columns of A are called *elementary transformations* on A and will turn out to be very useful tools in the theory of matrices.

The first of our transformations is the result on the rows of A of the interchange of two equations of the defining system. We define this and the corresponding column transformation in the

DEFINITION 1. *Let* i $\neq$ r *and* B *be the matrix obtained from* A *by interchanging its* i*th and* r*th rows (columns). Then* B *is said to be obtained from* A *by an elementary row (column) transformation of type 1.*

The rows (columns) of an m by n matrix are sequences of n (of m) elements, and the operations of addition and scalar multiplication (i.e., multiplication by a scalar) of such sequences were defined in Section 1.8.* The left members of (1) are linear forms. The addition of a scalar multiple of one equation of (1) to another results in the addition of a corresponding multiple of a corresponding linear form to another and hence to a corresponding result on the rows of A. Thus we make the following

DEFINITION 2. *Let* i *and* r *be distinct integers,* c *be a scalar, and* B *be the matrix obtained by the addition to the* i*th row (column) of* A *of the multiple by* c *of its* r*th row (column). Then* B *is said to be obtained from* A *by an elementary row (column) transformation of type 2.*

Our final type of transformation is induced by the multiplication of an

* We shall use a corresponding notation henceforth when we make references anywhere in our text to results in previous chapters. Thus, for example, by *Section* 4.7, *Theorem* 4.8, *Lemma* 4.9, *equation* (4.10) we shall mean *Section* 7, *Theorem* 8, *Lemma* 9, *equation* (10) in Chapter IV. However, if the prefix is omitted, as, for example, *Theorem* 8, we shall mean that theorem of the chapter in which the reference is made.

equation of the system (1) by a nonzero scalar a. The restriction $a \neq 0$ is made so that A will be obtainable from B by the like transformation for a^{-1}. Later we shall discuss matrices whose elements are polynomials in x and use elementary transformations with polynomial scalars a. We shall then evidently require a to be a polynomial with a polynomial inverse and hence to be a constant not zero. In view of this fact we shall phrase the definition in our present environment so as to be usable in this other situation and hence state it as

DEFINITION 3. *Let the scalar* a *possess an inverse* a^{-1} *and the matrix* B *be obtained as the result of the multiplication of the* i*th row (column) of* A *by* a. *Then* B *is said to be obtained from* A *by an elementary row (column*) transformation of type 3.*

The fundamental theorems in the theory of matrices are connected with the study of the matrices obtained from a given matrix A by the application of a finite sequence of elementary transformations, restricted by the particular results desired, to A. Thus, it is of basic importance to study first what occurs if we make no restriction whatever on the elementary transformations allowed. For convenience in our discussion we first make the

DEFINITION. *Let* A *and* B *be* m *by* n *matrices and let* B *be obtainable from* A *by the successive application of finitely many arbitrary elementary transformations. Then we shall say that* A *is* rationally equivalent *to* B *and indicate this by writing* $A \cong B$.

We now observe some simple consequences of our definition. First, we see that, if A is rationally equivalent to B and B is rationally equivalent to C, the combination of the elementary transformations which carry A to B with those which carry B to C will carry A to C. Then A is rationally equivalent to C. Observe next that every m by n matrix A is rationally equivalent to itself. For the elementary transformations of type 2 with $c = 0$ and of type 3 with $a = 1$ are identical transformations leaving all matrices unaltered.

Finally, we see that if an elementary transformation carries A to B there is an inverse transformation of the same type carrying B to A. In fact, the inverse of any transformation of type 2 defined for c is that defined for $-c$, inverse of any transformation of type 2 defined for c is that defined for $-c$, of type 3 defined by a is that defined for a^{-1}, of type 1 is itself. But then A is rationally equivalent to B if and only if B is rationally equivalent to A.

* The reader should verify the fact that, if we apply any elementary row transformation to A and then any column transformation to the result, the matrix obtained is the same as that which we obtain by applying first the column transformation and then the row transformation.

Thus we may and shall replace the terminology A *is rationally equivalent to* B in the definition above by A *and* B *are rationally equivalent.*

We have now shown that in order to prove that A and B are rationally equivalent it suffices to prove A and B both rationally equivalent to the same matrix C. As a tool in such proofs we then prove the following

LEMMA 1. *Let* $\mathrm{r} < \mathrm{m}$, $\mathrm{s} < \mathrm{n}$, *and* A *and* B *be* m *by* n *matrices of the form*

$$\mathrm{A} = \begin{pmatrix} \mathrm{A}_1 & 0 \\ 0 & \mathrm{A}_2 \end{pmatrix}, \qquad \mathrm{B} = \begin{pmatrix} \mathrm{B}_1 & 0 \\ 0 & \mathrm{B}_2 \end{pmatrix},$$

for r *by* s *rationally equivalent matrices* A_1 *and* B_1 *and* $\mathrm{m} - \mathrm{r}$ *by* $\mathrm{n} - \mathrm{s}$ *rationally equivalent matrices* A_2 *and* B_2. *Then* A *and* B *are rationally equivalent.*

For it is clear that any elementary transformation on the first r rows and s columns of A induces a corresponding transformation on A_1 and leaves A_2 and the zero matrices bordering it above unaltered. Clearly the sequence of such transformations induced by the transformations carrying A_1 to B_1 will replace A by the matrix

$$A_0 = \begin{pmatrix} B_1 & 0 \\ 0 & A_2 \end{pmatrix}.$$

We similarly follow this sequence of elementary transformations by elementary transformations on the last $m - r$ rows and $n - s$ columns of A_0 which carry A_2 to B_2 and obtain B.

It is important also to observe that *we may arbitrarily permute* the rows of A by a sequence of elementary row transformations of type 2, and similarly we may permute its columns. For any permutation results from some properly chosen sequence of interchanges.

Before continuing further with the study of rational equivalence we shall introduce the familiar properties of determinants in the language of matrix theory and shall also define some important special types of matrices. We shall then discuss another result used for the types of proofs mentioned above.

5. Determinants. Let B be the square matrix

$$B = (b_{ij}) \qquad (i, j = 1, \ldots, t). \tag{14}$$

The corresponding symbol

$$D = \begin{vmatrix} b_{11} & \ldots & b_{1t} \\ b_{21} & \ldots & b_{2t} \\ \ldots & \ldots & \ldots \\ b_{t1} & \ldots & b_{tt} \end{vmatrix} \tag{15}$$

is called a *t-rowed determinant* or determinant of *order t*. It is defined as the sum of the $t!$ terms of the form

$$(-1)^{i} b_{1i_1} b_{2i_2} \cdots b_{ti_t}, \tag{16}$$

where the sequence of subscripts $i_1, \ldots, i_t$ ranges over all permutations of $1, 2, \ldots, t$ and the permutation $i_1, \ldots, i_t$ may be carried into $1, 2, \ldots, t$ by i interchanges. That the sign $(-1)^i$ is unique is proved in L. E. Dickson's *First Course in the Theory of Equations*, and we shall assume this result as well as all the consequent properties of determinants derived there.

The determinant D will be spoken of here as *the determinant of* the matrix B and we shall indicate this by writing

$$D = |B| \tag{17}$$

(read D equals determinant B). Nonsquare matrices A do not have determinants, but their square submatrices have determinants called the *minors* of A. If A is a square matrix of $n > t$ rows, the complementary submatrix of any t-rowed square submatrix B is an $(n - t)$-rowed square matrix whose determinant and that of B are minors of A called *complementary minors*. In particular, every element a_{ij} of a matrix A defines a one-rowed square submatrix of A whose determinant is the element itself. Thus we have seen that *the elements of a matrix may be regarded either as its one-rowed square submatrices or as its one-rowed minors*. We now pass to a statement of some of the most important results on determinants.

The result on the interchange of rows and columns of determinants mentioned in Section 3 may now be stated as

LEMMA 2. *Let* A *be a square matrix. Then*

$$|\mathrm{A}'| = |\mathrm{A}|. \tag{18}$$

The next three properties of determinants are those frequently used in the computation of determinants, and we shall state them now in the language we have just introduced.

LEMMA 3. *Let* B *be the matrix obtained from a square matrix* A *by an elementary transformation of type 1. Then* $|\mathrm{B}| = -|\mathrm{A}|$.

LEMMA 4. *Let* B *be the matrix obtained from a square matrix* A *by an elementary transformation of type 2. Then* $|\mathrm{B}| = |\mathrm{A}|$.

LEMMA 5. *Let* B *be the matrix obtained from a square matrix* A *by an elementary transformation of type 3 defined for a scalar* a. *Then* $|\mathrm{B}| = \mathrm{a} \cdot |\mathrm{A}|$.

The reader will recall that Lemma 3 may be used in a simple fashion to obtain

LEMMA 6. *If a square matrix has two equal rows or columns, its determinant is zero.*

Another result of this type is

LEMMA 7. *If a square matrix has a zero row or column, its determinant is zero.*

Finally, we have

LEMMA 8. *Let* A, B, C *be* n*-rowed square matrices such that the* i*th row (column) of* C *is the sum of the* i*th row (column) of* A *and that of* B *while all other rows (columns) of* B *and* C *are the same as the corresponding rows (columns) of* A. *Then*

$$|C| = |A| + |B| . \tag{19}$$

There are, of course, many other properties of determinants, and of these we shall use only very few. Those we shall use are, of course, also well known to the reader. Of particular importance is that result which might be used to define determinants by an induction on order and which does yield the actual process ordinarily used in the expansion of a determinant. We let A be an n-rowed square matrix $A = (a_{ij})$ and define d_{ij} to be the complementary minor of a_{ij}. Then the result we refer to states that if we define $c_{ji} = (-1)^{i+j}d_{ij}$ then

$$|A| = \sum_{k=1}^{n} a_{ik}c_{ki} = \sum_{k=1}^{n} c_{jk}a_{kj} \qquad (i, j, = 1, \ldots, n) . \tag{20}$$

Thus, the determinant of A is obtainable as the sum of the products of the elements a_{ij} in any row (column) of A by their *cofactors* c_{ji}, that is, the properly signed and labeled minors $(-1)^{i+j}d_{ij}$.

The result (20) is of fundamental importance in our theory of matrices and will be applied presently together with the following parallel result. Let B be the matrix obtained from a square matrix A by replacing the ith row of A by its qth row. Then B has two equal rows and by Lemma 6 $|B| = 0$. We expand B as above according to the elements of its ith row and obtain as its vanishing determinant the sum of the products of all elements in the qth row of A by the cofactors of the elements in the ith row of A. Combining this result with the corresponding property about columns we have

$$\sum_{k=1}^{n} a_{ik}c_{kq} = \sum_{k=1}^{n} c_{sk}a_{kj} = 0 \tag{21}$$

$$(i \neq q, s \neq j; i, j, q, s = 1, \ldots, n) .$$

The equations (20) and (21) exhibit certain relations between the arbitrary square matrix A and the matrix we define as

$$\text{adj } A = (c_{ij}) \qquad (i, j = 1, \ldots, n). \tag{22}$$

These relations will have important later consequences. We call the matrix (22) the *adjoint* of A and see that if $A = (a_{ij})$ is an n-rowed square matrix its adjoint is the n-rowed square matrix with the cofactor of the element which appears in the jth row and ith column of A as the element in its own ith row and jth column. Clearly, if $A = 0$ then adj $A = 0$.

EXERCISES

1. Compute the adjoint of each of the matrices

$$a)\ \begin{pmatrix} 2 & -3 \\ 1 & 1 \end{pmatrix} \qquad b)\ \begin{pmatrix} -1 & 0 \\ 4 & 2 \end{pmatrix} \qquad c)\ \begin{pmatrix} 3 & 0 & -1 \\ -1 & 2 & 1 \\ -3 & 6 & 3 \end{pmatrix} \qquad d)\ \begin{pmatrix} 1 & 1 & -2 \\ 1 & 1 & -3 \\ 2 & 3 & -4 \end{pmatrix}$$

2. Expand the determinants below and verify the following instances of Lemma 8:

$$a)\ \begin{vmatrix} 3 & 2 & -1 \\ 1 & 2 & 0 \\ 0 & -1 & 3 \end{vmatrix} + \begin{vmatrix} 3 & -3 & -1 \\ 1 & -1 & 0 \\ 0 & 0 & 3 \end{vmatrix} = \begin{vmatrix} 3 & -1 & -1 \\ 1 & 1 & 0 \\ 0 & -1 & 3 \end{vmatrix}$$

$$b)\ \begin{vmatrix} 1 & -1 & 4 \\ 1 & -1 & 1 \\ 2 & 3 & 4 \end{vmatrix} + \begin{vmatrix} -1 & 1 & -3 \\ 1 & -1 & 1 \\ 2 & 3 & 4 \end{vmatrix} = \begin{vmatrix} 0 & 0 & 1 \\ 1 & -1 & 1 \\ 2 & 3 & 4 \end{vmatrix}$$

6. Special matrices. There are certain square matrices which have special forms but which occur so frequently in the theory of matrices that they have been given special names. The most general of these is the *triangular* matrix, that is, a square matrix having the property that either all its elements to the right or all to the left of its diagonal are zero. Thus a square matrix $A = (a_{ij})$ is triangular if it is true that either $a_{ij} = 0$ for all $j > i$ or that $a_{ij} = 0$ for all $j < i$. It is clear that A is triangular if and only if A' is triangular; and, moreover, we have

Theorem 1. *The determinant of a triangular matrix is the product* $a_{11}a_{22} \ldots a_{nn}$ *of its diagonal elements.*

The result above is clearly true if $n = 1$ so that $A = (a_{11})$, $|A| = a_{11}$. We assume it true for square matrices of order $n - 1$ and complete our induction by expanding $|A|$ according to the elements of its first row or first column in the respective cases above.

A matrix $A = (a_{ij})$ is called a *diagonal* matrix if it is a square matrix,

and $a_{ij} = 0$ for all $i \neq j$. Clearly, a diagonal matrix A is triangular so that its determinant is the product of its diagonal elements.

If all the diagonal elements of a diagonal matrix are equal, we call the matrix a *scalar* matrix and have $|A| = a_{11}^n$. The scalar matrix for which $a_{11} = 1$ is called the n-*rowed identity matrix* and will usually be designated by I. If there be some question as to the order of I or if we are discussing several identity matrices of different orders, we shall indicate the order by a subscript and thus shall write either I_n or I as is convenient for the n-rowed identity matrix.

Any scalar matrix may be indicated by

$$aI\,, \tag{23}$$

where $a = a_{11}$ is the common value of the diagonal elements of the matrix. We shall discuss the implications of this notation later.

It is natural to call any m by n matrix all of whose elements are zeros a *zero matrix*. In any discussion of matrices we shall use the notation 0 to represent not only the number zero but any zero matrix. The reader will find that this usage will cause neither difficulty nor confusion.

We shall frequently feel it desirable to consider square matrices of either of the forms

$$A = \begin{pmatrix} A_1 & 0 \\ A_3 & A_4 \end{pmatrix}, \qquad A_0 = \begin{pmatrix} A_1 & A_2 \\ 0 & A_4 \end{pmatrix}, \tag{24}$$

where A_1 is a square matrix. Then (24) implies that A_4 is necessarily square, and the reader should verify the fact that the Laplace expansion of determinants implies that

$$|A| = |A_0| = |A_1| \cdot |A_4|\,.$$

The property above and that of Theorem 1 are special instances of a more general situation. We let A be a square matrix and partition it as in (6) with $s = t$ and the submatrices A_{ii} all square matrices. Then the Laplace expansion clearly implies that if all the A_{ij} are zero matrices for either all $i > j$ or all $i < j$, then $|A| = |A_{11}| \ldots |A_{tt}|$. Evidently Theorem 1 is the case where the A_{ij} are one-rowed square matrices and the result considered in (24) the case where $t = 2$.

In connection with the discussion just completed we shall define a notation which is quite useful. Let A be a square matrix partitioned as in (6) and suppose that $s = t$, the A_{ii} are all square matrices, and every $A_{ij} = 0$

for $i \neq j$. Then A is composed of zero matrices and matrices $A_i = A_{ii}$ which are what we may call its *diagonal blocks*, and we shall indicate this by writing

$$A = \operatorname{diag}\{A_1, \ldots, A_t\}. \tag{25}$$

As above, the determinant of A is the product of the determinants of its submatrices $A_1, \ldots, A_t$.

In closing we note the following result which we referred to at the close of Section 4.

LEMMA 9. *Every nonzero* m *by* n *matrix* A *is rationally equivalent to a matrix*

$$\begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}, \tag{26}$$

where I *is an identity matrix.*

For by elementary transformations of type 1 we may carry any element $a_{pq} \neq 0$ of A into the element b_{11} of a matrix B which is rationally equivalent to A. By an elementary transformation of type 3 defined for $a = b_{11}^{-1}$ we replace B by a rationally equivalent matrix C with $c_{11} = 1$. We then apply elementary row transformations of type 2 with $c = -c_{r1}$ to replace C by the rationally equivalent matrix $D = (d_{ij})$ such that $d_{11} = 1$, $d_{r1} = 0$ for $r > 1$, and then use elementary column transformations of type 2 with $c = -d_{1r}$ to replace D by the matrix

$$A_0 = \begin{pmatrix} I_1 & 0 \\ 0 & A_1 \end{pmatrix}. \tag{27}$$

Now A_1 is an $m - 1$ by $n - 1$ matrix, and I_1 is the identity matrix of one row. Clearly, A and A_0 are rationally equivalent. Moreover, either $A_1 = 0$ and we have (26) for $I = I_1$, or our proof shows that A_1 is rationally equivalent to a matrix

$$B_1 = \begin{pmatrix} I_1 & 0 \\ 0 & A_2 \end{pmatrix}. \tag{28}$$

But then, by Lemma 1, A is rationally equivalent to a matrix

$$\begin{pmatrix} I_1 & 0 & 0 \\ 0 & I_1 & 0 \\ 0 & 0 & A_2 \end{pmatrix} = \begin{pmatrix} I_2 & 0 \\ 0 & A_2 \end{pmatrix}. \tag{29}$$

After finitely many such steps we obtain (26).

We shall show later that the number of rows in the matrix I of (26) is uniquely determined by A.

EXERCISES

1. Carry the following matrices into rationally equivalent matrices of the form (26)

$$a)\begin{pmatrix} 3 & 5 & 10 & 4 \\ 0 & 1 & 2 & 1 \\ -1 & -1 & -2 & 0 \end{pmatrix} \qquad b)\begin{pmatrix} 1 & 1 & 2 \\ 2 & 3 & 5 \\ 1 & 2 & 3 \end{pmatrix}$$

$$c)\begin{pmatrix} 1 & 0 & 1 & 2 \\ 2 & 0 & 2 & 3 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix} \qquad d)\begin{pmatrix} -1 & 1 & 1 & 1 \\ 3 & -3 & -3 & -3 \\ -2 & 2 & 2 & 2 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

2. Apply elementary row transformations only and carry each of the following matrices into a matrix of the form (26)

$$a)\begin{pmatrix} 2 & 1 & -2 \\ 1 & 1 & -3 \\ 3 & 2 & -4 \end{pmatrix} \qquad b)\begin{pmatrix} 1 & 0 & 1 & 0 \\ 2 & 2 & -5 & 0 \\ -2 & 1 & -5 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad c)\begin{pmatrix} 3 & 2 & 0 & 0 \\ 2 & 4 & 0 & 0 \\ 4 & 5 & 0 & 0 \end{pmatrix}$$

3. Apply elementary column transformations only and carry each of the following matrices into a matrix of the form (26).

$$a)\begin{pmatrix} 3 & 2 & -1 \\ 2 & 3 & -2 \\ 5 & 4 & -2 \end{pmatrix} \qquad b)\begin{pmatrix} 0 & -2 & 1 & 0 \\ 1 & 5 & -5 & 0 \\ 1 & 0 & -3 & 0 \\ 1 & 0 & -1 & -1 \end{pmatrix}$$

$$c)\begin{pmatrix} 1 & 0 & 3 & -1 \\ -1 & 2 & 4 & 5 \end{pmatrix} \qquad d)\begin{pmatrix} 0 & 1 & 0 & 2 \\ 0 & 5 & 1 & 3 \end{pmatrix}$$

4. Show that if the determinant of a square matrix A is not zero then A can be carried into the identity matrix by elementary row* transformations alone. Hint: The property $|A| \neq 0$ is preserved by elementary transformations. Some element in the first column of A must not be zero, and by row transformations we may carry A into a matrix with ones on the diagonal and zeros below and then into I.

7. Rational equivalence of rectangular matrices. The largest order of any nonvanishing minor of a rectangular matrix A is called the *rank* of A. The result of (20) states that every $(t+1)$-rowed minor of A is a sum of nu-

* Not every matrix may be carried into the form (26) by row transformations only, e.g., take $A = (1\ 1)$.

merical multiples of its t-rowed minors, and if the latter are all zero so are the former. We thus clearly have

LEMMA 10. *Let all* (r + 1)*-rowed minors of* A *vanish. Then the rank of* A *is at most* r.

We may also state this result as

LEMMA 11. *Let* A *have a nonzero* r*-rowed minor and let all* (r + 1)*-rowed minors of* A *vanish. Then* r *is the rank of* A.

Note that we are assigning zero as the rank of the zero matrix and that the rank of any nonzero matrix is at least 1.

The problem of computing the rank of a matrix A would seem from our definition and lemmas to involve as a minimum requirement the computation of at least one r-rowed minor of A and all $(r+1)$-rowed minors. The number of determinants to be computed would then normally be rather large, and the computations themselves generally quite complicated. However, the problem may be tremendously simplified by the application of elementary transformations. We are thus led to study the effect of such transformations on the rank of a matrix.

Let then A_0 result from the application of an elementary row transformation of either type 1 or type 3 to A. By Lemmas 3 and 5 every t-rowed minor of A_0 is the product by a nonzero scalar of a uniquely corresponding t-rowed minor of A, and it follows that A and A_0 have the same rank. If A_0 results when we add to the ith row of A the product by $c \neq 0$ of its gth row and B is a t-rowed square submatrix of A, the correspondingly placed submatrix B_0 of A_0 is equal to B if no row of B is a part of the ith row of A. If, however, a row of B is in the ith row of A and a row of B is in the gth row of B, then by Lemma 2.4 we have $|B_0| = |B|$. If, finally, a row of B is in the ith row of A but no row is in the gth row of A, then by Lemma 8 $|B_0| = |B| + c|C|$, where C is a t-rowed square matrix all but one of whose rows coincide with those of B, and this remaining row is obtained by replacing the elements of B in the ith row of A by the correspondingly columned elements in its gth row. But then it is easy to see that $\pm|C|$ is a minor of A as well as of A_0. If A has rank r we put $t = r + 1$ and see that $|B| = |C| = 0$, $|B_0| = 0$ for every $(r+1)$-rowed minor $|B_0|$ of A_0. Also there exists an r-rowed minor $|B| \neq 0$ in A, and our proof shows the existence of a corresponding minor $|B_0| = |B|$ or $|B_0| = |B| + c|C|$ in A_0. But then $|B_0| = 0$ implies that $|C| = -c^{-1}|B| \neq 0$, and A_0 has a nonzero r-rowed minor $\pm|C|$, A and A_0 have the same rank.

We observe, finally, that if an elementary row transformation be applied to the transpose A' of A to obtain A_1 and the corresponding column transformation be applied to A to obtain A_0, then $A_0' = A_1$. By the above

proof A' and A_1 have the same rank, by Lemma 2 A and A' have the same minors and hence the same rank, so that A_1 and $A_1' = A_0$ have the same rank. Hence, A and A_0 have the same rank. Thus, any two rationally equivalent matrices have the same rank.

Conversely, let the rank r of two m by n matrices A and B be the same and use Lemma 9 to carry A into a rationally equivalent matrix (26). It is clear that the rank of the matrix in (26) is the number of rows in the matrix I. By the above proof A and this matrix have the same rank, $I = I_r$, A is rationally equivalent to

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}. \tag{30}$$

Similarly, B is rationally equivalent to (30) and to A. We have thus proved what we regard as the principal result of this chapter.

Theorem 2. *Two* m *by* n *matrices are rationally equivalent if and only if they have the same rank.*

We have also the consequent

COROLLARY. *Every* m *by* n *matrix of rank* r *is rationally equivalent to an* m *by* n *matrix* (30).

A matrix is called *nonsingular* if it is a square matrix and its determinant is not zero. But then Theorem 2 implies, as in Ex. 4 of Section 6,

Theorem 3. *Every* n*-rowed nonsingular matrix is rationally equivalent to the* n*-rowed identity matrix.*

In closing let us observe a result of the application to a matrix of either row transformations only or column transformations only. We shall prove

Theorem 4. *Every* m *by* n *matrix of rank* $r > 0$ *may be carried into a matrix of the forms*

$$\begin{pmatrix} G \\ 0 \end{pmatrix}, \qquad (H \quad 0), \tag{31}$$

respectively, by a sequence of elementary row or column transformations only, where G *is an* r*-rowed matrix,* H *is an* r*-columned matrix, and both* G *and* H *have rank* r.

For A is equivalent to (30) by a sequence of elementary row and column transformations. Clearly, we may obtain (30) by first applying all the row transformations and then all the column transformations. If we then apply the inverses of the column transformations in reverse order to (30), we obtain the result of the application of the row transformations alone to A. But column transformations applied to (30) clearly carry this matrix into

a matrix of the form given by the first matrix of (31). Moreover, it is evident that the rank of this matrix is that of G, G has rank r. The result for column transformations is obtained similarly.

EXERCISES

1. Compute the rank r of the following matrices by using elementary transformations to carry each into a matrix with all but r rows (or columns) of zeros and an obvious r-rowed nonzero minor.

$$a)\ \begin{pmatrix} 1 & 1 & 3 \\ 1 & 5 & 2 \\ 1 & 5 & -1 \end{pmatrix} \qquad b)\ \begin{pmatrix} 2 & -1 & 4 \\ 1 & 3 & -2 \\ 1 & -11 & 14 \end{pmatrix}$$

$$c)\ \begin{pmatrix} 1 & -3 & 4 \\ 4 & -12 & 16 \\ 3 & -9 & 12 \end{pmatrix} \qquad d)\ \begin{pmatrix} 6 & 4 & 3 & -84 \\ 1 & 2 & 3 & -48 \\ 1 & -2 & 1 & -12 \\ 4 & 4 & -1 & -24 \end{pmatrix}$$

2. Carry the first of each of the following pairs of matrices into the second by elementary transformations. Hint: If necessary carry A and B into the form (30) and then apply the inverses of those transformations which carry B into (30) to carry (30) into B.

$$a)\ A = \begin{pmatrix} 2 & -1 & 3 \\ 1 & -1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

$$b)\ A = \begin{pmatrix} 1 & -2 & 1 \\ 1 & -2 & 2 \\ 2 & -4 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & 0 & -1 \\ 6 & 0 & 3 \\ 1 & 0 & 1 \end{pmatrix}$$

$$c)\ A = \begin{pmatrix} 1 & -2 & 1 \\ 2 & -4 & 2 \\ 3 & -6 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

CHAPTER III

EQUIVALENCE OF MATRICES AND OF FORMS

1. Multiplication of matrices. If $x_1, \ldots, x_m$ and $y_1, \ldots, y_n$ are variables related by a system of linear equations

$$x_i = \sum_{j=1}^{n} a_{ij} y_j \qquad (i = 1, \ldots, m), \tag{1}$$

this system was said in Section 1.9 to define a linear mapping carrying the x_i to the y_j. We call the m by n matrix $A = (a_{ij})$ the *matrix of the mapping* (1).

Suppose now that $z_1, \ldots, z_q$ are variables related to $y_1, \ldots, y_n$ by a second linear mapping

$$y_j = \sum_{k=1}^{q} b_{jk} z_k \qquad (j = 1, \ldots, n), \tag{2}$$

with n by q matrix $B = (b_{jk})$, carrying the y_j to the z_k. Then, if we substitute (2) in (1) we obtain a third linear mapping

$$x_i = \sum_{k=1}^{q} c_{ik} z_k \qquad (i = 1, \ldots, m), \tag{3}$$

with m by q matrix $C = (c_{ik})$, and it is easily verified by substitution that

$$c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk} \qquad (i = 1, \ldots, m;\ k = 1, \ldots, q). \tag{4}$$

The linear mapping (3) is usually called the *product* of the mappings (1) and (2), and we shall also write $C = AB$ and call the matrix C the *product* of the matrix A by the matrix B.

We have now defined the product AB of an m by n matrix A and an n by q matrix B to be a certain m by q matrix C. Moreover, we have defined C so that the element c_{ik} in its ith row and kth column is obtained

as the sum $c_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + \ldots + a_{in}b_{nk}$ of the products of the elements a_{ij} in the ith row

$$(a_{i1}, a_{i2}, \ldots, a_{in}) \tag{5}$$

of A, by the corresponding elements b_{jk} in the kth column

$$\begin{pmatrix} b_{1k} \\ b_{2k} \\ \cdot \\ \cdot \\ \cdot \\ b_{nk} \end{pmatrix} \tag{6}$$

of B. Thus we have stated what we shall speak of as the *row by column* rule for multiplying matrices.

Observe that if either A or B is a zero matrix the product AB is also. Moreover, if A is an m by n matrix, then we have

$$I_m A = A I_n = A, \tag{7}$$

where I_r represents the r-rowed identity matrix defined for every r as in Section 2.6. Observe also that I_m is the matrix of the linear transformation $x_i = y_i$ for $i = 1, \ldots, m$, and thus in this case the product of (1) by (2) is immediately (2); hence (7) is trivially true.

We have not defined and shall not define the product AB of two matrices in which the number of columns in A is not the same as the number of rows in B. Then, evidently, the fact that AB is defined need not imply that BA is defined. But when both are defined, they are generally not equal and may not even be matrices of the same size. This latter fact is clearly so if, for example, A is m by n, B is n by m, and $m \neq n$.

If A and B are n-rowed square matrices, we shall say that A and B are *commutative* if $AB = BA$. Note the examples of noncommutative square matrices in the exercises below.

Finally, let us observe the following

Theorem 1. *The transpose of a product of two matrices is the product of their transposes in reverse order.*

In symbols we state this result as

$$(AB)' = B'A'. \tag{8}$$

Here A is an m by n matrix, B is an n by q matrix, $(AB)'$ is a q by m matrix, which we state is the product of the q by n matrix B' and the n by m

matrix A'. We leave the direct application of the row by column rule to prove this result as an exercise for the reader.

EXERCISES

1. Compute (3) and hence the product $C = AB$ for the following linear changes of variables (mappings) and afterward compute C by the row by column rule.

$$a)\quad \begin{cases} x_1 = 2y_1 + y_2 \\ x_2 = 3y_1 - y_2 \\ x_3 = y_1 + 2y_2 \end{cases} \qquad \begin{cases} y_1 = z_1 - z_2 + z_3 \\ y_2 = -2z_1 + z_2 - 3z_3 \end{cases}$$

$$b)\quad \begin{cases} x_1 = 2y_1 + 3y_2 - y_3 \\ x_2 = y_1 + y_2 + 4y_3 \\ x_3 = y_2 - 9y_3 \end{cases} \qquad \begin{cases} y_1 = -13z_1 + 26z_2 + 13z_3 \\ y_2 = 9z_1 - 18z_2 - 9z_3 \\ y_3 = z_1 - 2z_2 - z_3 \end{cases}$$

2. Compute the following matrix products AB. Compute also BA in the cases where the latter product is defined.

$$a)\quad \begin{pmatrix} 4 & 3 & 2 \\ 3 & 2 & 1 \\ 2 & 1 & -1 \end{pmatrix}\begin{pmatrix} -1 & -2 & -3 \\ 1 & 3 & 0 \\ -1 & -2 & 4 \end{pmatrix} \qquad b)\quad \begin{pmatrix} 2 & 1 & 4 \\ 4 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 3 & 2 \\ -1 & 0 & 1 \\ 3 & 2 & 0 \end{pmatrix}$$

$$c)\quad \begin{pmatrix} 1 & -3 \\ -2 & 5 \\ 3 & -1 \\ 0 & -2 \end{pmatrix}\begin{pmatrix} 3 & 2 & 1 & 3 \\ 1 & 1 & 4 & 0 \end{pmatrix} \qquad d)\quad \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}(2 \quad -1 \quad 3 \quad 4)$$

$$e)\quad \begin{pmatrix} 6 \\ 2 \\ 0 \\ 1 \end{pmatrix}(-1 \quad 2 \quad 3 \quad 2)$$

3. Let the symbol E_{ij} represent the three-rowed square matrix with unity in the ith row and jth column and zeros elsewhere. Verify by explicit computation that $E_{ij}E_{jk} = E_{ik}$ and that if $j \neq g$ then $E_{ij}E_{gk} = 0$.

2. The associative law. It is important to know that matrix multiplication has the property

$$(AB)C = A(BC) \tag{9}$$

for every m by n matrix A, n by q matrix B, q by s matrix C. This result is known as the *associative law* for matrix multiplication and it may be shown as a consequence that no matter how we group the factors in forming a product $A_1 \ldots A_t$ the result is the same. In particular, the powers A^t of any square matrix are unique. We shall assume these two consequences of

(9) without further proof and refer the reader to treatises on the foundations of mathematics for general discussions of such questions.

To prove (9) we write $A = (a_{ij})$, $B = (b_{jk})$, $C = (c_{kl})$, where in all cases $i = 1, \ldots, m; j = 1, \ldots, n; k = 1, \ldots, q; l = 1, \ldots, s$. Then it is clear that the element in the ith row and lth column of $G = (AB)C$ is

$$g_{il} = \sum_{k=1}^{q} \left(\sum_{j=1}^{n} a_{ij} b_{jk} \right) c_{kl}, \tag{10}$$

while that in the same position in $H = A(BC)$ is

$$h_{il} = \sum_{j=1}^{n} a_{ij} \left(\sum_{k=1}^{q} b_{jk} c_{kl} \right). \tag{11}$$

Each of these expressions is a sum of nq terms which are respectively of the form $(a_{ij}b_{jk})c_{kl}$ and $a_{ij}(b_{jk}c_{kl})$. But those terms in the respective sums with the same sets of subscripts are equal, since we have already assumed that the elements of our matrices satisfy the associative law $a(bc) = (ab)c$. Hence, $g_{il} = h_{il}$ for all i and l, $G = H$, and (9) is proved.

EXERCISES

Compute the products $(AB)C$ and $A(BC)$ in the following cases.

a) $A = \begin{pmatrix} 2 & -1 & 3 \\ 3 & 1 & 2 \\ 0 & -1 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 2 & -1 \\ 1 & 2 \\ -1 & 1 \end{pmatrix}$, $C = \begin{pmatrix} 1 & 0 & 4 \\ -1 & 3 & 2 \end{pmatrix}$

b) $A = \begin{pmatrix} 2 & 2 & -3 \\ 3 & -1 & 4 \end{pmatrix}$, $B = \begin{pmatrix} 1 & -1 \\ 0 & -5 \\ -1 & -2 \end{pmatrix}$, $C = \begin{pmatrix} 2 & -1 & 0 & 1 \\ -1 & 1 & 1 & 0 \end{pmatrix}$

c) $A = (1 \quad 2 \quad -1 \quad 3)$, $B = \begin{pmatrix} 2 & -1 \\ 1 & 2 \\ 0 & -1 \\ 1 & 3 \end{pmatrix}$, $C = \begin{pmatrix} 1 \\ -2 \end{pmatrix}$

3. Products by diagonal and scalar matrices. Let $A = (a_{ij})$ be an m by n matrix and B be a diagonal matrix, and designate the ith diagonal element of B by b_i. Then our definition of product implies that if B is m-rowed so that BA is defined, then

$$BA = (b_i a_{ij}) \qquad (i = 1, \ldots, m; j = 1, \ldots, n); \tag{12}$$

while if B is n-rowed, then

$$AB = (a_{ij}b_j) \qquad (i = 1, \ldots, m; j = 1, \ldots, n). \tag{13}$$

Thus the product of a matrix A by a diagonal matrix B on the left is obtained as the result of multiplying the rows of A in turn by the corresponding diagonal elements of B; the product of A by a diagonal matrix on the right is the result of multiplying the columns of A in turn by the corresponding diagonal elements of B.

Now, let $m = n$, A be a square matrix. Then from (12) and (13) we see that $AB = BA$ if and only if

$$(b_i - b_j)a_{ij} = 0 \qquad (i, j = 1, \ldots, n). \tag{14}$$

As an immediate consequence of the case $b_1 = \ldots = b_n$ we have the very simple

Theorem 2. *Every* n*-rowed scalar matrix is commutative with all* n*-rowed square matrices.*

We next see that, if $i \neq j$ and $b_i \neq b_j$, then (14) implies that $a_{ij} = 0$. This gives the result we shall state as

Theorem 3. *Let the diagonal elements of an* n*-rowed diagonal matrix* B *be all distinct. Then the only* n*-rowed square matrices commutative with* B *are the* n*-rowed diagonal matrices.*

We may now prove the converse of Theorem 2—a result which is the inspiration of the name *scalar matrix.*

Theorem 4. *The only* n*-rowed square matrices which are commutative with every* n*-rowed square matrix are the scalar matrices.*

For let

$$B = (b_{ij}) \qquad (i, j, = 1, \ldots, n) \tag{15}$$

and suppose that B is commutative with *every* n-rowed square matrix A. We shall select A in various ways to obtain our theorem. First, we let E_i be the diagonal matrix with unity in its jth row and column and zeros elsewhere and put $BE_j = E_jB$. Equations (12) and (13) imply that the jth row of E_jB is the same as that of B and the jth column of BE_j is the same as that of B, while all other columns of BE_j are zero. Thus if $i \neq j$, the elements in the ith column of E_jB must be zero. Since b_{ji} is in the ith column, we have $b_{ji} = 0$ for $j \neq i$, and B is a diagonal matrix. If D_1 is the matrix with 1 in its first row and jth column and zeros elsewhere, the

product BD_j has b_{11} in its first row and jth column and is equal to the matrix D_jB which has b_{jj} in this same place. Hence, $b_{jj} = b_{11} = b$ for $j = 2, \ldots, n$, and B is the scalar matrix bI_n.

Let us now observe that if A is any m by n matrix and a is any scalar, then

$$(aI_m)A = A(aI_n) \tag{16}$$

is an m by n matrix whose element in the ith row and jth column is the product by a of the corresponding element of A. This is then a type of product

$$aA = Aa \tag{17}$$

like that defined in Chapter I for sequences, and we shall call such a product the *scalar product* of a by A. However, we have defined (17) as the instances (16) of our matrix product (4).

EXERCISES

1. Compute the products AB and BA by the use of (12) and (13) as well as the row by column rule if

$$a)\ A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 3 \end{pmatrix}, \qquad B = \begin{pmatrix} 2 & 4 & -5 \\ -4 & 0 & 1 \\ -1 & -3 & -2 \end{pmatrix}$$

$$b)\ A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} -1 & 0 & -2 \\ 2 & 1 & 4 \\ -2 & 3 & -3 \end{pmatrix}$$

$$c)\ A = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & -2 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$d)\ A = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 0 \end{pmatrix}$$

2. Find all three-rowed square matrices B such that $BA = AB$ if

$$a)\ A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \qquad b)\ A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

3. Prove by direct multiplication that $BA = -AB$ if $i^2 = -1$ and

$$A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

4. Let w be a primitive cube root of unity. Prove that $BA = wAB$ if

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & w & 0 \\ 0 & 0 & w^2 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ a & 0 & 0 \end{pmatrix}$$

5. Show that the matrix B of Ex. 4 has the property $B^3 = aI$ and that the matrix A has the property $A^3 = I$. Obtain similar results for the matrices of Ex. 3.

6. Compute BAB if

$$A = \begin{pmatrix} c & -d \\ \bar{d} & \bar{c} \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

where c and d are any ordinary complex numbers, $\bar{c}$ and $\bar{d}$ are their conjugates.

4. Elementary transformation matrices. We shall show that the matrix which is the result of the application of any elementary row (column) transformation to an m by n matrix A is a corresponding product EA (the product AE) where E is a uniquely determined square matrix. We might of course give a formula for each E and verify the statement, but it is simpler to describe E and to obtain our results by a device which is a consequence of the following

Theorem 5. *Let* A *be an* m *by* n *matrix,* B *be an* n *by* q *matrix so that* C = AB *is an* m *by* q *matrix. Apply an elementary row (column) transformation to* A (*to* B) *resulting in what we shall designate by* A_0(by $B^{(0)}$), *and then the same elementary transformation to* C *resulting in* C_0 (*in* $C^{(0)}$). *Then*

$$C_0 = A_0B, \qquad C^{(0)} = AB^{(0)}. \tag{18}$$

For proof we see that if we replace a_{ij} by a_{sj} in the right members of (4) we get c_{sk}. Thus we obtain the result of an elementary row transformation of type 1 on AB by applying it to A. Our definitions also imply that for elementary row transformations of type 3 the result stated as (18) follows from

$$\sum_{j=1}^{n} (aa_{ij})b_{jk} = a\sum_{j=1}^{n} a_{ij}b_{jk} = ac_{ik} \tag{19}$$

$$(i = 1, \ldots, m;\ k = 1, \ldots, q).$$

Finally, we see that for type 2 they follow from

$$(20)\qquad \sum_{j=1}^{n}(a_{ij}+ca_{sj})b_{jk}=\left(\sum_{j=1}^{n}a_{ij}b_{jk}\right)+c\left(\sum_{j=1}^{n}a_{sj}b_{jk}\right)=c_{ik}+cc_{sk}$$

$$(i=1,\ldots,n;\ k=1,\ldots,q),$$

and we have proved the first equation in (18). The corresponding column result $C^{(0)}=AB^{(0)}$ has an obvious parallel proof or may be thought of as being obtained by the process of transposition. It is surely unnecessary to supply further details.

We now write $A=IA$ where I is the m-rowed identity matrix and apply Theorem 5 to obtain $A_0=I_0A$, in which I_0 is the matrix called E above. Then we see that to apply any elementary row transformation to A we simply multiply A on the left by either E_{ij}, $P_{ij}(c)$, or $R_i(a)$. Here we define E_{ij} to be the matrix obtained by interchanging the ith and jth rows of I, $P_{ij}(c)$ by adding c times the jth row of I to its ith row, $R_i(a)$ by multiplying the ith row of I by $a\neq 0$. We shall call E_{ij}, $P_{ij}(c)$, and $R_i(a)$ *elementary transformation matrices* of types 1, 2, and 3, respectively.

Observe that

$$(21)\qquad E'_{ij}=E_{ji}=E_{ij},\qquad E_{ij}E_{ij}=I,$$

so that, if we now assume that E_{ij} is n-rowed, the product AE_{ij} is the result of an elementary column transformation of type 1 on A. Similarly,

$$(22)\qquad [P_{ij}(c)]'=P_{ji}(c),\qquad P_{ij}(-c)P_{ij}(c)=P_{ij}(c)P_{ij}(-c)=I,$$

and if $P_{ji}(c)$ is n-rowed, then $AP_{ji}(c)$ is the result of an elementary column transformation of type 2 on A. Finally,

$$(23)\qquad [R_i(a)]'=R_i(a),\qquad R_i(a^{-1})R_i(a)=R_i(a)R_i(a^{-1})=I,$$

and if $R_i(a)$ is n-rowed, then $AR_i(a)$ is the result of an elementary column transformation of type 3 on A. Thus the elementary column transformations give rise to exactly the same set of elementary transformation matrices as were obtained from the row transformations.

We shall now interpret the results of Section 2.7 in terms of elementary transformation matrices. First of all, we may interpret Theorem 2.2 as the following

LEMMA 1. *Let* A *and* B *be* m *by* n *matrices. Then there exist elementary transformation matrices* $P_1, \ldots, P_s, Q_1, \ldots, Q_t$ *such that*

$$B = (P_1 \ldots P_s)A(Q_1 \ldots Q_t)$$

if and only if A *and* B *have the same rank.*

Theorem 2.3 is the case of Lemma 1 where A is the n-rowed identity matrix, and consequently $B = P_1 \ldots P_s Q_1 \ldots Q_t$. Thus we obtain

LEMMA 2. *Every nonsingular matrix is a product of elementary transformation matrices.*

We shall close the results with an important consequence of Theorem 2.4.

Theorem 6. *The rank of a product of two matrices does not exceed the rank of either factor.*

For, by Theorem 2.4, if the rank of A is r, there exists a sequence of elementary transformations carrying A into an m by n matrix A_0 whose bottom $m - r$ rows are all zero. By Theorem 5, if we apply these transformations to $C = AB$, we obtain a rationally equivalent matrix $C_0 = A_0B$. Then the bottom $m - r$ rows of the m-rowed matrix C_0 are all zero, and the rank of C_0 is the rank of C and is at most r, as desired. The corresponding result on the relation between the ranks of C and B is obtained similarly.

EXERCISES

1. Express the following as products of elementary transformation matrices.

$$a) \begin{pmatrix} 7 & 3 \\ 2 & 1 \end{pmatrix} \qquad b) \begin{pmatrix} 1 & 1 & 1 \\ 2 & -6 & 1 \\ 3 & 4 & 2 \end{pmatrix} \qquad c) \begin{pmatrix} 6 & 4 & 3 \\ 1 & 2 & 3 \\ 1 & -2 & 1 \end{pmatrix}$$

2. Find the elementary transformation matrices corresponding to the elementary row transformations used in Ex. 2 of Section 2.6 and carry the matrices of that exercise into the form (2.30) by matrix multiplication.

5. The determinant of a product. In the theory of determinants it is shown that the symbol for the product of two determinants may be computed as the row by column product of the symbols for its factors. In our present terminology this result may be stated as

Theorem 7. *The determinant of a product of two square matrices is the product of the determinants of the factors, that is,*

$$|AB| = |A| \cdot |B| . \tag{24}$$

The usual proof in determinant theory of the result is quite complicated, and it is interesting to note that it is possible to derive the theorem as a

simple consequence of our theorems which were obtained independently and which we should have wished to derive even had Theorem 7 been assumed. We shall, therefore, give such a derivation. We thus let A and B be n-rowed square matrices and see that Theorem 6 states that if $|A| = 0$ then $|AB| = 0$. Hence, let A be nonsingular so that, by Lemma 2,

$$A = P_1 \dots P_s ,$$

where the P_i are elementary transformation matrices. From our definitions we see that, if E is an n-rowed elementary transformation matrix of type 1, 2, or 3, then $|E| = -1$, 1, or a, respectively. Thus, if G is an n-rowed square matrix and $G_0 = EG$, then Lemmas 2.3, 2.4, and 2.5 imply that $|G_0| = -|G|$, $|G|$, $a|G|$, respectively, and hence $|G_0| = |E| \cdot |G|$. It follows clearly that, if $E_1, \dots, E_t$ are any elementary transformation matrices, then $|E_t E_{t-1} \dots E_1 G| = |E_t| \dots |E_1| \cdot |G|$. We apply this result first to A to obtain $|A| = |P_1| \dots |P_s|$ and then to AB to obtain $|AB| = |P_1 \dots P_s B| = |P_1| \dots |P_s| \cdot |B| = |A| \cdot |B|$ as desired.

6. Nonsingular matrices. An n-rowed square matrix A is said to have an *inverse* if there exists a matrix B such that $AB = BA = I$ is the n-rowed identity matrix. Clearly, B is an n-rowed square matrix which we shall designate by A^{-1} and thus write

$$AA^{-1} = A^{-1}A = I . \tag{25}$$

Moreover, we have

Theorem 8. *A square matrix* A *has an inverse if and only if* A *is nonsingular.*

For if (25) holds, we apply Theorem 7 to obtain $|A| \cdot |A^{-1}| = |I| = 1$, $|A| \neq 0$. The converse may be shown to follow from (21), (22), (23), and Lemma 2; but we shall prove instead the result that if $|A| \neq 0$ then A^{-1} is uniquely determined as the matrix

$$A^{-1} = |A|^{-1} \cdot \operatorname{adj} A . \tag{26}$$

This formula follows from the matrix equation

$$A(\operatorname{adj} A) = (\operatorname{adj} A)A = |A| \cdot I \tag{27}$$

by multiplication by the scalar $|A|^{-1}$, and we observe that (27) is the interpretation of (2.20) and (2.21) in terms of matrix product, where adj A is our symbol for the adjoint matrix defined in (2.22).

We now prove A^{-1} unique by showing that if either $AB = I$ or $BA = I$ then B is necessarily the matrix A^{-1} of (26). This is clear since in either case $|A| \neq 0$, A^{-1} of (26) exists, $A^{-1} = A^{-1}I = A^{-1}(AB) = (A^{-1}A)B = IB = B$, and similarly if $BA = I$.

We note also that, if A and B are nonsingular,

$$(AB)^{-1} = B^{-1}A^{-1}. \tag{28}$$

For $(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AA^{-1} = I$. Finally, if A is nonsingular we have

$$(A^{-1})' = (A')^{-1}. \tag{29}$$

For $I' = I = (AA^{-1})' = (A^{-1})'A'$, $(A^{-1})'$ is the inverse of A'.

A linear mapping (1) with $m = n$ has an *inverse* mapping (2) with $n = q$ if the product (3) is the identical mapping, that is, if $C = AB$ is the identity matrix. But this is then possible if and only if $|A| \neq 0$, that is, (1) is what we called a nonsingular linear mapping in Section 1.9. We shall use this concept later in studying the equivalence of forms.

EXERCISES

1. Show that if A is an n-rowed square matrix of rank $n - 1 \neq 0$, then adj A has rank 1. Hint: By (27) we have $|A| = 0$, $PAQ(Q^{-1} \cdot \text{adj } A) = 0$ for

$$PAQ = \begin{pmatrix} I_{n-1} & 0 \\ 0 & 0 \end{pmatrix}.$$

Then the first $n - 1$ rows of $Q^{-1} \cdot$ adj A must be zero, adj A has rank 1.

2. Use the result above and (28) to prove that adj (adj A) $= |A|^{n-2}A$ if $n > 2$ and adj (adj A) $= A$ if $n = 2$ and $|A| \neq 0$.

3. Use Ex. 1 and (27) to show that $|\text{adj } A| = |A|^{n-1}$.

4. Compute the inverses of the following matrices by the use of (26).

a) $\begin{pmatrix} b & bc-1 \\ 1 & c \end{pmatrix}$ b) $\begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ c) $\begin{pmatrix} 3 & -2 & 0 \\ 0 & 3 & -2 \\ -2 & 0 & 3 \end{pmatrix}$

d) $\begin{pmatrix} 2 & 3 & 4 \\ 1 & 2 & 6 \\ 0 & 0 & 1 \end{pmatrix}$ e) $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 3 & 6 \end{pmatrix}$ f) $\begin{pmatrix} 1 & -1 & 0 & 2 \\ 0 & 1 & 1 & -1 \\ 2 & 1 & 2 & 1 \\ 3 & -2 & 1 & 6 \end{pmatrix}$

g) $\begin{pmatrix} 2 & -1 & 1 & 6 \\ 0 & 1 & 2 & 1 \\ -1 & 1 & 1 & -2 \\ 1 & 0 & 2 & 3 \end{pmatrix}$ h) $\begin{pmatrix} 2 & -5 & 2 & -3 \\ -1 & -3 & 3 & -1 \\ 1 & 1 & -1 & 0 \\ -1 & 1 & 0 & 1 \end{pmatrix}$

5. Let A be the matrix of (d) above and B be the matrix of (e). Compute $C = (AB)^{-1}$ by (28) and verify that $(AB)C = I$ by direct multiplication.

7. Equivalence of rectangular matrices. Our considerations thus far have been devised as relatively simple steps toward a goal which we may now attain. We first make the

DEFINITION. *Two* m *by* n *matrices* A *and* B *are called* ***equivalent*** *if there exist nonsingular matrices* P *and* Q *such that*

$$PAQ = B. \tag{30}$$

Observe that P and Q are necessarily square matrices of m and n rows, respectively. By Lemma 2 both P and Q are products of elementary transformation matrices and therefore A *and* B *are equivalent if and only if* A *and* B *are rationally equivalent.* The reader should notice that the definition of rational equivalence is to be regarded here as simply another form of the definition of equivalence given above and, while the previous definition is more useful for proofs, that above is the one which has always been given in previous expositions of matrix theory. We may now apply Lemma 1 and have the principal result of the present chapter.

Theorem 9. *Two* m *by* n *matrices are equivalent if and only if they have the same rank.*

We emphasize in closing that, if A and B are equivalent, the proof of Theorem 2.2 shows that the elements of P and Q in (30) may be taken to be rational functions, with rational coefficients, of the elements of A and B.

EXERCISES

1. Compute matrices P and Q for each of the matrices A of Ex. 1 of Section 2.6 such that PAQ has the form (2.30). Hint: If A is m by n, we may obtain P by applying those elementary row transformations used in that exercise to I_m and similarly for Q. (The details of an instance of this method are given in the illustrative example at the end of Section 8.)

2. Show that the product AB of any three-rowed square matrices A and B of rank 2 is not zero. Hint: There exist matrices P and Q such that $A_0 = PAQ$ has the form (2.30) for $r = 2$. Then, if $AB = 0$, we have $A_0B_0 = 0$ where $B_0 = Q^{-1}B$ has the same rank as B and may be shown to have two rows with elements all zero.

3. Compute the ranks of A, B, AB for the following matrices. Hint: Carry A into a simpler matrix $A_0 = PA$ by row transformations alone, B into $B_0 = BQ$ by

column transformations alone, and thus compute the rank of $A_0B_0 = P(AB)Q$ instead of that of AB.

$$a)\ A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 1 & 3 & 5 \end{pmatrix}, \qquad B = \begin{pmatrix} 3 & 4 & 5 \\ 0 & 2 & 4 \\ -1 & 1 & 3 \end{pmatrix}$$

$$b)\ A = \begin{pmatrix} -1 & 2 & 0 \\ 1 & 1 & 0 \\ -4 & 5 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 3 & 2 \\ 2 & 6 & 4 \\ -1 & -4 & 1 \end{pmatrix}$$

$$c)\ A = \begin{pmatrix} 3 & -5 & 2 & 4 \\ 1 & -2 & 1 & 3 \\ 1 & -1 & 0 & -2 \\ 5 & -8 & 3 & 5 \end{pmatrix}, \qquad B = \begin{pmatrix} -4 & 10 & 2 & 6 \\ -2 & 6 & 2 & 4 \\ 3 & -4 & 2 & -1 \\ -1 & 2 & 0 & 1 \end{pmatrix}$$

8. Bilinear forms. As we indicated at the close of Chapter I, the problem of determining the conditions for the equivalence of two forms of the same restricted type is customarily modified by the imposition of corresponding restrictions on the linear mappings which are allowed. We now precede the introduction of those restrictions which are made for the case of bilinear forms by the presentation of certain notations which will simplify our discussion.

The one-rowed matrices

$$x' = (x_1, \ldots, x_m), \qquad y' = (y_1, \ldots, y_n) \tag{31}$$

have one-columned matrices x and y as their respective transposes. We let A be the m by n matrix of the system of equations (1) and see that this system may be expressed as either of the matrix equations

$$x = Ay, \qquad x' = y'A'. \tag{32}$$

We have called (1) a nonsingular linear mapping if $m = n$ and A is nonsingular. But then the solution of (1) for $y_1, \ldots, y_n$ as linear forms in $x_1, \ldots, x_n$ is the solution

$$y = A^{-1}x, \qquad y' = x'(A')^{-1} = x'(A^{-1})' \tag{33}$$

of (32) for y in terms of x (or y' in terms of x'). We shall again consider m by n matrices A and variables x_i and y_j and shall now introduce the notation

$$x = P'u \tag{34}$$

for a nonsingular linear mapping carrying the x_i to new variables u_k, for $i, k = 1, \ldots, m$, so that the transpose P of P' is a nonsingular m-rowed square matrix and $u' = (u_1, \ldots, u_m)$. Similarly, we write

$$y = Qv \tag{35}$$

for a nonsingular n-rowed square matrix Q and $v' = (v_1, \ldots, v_n)$. We now return to the study of bilinear forms.

A bilinear form $f = \Sigma x_i a_{ij} y_j$, for $i = 1, \ldots, m$ and $j = 1, \ldots, n$, is a scalar which may be regarded as a one-rowed square matrix and is then the matrix product

$$f = x'Ay\,. \tag{36}$$

Here x and y are given by (31), and we call the m by n matrix A *the matrix* of f, its rank *the rank* of f. Also let $g = x'By$ be a bilinear form in $x_1, \ldots, x_m$ and $y_1, \ldots, y_n$ with m by n matrix B. Then we shall say that f and g are *equivalent* if there exist nonsingular linear mappings (34) and (35) such that the matrix of the form in $u_1, \ldots, u_m$ and $v_1, \ldots, v_n$ into which f is carried by these mappings is B. But if (34) holds, then $x' = u'P$ and

$$f = (u'P)A(Qv) = u'(PAQ)v\,,$$

so that $B = PAQ$ and A are equivalent. Thus, *two bilinear forms* f *and* g *are equivalent if and only if their matrices are equivalent.* By Theorem 9 we see that *two bilinear forms are equivalent if and only if they have the same rank.* It follows also that every bilinear form of rank r is equivalent to the form

$$x_1y_1 + \ldots + x_ry_r\,. \tag{37}$$

These results complete the study of the equivalence of bilinear forms.

ILLUSTRATIVE EXAMPLE

We shall find nonsingular linear mappings (34) and (35) which carry the form

$$f = 2x_1y_1 - 3x_1y_2 + x_1y_3 - x_2y_1 + 5x_2y_3 - 6x_3y_1 + 3x_3y_2 + 19x_3y_3$$

into a form of the type (37). The matrix of f is

$$A = \begin{pmatrix} 2 & -3 & 1 \\ -1 & 0 & 5 \\ -6 & 3 & 19 \end{pmatrix}.$$

We interchange the first and second rows of A, add twice the new first row to the new second row, add -6 times the new first row to the third row, and obtain

$$\begin{pmatrix} -1 & 0 & 5 \\ 0 & -3 & 11 \\ 0 & 3 & -11 \end{pmatrix},$$

which evidently has rank 2. We then add the second row to the third row, multiply the first row by -1, the second row by $-\frac{1}{3}$, and obtain

$$PA = \begin{pmatrix} 1 & 0 & -5 \\ 0 & 1 & -\frac{11}{3} \\ 0 & 0 & 0 \end{pmatrix}.$$

The matrix P is obtained by performing the transformations above on the three-rowed identity matrix, and hence

$$P = \begin{pmatrix} 0 & -1 & 0 \\ -\frac{1}{3} & -\frac{2}{3} & 0 \\ 1 & -4 & 1 \end{pmatrix}.$$

We continue and carry PA into PAQ of the form (2.30) for $r = 2$ by adding five times the first column and $\frac{11}{3}$ times the second column of PA to its third column. Then

$$Q = \begin{pmatrix} 1 & 0 & 5 \\ 0 & 1 & \frac{11}{3} \\ 0 & 0 & 1 \end{pmatrix}.$$

The corresponding linear mappings (34) and (35) are given respectively by

$$\begin{cases} x_1 = -\frac{1}{3}u_2 + u_3 \\ x_2 = -u_1 - \frac{2}{3}u_2 - 4u_3 \\ x_3 = u_3 \end{cases}, \qquad \begin{cases} y_1 = v_1 + 5v_3 \\ y_2 = v_2 + \frac{11}{3}v_3 \\ y_3 = v_3 \end{cases}.$$

We verify by direct substitution that

$$\begin{aligned} f &= (-\tfrac{1}{3}u_2 + u_3)(2v_1 + 10v_3 - 3v_2 - 11v_3 + v_3) \\ &\quad + (u_1 + \tfrac{2}{3}u_2 + 4u_3)(v_1 + 5v_3 - 5v_3) \\ &\quad + u_3(-6v_1 - 30v_3 + 3v_2 + 11v_3 + 19v_3) \\ &= -\tfrac{2}{3}u_2v_1 + u_3v_2 + 2u_3v_1 - 3u_3v_2 + u_1v_1 + \tfrac{2}{3}u_2v_1 + 4u_3v_1 - 6u_3v_1 + 3u_3v_2 \\ &= u_1v_1 + u_2v_2, \end{aligned}$$

as desired.

EXERCISES

1. Use the method above to find nonsingular linear mappings which carry the following bilinear forms into forms of the type (37).

a) $2x_1y_1 + 3x_1y_2 - x_2y_1 - 2x_2y_2$

b) $x_1y_1 - x_1y_2 + x_1y_3 + 4x_2y_1 - 3x_2y_2 + 2x_2y_3 - x_3y_1 + 2x_3y_2 - 3x_3y_3$

c) $2x_1y_1 + 3x_1y_2 - x_1y_3 + 5x_2y_1 + 2x_2y_2 + x_2y_3 + 3x_3y_1 - x_3y_2 + 2x_3y_3$

d) $2x_1y_1 - x_1y_2 + 3x_1y_3 + x_1y_4 - 2x_2y_1 + 3x_2y_2 - 13x_2y_3 + 5x_2y_4 + x_3y_1 - x_3y_3 + 2x_3y_4 + 4x_4y_1 - x_4y_2 + x_4y_3 + 5x_4y_4$

2. Use the method above to find a nonsingular linear mapping on x_1, x_2, x_3 such that it and the identity mapping on y_1, y_2, y_3 carry the following forms into forms of the type (37).

a) $-3x_1y_1 + 5x_1y_2 + x_2y_1 - 2x_2y_2$

b) $3x_1y_1 + x_1y_2 + 4x_2y_1 + 2x_2y_2$

c) $x_1y_1 - 4x_1y_2 + x_1y_3 - x_2y_1 + x_2y_2 + 2x_3y_2 - x_3y_3$

d) $3x_1y_2 + 5x_1y_3 + x_2y_2 + 2x_2y_3 + x_3y_1 - 2x_3y_2 + x_3y_3$

e) $-x_1y_2 + x_1y_3 + x_1y_4 + x_2y_2 + 2x_2y_3 - 3x_2y_4 + x_3y_1 - 2x_3y_2 + 3x_3y_3 + 4x_3y_4 + 2x_4y_2 - x_4y_3 - 3x_4y_4$

3. Find a nonsingular linear mapping on y_1, y_2, y_3 such that it and the identical mapping on x_1, x_2, x_3 carry the forms of Ex. 2 into forms of the type (37). Hint: The matrices A of the forms of Ex. 2 are nonsingular so that the corresponding matrices P have the property $PA = I$. Then $P = A^{-1}$, $AQ = I$ has the unique solution $Q = P$.

4. Use elementary row transformations as above to compute the inverses of the matrices of Section 6, Ex. 4.

5. Use elementary column transformations to compute the inverses of the following matrices.

a) $\begin{pmatrix} -1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 3 & 2 & 5 \\ -1 & 0 & -1 & -2 \end{pmatrix}$ b) $\begin{pmatrix} -2 & 1 & 0 & 1 \\ 1 & 0 & 2 & -1 \\ -4 & 1 & -3 & 1 \\ -1 & 0 & -2 & 2 \end{pmatrix}$

c) $\begin{pmatrix} 0 & -4 & 1 & -1 \\ -1 & 3 & 0 & 1 \\ 2 & -3 & 0 & 0 \\ 1 & 3 & -1 & 1 \end{pmatrix}$ d) $\begin{pmatrix} -3 & -1 & 0 & 1 \\ 1 & 2 & -1 & 0 \\ -4 & -2 & 1 & 1 \\ 3 & 0 & 1 & -1 \end{pmatrix}$

9. Congruence of square matrices. There are some important problems regarding special types of bilinear forms as well as the theory of equivalence of quadratic forms which arise when we restrict the linear mappings we use. We let $m = n$ so that the matrices A of forms $f = x'Ay$ are square matrices. Then (34) and (35) are called *cogredient* mappings if $Q = P'$. Then f and g are clearly equivalent under cogredient mappings if and only if

$$B = PAP'. \tag{38}$$

We shall call A and B *congruent* if there exists a nonsingular matrix P satisfying (38).

We shall not study the complicated question as to the conditions that two arbitrary square matrices be congruent but shall restrict our attention to two special cases.

Before passing to this study we observe that Lemma 2 and Section 7 imply that A and B are congruent if and only if A may be carried into B by a sequence of operations each of which consists of an elementary row transformation followed by the corresponding column transformation. Thus $P = P_s \dots P_1$, where the P_k are elementary transformation matrices, $B = P_s \dots P_1 A P_1' \dots P_s' = P_s \dots P_2(P_1 A P_1')P_2' \dots P_s'$, and so forth as desired. We shall speak of such operations on a matrix A as *cogredient elementary transformations* of the three types and shall use them in our study of the congruence of matrices.

10. Skew matrices and skew bilinear forms. A square matrix A is called *symmetric* if $A' = A$, and *skew* if $A' = -A$. If $B = PAP'$ is congruent to A then $B' = PA'P'$, B is symmetric if and only if A is symmetric, B is skew if and only if A is skew.

If $A = (a_{ij})$ is a skew matrix, then $a_{ji} = -a_{ij}$ for all i and j. Hence $a_{ii} = -a_{ii}$ and consequently every diagonal element of A is zero. We use this result in the proof of

Theorem 10. *Two* n*-rowed skew matrices are congruent if and only if they the same rank* r. *Moreover* r *is an even integer* 2t, *and every skew matrix is thus congruent to a matrix*

$$\begin{pmatrix} 0 & -I_t & 0 \\ I_t & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}. \tag{39}$$

For either $A = 0 = PAP'$ for every P and our result is trivial, or some $a_{ij} \neq 0$. We may interchange the ith row and first row, the jth and second row and thus also the corresponding columns by cogredient elementary transformations of type 1. We thus obtain a skew matrix $H = (h_{ij})$ congruent to A and with $a_{ij} = h_{12} \neq 0$, $h_{21} = -h_{12}$, $h_{11} = h_{22} = 0$. Multiply the first row and column of H by h_{21}^{-1} and obtain a skew matrix $C = (c_{ij})$ congruent to A and with $c_{12} = -1$, $c_{21} = 1$, $c_{11} = c_{22} = 0$. We now apply a sequence of cogredient elementary transformations of type 2 where we add $-c_{j1}$ times the second row of C to its jth row as well as c_{j2} times the first row of C to its jth row for $j = 3, \dots, n$, and thus obtain the skew matrix

$$A_0 = \begin{pmatrix} E & 0 \\ 0 & A_1 \end{pmatrix}, \qquad E = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{40}$$

The matrix A_0 is congruent to A, A_1 is necessarily a skew matrix of $n-2$ rows, and any cogredient elementary transformation on the last $n-2$ rows and columns of A_0 induces corresponding transformations on A_1, carrying it to a congruent skew matrix H_1 and carrying A_0 to a congruent skew matrix

$$\begin{pmatrix} E & 0 \\ 0 & H_1 \end{pmatrix}.$$

It follows that, after a finite number of such steps, we may replace A by a congruent skew matrix

$$G = \operatorname{diag}\{E_1, \ldots, E_t, 0, \ldots, 0\} \tag{41}$$

with each $E_k = E$. Clearly, G and A have rank $2t$. If B also is a skew matrix of rank $2t$, then B is congruent to (41) and to A, both A and B are congruent to (39).

If A is a skew matrix, the corresponding bilinear form $x'Ay$ is a *skew bilinear form*. Hence, two such forms are equivalent under cogredient nonsingular linear mappings if and only if they have the same rank. Moreover, if f is a skew bilinear form of rank $2t$ it is equivalent under cogredient nonsingular linear mappings to $(x_1y_2 - x_2y_1) + \ldots + (x_{2t-1}y_{2t} - x_{2t}y_{2t-1})$.

EXERCISES

Use a method analogous to that of the exercises of Section 8 to find cogredient linear mappings carrying the following skew forms to forms of the type above.

a) $x_1y_2 - x_2y_1 + 2x_1y_3 - 2x_3y_1 + 3x_2y_3 - 3x_3y_2$

b) $2x_2y_1 - 2x_1y_2 - x_1y_3 + x_3y_1 + 2x_2y_3 - 2x_3y_2$

c) $x_1y_2 - x_2y_1 + 3x_1y_3 - 3x_3y_1 - 4x_4y_1 + 4x_1y_4 + 4x_2y_3 - 4x_3y_2 + 8x_2y_4 - 8x_4y_2 + 8x_3y_4 - 8x_4y_3$

11. Symmetric matrices and quadratic forms. The theory of symmetric matrices is considerably more extensive and complicated than that of skew matrices, and we shall obtain only some of its most elementary results. Our principal conclusion may be stated as

Theorem 11. *Every symmetric matrix* A *is congruent to a diagonal matrix of the same rank as* A.

We may evidently assume that $A = A' \neq 0$, and we shall prove first that A is congruent to a symmetric matrix $H = (h_{ij})$ with some diagonal element $h_{ii} \neq 0$. This is true for $A = H$ if some diagonal element of A is not zero. Otherwise there is some $a_{ij} \neq 0$, $a_{ji} = a_{ij}$, and $a_{ii} = a_{jj} = 0$. We then obtain H as the result of adding the jth row of A to its ith row and

the jth column of A to its ith column, $h_{ii} = a_{jj} + a_{ij} + a_{ij} = 2a_{ij} \neq 0$ as desired. We now permute the rows and corresponding columns of H to obtain a congruent symmetric matrix C with $c_{11} = h_{ii} \neq 0$. Then we add $-c_{11}^{-1}c_{k1}$ times the first row to its kth row, follow with the corresponding column transformation, and obtain a symmetric matrix

$$\begin{pmatrix} c_{11} & 0 \\ 0 & A_1 \end{pmatrix} \tag{42}$$

congruent to A. Clearly, A_1 is a symmetric matrix with $n-1$ rows. As in the proof of Theorem 10 we carry out a finite number of such steps, and it is clear that we ultimately obtain a diagonal matrix. It is a matrix equivalent to A and must have the same rank.

The result above may be applied to obtain a corresponding result on *symmetric bilinear forms* of rank r, that is, bilinear forms $f = x'Ay$ defined by a symmetric matrix A of rank r. Theorem 11 then states that f is equivalent under cogredient transformations to a form

$$a_1x_1y_1 + \ldots + a_rx_ry_r\,. \tag{43}$$

The results of Theorem 11 may also be applied to quadratic forms $f = f(x_1, \ldots, x_n)$. As we saw in Section 1.7, f is the one-rowed square matrix product

$$f = x'Ax = \sum_{i,j=1}^{n} x_i a_{ij} x_j \tag{44}$$

for a symmetric matrix A. We call the uniquely determined symmetric matrix A the *matrix of* f and its rank *the rank of* f. Now in Section 1.9 we defined the equivalence of any quadratic form f and any second quadratic form $g = y'By$. We may then use the notations developed above and see that f and g are equivalent if and only if A and B are congruent. For if our nonsingular linear mapping is represented by the matrix equation $x = P'u$, then $x' = u'P$ is a consequence, and $f = u'(PAP')u$, f and g are equivalent if and only if $B = PAP'$. Thus Theorem 11 states that every quadratic form of rank r is equivalent to

$$a_1x_1^2 + \ldots + a_rx_r^2\,. \tag{45}$$

The form (45) is of course to be regarded as a form in $x_1, \ldots, x_n$ with matrix diag $\{a_1, \ldots, a_r, 0, \ldots, 0\}$. However, it may be regarded as a form in $x_1, \ldots, x_r$ with nonsingular matrix diag $\{a_1, \ldots, a_r\}$. We shall

call a quadratic form $f = x'Ax$ in $x_1, \ldots, x_n$ with nonsingular matrix A a *nonsingular form*, and we have shown that *every quadratic form of rank* r *in* n *variables may be written as a nonsingular form in* r *variables whose matrix is a diagonal matrix.*

EXERCISES

1. What is the symmetric matrix A of the following quadratic forms?

a) $3x_1^2 + x_1x_2 + 2x_1x_3 - 3x_2x_4 + x_4^2$

b) $2x_1x_2 - 3x_3x_4 + x_2^2$

c) $x_1^2 - 3x_1x_2 + 2x_1x_4 - 3x_1^2$

2. Find a nonsingular matrix P with rational elements for each of the following matrices A such that PAP' is a diagonal matrix. Determine P by writing $A = IAI'$ and by applying cogredient elementary transformations.

a) $\begin{pmatrix} 6 & 1 & -1 \\ 1 & 14 & -3 \\ -1 & -3 & 1 \end{pmatrix}$ *b)* $\begin{pmatrix} 2 & 4 & 1 \\ 4 & 9 & 4 \\ 1 & 4 & 6 \end{pmatrix}$

c) $\begin{pmatrix} 4 & -1 & 5 \\ -1 & -1 & 2 \\ 5 & 2 & -2 \end{pmatrix}$ *d)* $\begin{pmatrix} 10 & -3 & 3 \\ -3 & 1 & -1 \\ 3 & -1 & 1 \end{pmatrix}$

e) $\begin{pmatrix} 0 & 0 & 2 & 3 \\ 0 & 0 & -2 & -3 \\ 2 & -2 & 0 & -1 \\ 3 & -3 & -1 & -3 \end{pmatrix}$ *f)* $\begin{pmatrix} 7 & 6 & 0 & -1 \\ 6 & 15 & 0 & 1 \\ 0 & 0 & 2 & 3 \\ -1 & 1 & 3 & 5 \end{pmatrix}$

g) $\begin{pmatrix} -3 & -4 & 1 & 0 \\ -4 & -5 & 0 & -5 \\ 1 & 0 & 1 & 1 \\ 0 & -5 & 1 & 14 \end{pmatrix}$ *h)* $\begin{pmatrix} 3 & 2 & 1 & -1 \\ 2 & 2 & 1 & -1 \\ 1 & 1 & 1 & 0 \\ -1 & -1 & 0 & 0 \end{pmatrix}$

3. Write the symmetric bilinear forms whose matrices are those of (*a*), (*b*), (*c*), and (*d*) of Ex. 2 and use the cogredient linear mappings obtained from that exercise to obtain equivalent forms with diagonal matrices.

4. Apply the process of Ex. 3 to (*e*), (*f*), (*g*), and (*h*) of Ex. 2 for quadratic forms.

5. Which of the matrices of Ex. 2 are congruent if we allow any complex numbers as elements of P?

6. Show that the forms $f = x_1^2 + x_2^2$ and $g = x_1^2 - x_2^2$ are not equivalent under linear mappings with real coefficients. Hint: Consider the possible signs of *values* of f and of g.

12. Nonmodular fields. In our discussion of the congruence and the equivalence of two matrices A and B the elements of the transformation matrices P and Q have thus far always been rational functions, with rational coefficients, of the elements of A and B. While we have mentioned this fact before, it has not, until now, been necessary to emphasize it. But the reader will observe that we have not, as yet, given conditions that two symmetric matrices be congruent, and our reason is that it is not possible to do so without some statement as to the nature of the quantities which we allow as elements of the transformation matrices P. We shall thus introduce an algebraic concept which is one of the most fundamental concepts of our subject—the concept of a field.

A field of complex numbers is a set F of at least two distinct complex numbers $a, b, \ldots$, such that $a + b$, ab, $a - b$, and a/c are in F for every $a, b, c \neq 0$ in F. Examples of such fields are, then, the set of all real numbers, the set of all complex numbers, and the set of all rational functions with rational coefficients of any fixed complex number c.

If F is any field of complex numbers, the set $K = F(x)$ of all rational functions in x with coefficients in F is a mathematical system having properties, with respect to rational operations, just like those of F. Now it is true that even if one were interested only in the study of matrices whose elements are ordinary complex numbers there would be a stage of this study where one would be forced to consider also matrices whose elements are rational functions of x. Thus we shall find it desirable to define the concept of a field in such a general way as to include systems like the field K defined above. We shall do so and *shall assume henceforth that what we called constants in Chapter I and scalars thereafter are elements of a fixed field* F.

The fields we have already mentioned all contain the complex number unity and are closed with respect to rational operations. But it is clearly possible to obtain every rational number by the application to unity of a finite number of rational operations. Thus all our fields contain the field of all rational numbers and are what are called *nonmodular fields*. The fields called *modular fields* will be defined in Chapter VI. We now make the following brief

DEFINITION. *A set of elements* F *is said to form a nonmodular field if* F *contains the set of all rational numbers and is closed with respect to rational operations such that the following properties hold*:

$$\text{I. } (a + b) + c = a + (b + c), \qquad (ab)c = a(bc);$$

$$\text{II. } a(b + c) = ab + ac;$$

$$\text{III. } a + b = b + a, \qquad ab = ba$$

for every a, b, c *of* F.

The difference $a - b$ is always defined in elementary algebra to be a solution x in F of the equation

$$x + b = a, \tag{46}$$

and the quotient a/b to be a solution y in F of the equation*

$$yb = a. \tag{47}$$

Thus our hypothesis that F is closed with respect to rational operations should be interpreted to mean that any two elements a and b of F determine a unique sum $a + b$ and a unique product ab in F such that (46) has a solution in F and (47) has a solution in F if $b \neq 0$. In the author's *Modern Higher Algebra* it is shown that the solutions of (46) and (47) are unique. In fact, it may be concluded that the rational numbers 0 and 1 have the properties

$$a + 0 = a1 = a, \qquad a0 = 0, \tag{48}$$

for every a of F and that there exists a unique solution $x = -a$ of $x + a = 0$ and a unique solution $y = b^{-1}$ of $yb = 1$ for $b \neq 0$. Then the solutions of (46) and (47) are uniquely determined by $x = a + (-b)$, $y = ab^{-1}$.

We also see that the rational number -1 is defined so that $(-1) + 1 = 0$, and thus $(-1 + 1)a = 0 \cdot a = 0$, whereas $(-1 + 1)a = -1 \cdot a + 1 \cdot a = -1 \cdot a + a$. Hence $-a = -1 \cdot a$. It is also true that $-(-a) = a$, $(-a)(-b) = ab$ for every a and b of a field F.

EXERCISES

1. Let a, b, and c range over the set of all rational numbers and F consist of all matrices of the following types. Prove that F is a field. (Use the definition of addition of matrices in (52).)

a) $\begin{pmatrix} a & -2b \\ b & a \end{pmatrix}$ b) $\begin{pmatrix} a+b & 4b \\ -b & a-b \end{pmatrix}$ c) $\begin{pmatrix} a & b & c \\ 2c & a & b \\ 2b & 2c & a \end{pmatrix}$

2. Show that if a, b, c, and d range over all rational numbers and $i^2 = -1$, the set of all matrices of the following kind form a quasi-field which is not a field.

$$\begin{pmatrix} a + bi & 3(c + di) \\ c - di & a - bi \end{pmatrix}.$$

* Note that in view of III the property II implies that $(b + c)a = ba + ca$, and the existence of a solution of (46) is equivalent to that of $b + x = a$, of (47) to that of $by = a$. But there are mathematical systems called *quasi-fields* in which the law $ab = ba$ does not hold, and for these systems the properties just mentioned must be made as additional assumptions.

13. Summary of results. The theory completed thus far on polynomials with constant coefficients and matrices with scalar elements may now be clarified by restating our principal results in terms of the concept of a field. We observe first that if $f(x)$ and $g(x)$ are nonzero polynomials in x with coefficients in a field F then they have a greatest common divisor $d(x)$ with coefficients in F, and $d(x) = a(x)f(x) + b(x)g(x)$ for polynomials $a(x)$, $b(x)$ with coefficients in F.

We next assume that A and B are two m by n matrices with elements in a field F and say that A and B are equivalent in F if there exist nonsingular matrices P and Q with elements in F such that $PAQ = B$. Then A and B are equivalent in F if and only if they have the same rank. Moreover, correspondingly, two bilinear forms with coefficients in F are equivalent in F if and only if they have the same rank. Since the rank of a matrix (and of a corresponding bilinear form) is defined without reference to the nature of the field F containing its elements, the particular F chosen to contain the elements of the matrices is relatively unimportant for the theory.

If A and B are square matrices with elements in a field F, then we call A and B congruent in F if there exists a nonsingular matrix P with elements in F such that $PAP' = B$. Similarly, we say that the bilinear forms $x'Ay$ and $x'By$ are equivalent in F under cogredient transformations* if A and B are congruent in F. When $A' = -A$ the matrix A is skew, and every matrix B congruent in F to A is skew, two skew matrices with elements in F are congruent in F if and only if they have the same rank. Hence, the precise nature of F is again unimportant.

Let $A = A'$ be a symmetric matrix with elements in F so that any matrix B congruent in F to A also is a symmetric matrix with elements in F. Then two corresponding quadratic forms $x'Ax$ and $x'Bx$ are equivalent in F if and only if A and B are congruent in F. Moreover, we have shown that every symmetric matrix of rank r and elements in F is congruent in F to a diagonal matrix diag $\{a_1, \ldots, a_r, 0, \ldots, 0\}$ with $a_i \neq 0$ in F and that correspondingly every quadratic form $x'Ax$ is equivalent in F to $a_1x_1^2 + \ldots + a_rx_r^2$.

The problem of finding necessary and sufficient conditions for two quadratic forms with coefficients in a field F to be equivalent in F is one involving the nature of F in a fundamental way, and no simple solution of this problem exists for F an arbitrary field. In fact, we can obtain results only after rather complete specialization of F, and these results may be seen to *vary* as we change our assumptions on F.

* We leave to the reader the explicit formulation of the definitions of equivalence in F of two forms, of two bilinear forms, and of two bilinear forms under cogredient linear mappings, where all the forms considered have elements in F.

The simplest conditions are those given in

Theorem 12. *Let* F *be a field with the property that for every* a *of* F *there exists a quantity* b *such that* $b^2 = a$. *Then two symmetric matrices with elements in* F *are congruent in* F *if and only if they have the same rank.*

For every $A = A'$ of rank r is congruent to $A_0 = \text{diag}\ \{a_1, \ldots, a_r, 0, \ldots, 0\}$ for $a_i \neq 0$ and $a_i = b_i^2$ for $b_i \neq 0$ in F. Then if $P = \text{diag}\ \{b_1^{-1}, \ldots, b_r^{-1}, 0, \ldots, 0\}$, $PA_0P' = \text{diag}\ \{I_r, 0\}$. If also $B = B'$ has rank r, then B is also congruent in F to diag $\{I_r, 0\}$ and hence to A. The converse follows from Theorem 2.2.

We then have the obvious consequences.

COROLLARY I. *Two symmetric matrices whose elements are complex numbers are congruent in the field of all complex numbers if and only if they have the same rank.*

COROLLARY II. *Let* F *be the field of either Theorem 12 or Corollary I. Then two quadratic forms with coefficients in* F *are equivalent in* F *if and only if they have the same rank. Hence every such form of rank* r *is equivalent in* F *to*

$$x_1^2 + \ldots + x_r^2. \tag{49}$$

14. Addition of matrices. There is one other result on symmetric matrices over an arbitrary field which will be seen to have evident interest when we state it. Its proof involves the computation of the product of two matrices

$$A = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}, \qquad B = \begin{pmatrix} B_1 & B_2 \\ B_3 & B_4 \end{pmatrix}, \tag{50}$$

which have been partitioned into two-rowed square matrices whose elements are rectangular matrices. If these matrices were one-rowed square matrices, that is to say in F, we should have the formula

$$AB = \begin{pmatrix} A_1B_1 + A_2B_3 & A_1B_2 + A_2B_4 \\ A_3B_1 + A_4B_3 & A_3B_2 + A_4B_4 \end{pmatrix}. \tag{51}$$

But it is also true that if the partitioning of any A and B is carried out so that the products in (51) have meaning and if we define the sum of two matrices appropriately, then (51) will still hold. Thus (51) will have major importance as a formula for representing matrix computations.

We now let $A = (a_{ij})$ and $B = (b_{ij})$, where $i = 1, \ldots, m$ and $j = 1, \ldots, n$, so that A and B are m by n matrices. Then we define

$$S = A + B = (s_{ij}), \qquad s_{ij} = a_{ij} + b_{ij} \quad (i = 1, \ldots, m; j = 1, \ldots, n). \tag{52}$$

We have thus defined *addition* for any two matrices of the same shape such that $A + B$ is the matrix whose elements are the sums of correspondingly placed elements in A and B.

The elements of our matrices are in a field F, and $a_{ij} + b_{ij} = b_{ij} + a_{ij}$. If $C = (c_{ij})$ is also an m by n matrix, we have $(a_{ij} + b_{ij}) + c_{ij} = a_{ij} + (b_{ij} + c_{ij})$. Hence we have the properties

$$A + B = B + A\,, \qquad (A + B) + C = A + (B + C)\,. \tag{53}$$

We observe also that if 0 is the m by n zero matrix, then $A + 0 = A$, $A + (-1 \cdot A) = 0$.

Now let $C = (c_{jk})$ be any n by q matrix. Then

$$(A + B)C = AC + BC\,. \tag{54}$$

For this equation is clearly a consequence of the corresponding property of F, that is, of

$$(a_{ij} + b_{ij})c_{jk} = a_{ij}c_{jk} + b_{ij}c_{jk}\,. \tag{55}$$

We have thus seen that addition of matrices has the properties (53) always assumed for addition of the elements of our matrices and that the law (54), which we call the *distributive law for matrix addition and multiplication*, also holds. Clearly if D is a matrix such that DA is defined, then similarly we have

$$D(A + B) = DA + DB\,. \tag{56}$$

Observe, however, that if $n > 1$ and A and B are n-rowed square matrices, then $|A + B|$ and $|A| + |B|$ are usually not equal. For example, if A and B are equal, then $|A| + |B| = 2|A|$ while $|A + B| = |2A| = 2^n|A|$.

Let us now apply our definitions to derive (51). We let $A = (a_{ij})$ be an m by n matrix, $B = (b_{jk})$ be an n by q matrix, and A_1 be an s by t matrix, so that $A_1 = (a_{ij})$ but now with $i = 1, \ldots, s$ and $j = 1, \ldots, t$. Then (51) has meaning only if B_1 has t rows, and we thus assume that B_1 is a matrix of t rows and g columns. Our partitioning is now completely determined and necessarily A_2 has s rows and $n - t$ columns, A_3 has $m - s$ rows and t columns, A_4 has $m - s$ rows and $n - t$ columns, B_2 has t rows and $q - g$ columns, B_3 has $n - t$ rows and g columns, B_4 has $n - t$ rows

and $q - g$ columns. The element in the ith row and kth column of AB may clearly be expressed as

$$\sum_{j=1}^{n} a_{ij}b_{jk} = \sum_{j=1}^{t} a_{ij}b_{jk} + \sum_{j=t+1}^{n} a_{ij}b_{jk}$$
$$(i = 1, \ldots, m;\ k = 1, \ldots, q).$$

But this equation is equivalent to the matrix equation given by

$$(57) \qquad A = (D_1 \quad D_2), \qquad B = \begin{pmatrix} E_1 \\ E_2 \end{pmatrix}, \qquad AB = D_1E_1 + D_2E_2,$$

where we define D_1, D_2, E_1, E_2 by

$$(58) \quad D_1 = \begin{pmatrix} A_1 \\ A_3 \end{pmatrix}, \qquad D_2 = \begin{pmatrix} A_2 \\ A_4 \end{pmatrix}, \qquad E_1 = (B_1, B_2), \qquad E_2 = (B_3, B_4).$$

Moreover, we may obtain (51) from (57) by simply using the ranges 1, 2, $\ldots$, s and $s + 1, \ldots, m$ for i separately, as well as 1, 2, $\ldots$, g and $g + 1, \ldots, q$ for j separately. In matrix language we have used (58) and computed

$$(59) \quad \begin{pmatrix} A_1 \\ A_3 \end{pmatrix}(B_1, B_2) = \begin{pmatrix} A_1B_1 & A_1B_2 \\ A_3B_1 & A_3B_2 \end{pmatrix}, \qquad \begin{pmatrix} A_2 \\ A_4 \end{pmatrix}(B_3, B_4) = \begin{pmatrix} A_2B_3 & A_2B_4 \\ A_4B_3 & A_4B_4 \end{pmatrix}$$

as the result of partition of matrices and then have used (57) and addition of matrices in (59) to give (51).

We shall now apply the process above to prove the following theorem on symmetric matrices mentioned above.

Theorem 13. *Let* A_1 *and* B_1 *be* r*-rowed nonsingular symmetric matrices with elements in* F, *and* A *and* B *be the corresponding* n*-rowed symmetric matrices*

$$(60) \qquad \mathrm{A} = \begin{pmatrix} \mathrm{A}_1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad \mathrm{B} = \begin{pmatrix} \mathrm{B}_1 & 0 \\ 0 & 0 \end{pmatrix}.$$

of rank r. *Then* A *and* B *are congruent in* F *if and only if* A_1 *and* B_1 *are congruent in* F.

For if A_1 and B_1 are congruent in F there exists a nonsingular matrix P_1 such that $P_1A_1P_1' = B_1$. Then $P = \mathrm{diag}\,\{P_1, I_{n-r}\}$ is nonsingular, and com-

putation by the use of (51) gives $PAP' = B$. Conversely, if $PAP' = B$ for a nonsingular matrix P we may write

$$P = \begin{pmatrix} P_1 & P_2 \\ P_3 & P_4 \end{pmatrix},$$

where P_1 is an r-rowed square matrix, and we shall have

$$P' = \begin{pmatrix} P_1' & P_3' \\ P_2' & P_4' \end{pmatrix}, \qquad PAP' = P \begin{pmatrix} A_1P_1' & A_1P_3' \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} P_1A_1P_1' & P_1A_1P_3' \\ P_3A_1P_1' & P_3A_1P_3' \end{pmatrix}$$

But then $B_1 = P_1A_1P_1'$, and P_1 must be nonsingular since $|B_1| = |P_1'| \cdot |A_1| \cdot |P_1| \neq 0$. Hence B_1 and A_1 are congruent in F.

The result above thus states that, if f and g are quadratic forms with coefficients in F so that f and g are equivalent only if they have the same rank r, then f may be written as a nonsingular form f_0 in r variables, g may be written as a nonsingular form g_0 in r variables, and finally the original forms f and g are equivalent in F if and only if f_0 and g_0 are equivalent in F.

ORAL EXERCISES

1. Compute $A + B$ if

$$a)\ A = \begin{pmatrix} 2 & -1 & 3 \\ 1 & 0 & 2 \\ -1 & 3 & 4 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 7 & -6 \\ -2 & 1 & -5 \\ 4 & 3 & -1 \end{pmatrix}$$

$$b)\ A = \begin{pmatrix} -3 & 4 & 5 \\ 5 & -1 & 2 \\ 3 & 1 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} -3 & 5 & 3 \\ 4 & -1 & 1 \\ 5 & 2 & 1 \end{pmatrix}$$

2. Verify that $(A + B)' = A' + B'$ for any m by n matrices A and B.

3. Show that every n-rowed square matrix A is expressible uniquely as the sum of a symmetric matrix B and a skew matrix C. Hint: Put $A = B + C$ with $B = B'$, $-C = C'$, compute A', and solve.

15. Real quadratic forms. We shall close our study of symmetric matrices and hence of quadratic forms with coefficients in F as well by considering the case where F is the field of all real numbers. Let then $f = x'Ax$ have rank r so that we may take $f = a_1x_1^2 + \ldots + a_rx_r^2$ for real $a_i \neq 0$. We now call the number of positive a_i the index t of f and prove

Theorem 14. *Two quadratic forms with real coefficients are equivalent in the field of all real numbers if and only if they have both the same rank and the same index.*

For proof we observe, first, that by Section 14 there is no loss of generality if we assume that $f = x'Ax$ where A is a nonsingular diagonal matrix, that is, $r = n$. Moreover, there is clearly no loss of generality if we take $A = \text{diag}\ \{d_1, \ldots, d_t, -d_{t+1}, \ldots, -d_r\}$ for positive d_i. Then there exist real numbers $p_i \neq 0$ such that $p_i^2 = d_i$, and if P is the nonsingular matrix $\text{diag}\ \{p_1^{-1}, \ldots, p_r^{-1}\}$ then PAP' is the matrix $\text{diag}\ \{1, \ldots, 1, -1, \ldots, -1\}$ with t elements 1 and $r - t$ elements -1. Thus, f is equivalent in F to

$$(x_1^2 + \ldots + x_t^2) - (x_{t+1}^2 + \ldots + x_r^2)\,. \tag{61}$$

Now, if g has the same rank and index as f, it is equivalent in F to (61) and hence to f. Conversely, let g have rank $r = n$ and index s so that g is equivalent in F to

$$(x_1^2 + \ldots + x_s^2) - (x_{s+1}^2 + \ldots + x_r^2)\,. \tag{62}$$

We propose to show that $s = t$. There is clearly no loss of generality if we assume that $s \geqq t$ and show that if $s > t$ we arrive at a contradiction.

Hence, let $s > t$. Our hypothesis that the form f defined by (61) and the form g defined by (62) are equivalent in the real field implies that there exist real numbers d_{ij} such that if we substitute the linear forms

$$x_i = d_{i1}y_1 + \ldots + d_{in}y_n \qquad (i = 1, \ldots, n)\,, \tag{63}$$

in $f = f(x_1, \ldots, x_n)$, we obtain as a result $(y_1^2 + \ldots + y_s^2) - (y_{s+1}^2 + \ldots + y_n^2)$. Put $x_1 = x_2 = \ldots = x_t = 0$ and $y_{s+1} = \ldots = y_n = 0$ in (63) and consider the resulting t equations

$$d_{i1}y_1 + \ldots + d_{is}y_s = 0 \qquad (i = 1, \ldots, t)\,. \tag{64}$$

These are t linear homogeneous equations in $s > t$ unknowns, and there exist real numbers $v_1, \ldots, v_s$ not all zero and satisfying these equations. The remaining $n - t$ equations of (63) then determine the values of x_j as certain numbers u_j for $j = t + 1, \ldots, n$; and we have the result $h = f(0, 0, \ldots, 0, u_{t+1}, \ldots, u_n) = v_1^2 + \ldots + v_s^2 > 0$. But clearly $h = -(u_{t+1}^2 + \ldots + u_n^2) \leqq 0$, a contradiction.

We have now shown that two quadratic forms with real coefficients and the same rank are equivalent in the field of all complex numbers but that, if their indices are distinct, they are inequivalent in the field of all real numbers. We shall next study in some detail the important special case $t = r$ of our discussion.

A symmetric matrix A and the corresponding quadratic form $f = x'Ax$ are called *semidefinite* of rank r if A is congruent in F to a matrix

$$\begin{pmatrix} aI_r & 0 \\ 0 & 0 \end{pmatrix},$$

for $a \neq 0$ in F. Thus f is semidefinite if it is equivalent to a form $a(x_1^2 + \ldots + x_r^2)$. We call A and f definite if $r = n$, that is, A is both semidefinite and nonsingular.

If F is the field of all real numbers, we may take $a = 1$ and call A and f positive or take $a = -1$ and call A and f negative. Then A and f are negative if and only if $-A$ and $-f$ are positive. Thus we may and shall restrict our attention to positive symmetric matrices and positive quadratic forms without loss of generality.

If $f(x_1, \ldots, x_n)$ is any real quadratic form, we have seen that there exists a nonsingular transformation (63) with real d_{ij} such that $f = y_1^2 + \ldots + y_t^2 - (y_{t+1}^2 + \ldots + y_r^2)$. If $c_1, \ldots, c_n$ are any real numbers and if we put $x_i = c_i$ in (63), there exist unique solutions $y_j = d_j$ of the resulting system of linear equations, and the d_j may readily be seen to be all zero if and only if the c_i are all zero. Now if $t < r$, we have $f < 0$ for $y_1 = \ldots = y_t = 0, y_{t+1} = 1, f(c_1, \ldots, c_n) < 0$. Conversely, if $f(c_1, \ldots, c_n) < 0$, then $t < r$. For otherwise $f = y_1^2 + \ldots + y_r^2$, $f(c_1, \ldots, c_n) = d_1^2 + \ldots + d_r^2 \geqq 0$. If $t = r < n$, then we put $y_{r+1} = 1$ and all other $y_j = 0$ and have $c_1, \ldots, c_n$ not all zero such that $f(c_1, \ldots, c_n) = 0$. Hence, if $f(c_1, \ldots, c_n) > 0$ for all real c_i not all zero, the form f is positive definite. Conversely, if f is positive definite, we have $f = y_1^2 + \ldots + y_n^2$, $f(c_1, \ldots, c_n) = d_1^2 + \ldots + d_n^2 > 0$ for all d_j not all zero and hence for all c_i not all zero. We have proved

Theorem 15. *A real quadratic form* $f(x_1, \ldots, x_n)$ *is positive semidefinite if and only if* $f(c_1, \ldots, c_n) \geqq 0$ *for all real* c_i, *is positive definite if and only if* $f(c_1, \ldots, c_n) > 0$ *for all real* c_i *not all zero.*

As a consequence of this result we shall prove

Theorem 16. *Every principal submatrix of a positive semidefinite matrix is positive semidefinite, every principal submatrix of a positive definite matrix is positive definite.*

For a principal submatrix B of a symmetric matrix A is defined as any m-rowed symmetric submatrix whose rows are in the i_1th, $\ldots$, i_mth rows of A and whose corresponding columns are in the corresponding columns of A. Put $x_0' = (x_{i_1}, \ldots, x_{i_m})$ so that $g = x_0'Bx_0$ is the quadratic form with B as matrix, and we obtain g from f by putting $x_j = 0$ in f for $j \neq i_k$. Clearly, if $f \geqq 0$ for all $x_i = c_i$, then $g \geqq 0$ for all values of the x_{i_k}, and

hence B is positive semidefinite by Theorem 15. If A is positive definite and B is singular, then $g = 0$ for x_{i_k} not all zero, and hence $f = 0$ for the x_j above all zero and for the x_{i_k} not all zero, a contradiction.

The converse of Theorem 16 is also true, and we refer the reader to the author's *Modern Higher Algebra* for its proof. We shall use the result just obtained to prove

Theorem 17. *Let* A *be an* m *by* n *matrix of rank* r *and with real elements. Then* AA′ *is a positive semidefinite real symmetric matrix of rank* r.

For we may write

$$A = P\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}Q, \qquad QQ' = \begin{pmatrix} Q_1 & Q_2 \\ Q_3 & Q_4 \end{pmatrix},$$

where P and Q are nonsingular matrices of m and n rows, respectively. Then QQ' is a positive definite symmetric matrix, and we partition QQ' so that Q_1 is an r-rowed principal submatrix of QQ'. By Theorem 16 the matrix Q_1 is positive definite,

$$AA' = P\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}QQ'\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}P' = P\begin{pmatrix} Q_1 & 0 \\ 0 & 0 \end{pmatrix}P' = PCP'$$

is congruent to the positive semidefinite matrix C of rank r and hence has the property of our theorem.

EXERCISE

What are the ranks and indices of the real symmetric matrices of Ex. 2, Section 11?

CHAPTER IV

LINEAR SPACES

1. Linear spaces over a field. The set V_n of all sequences

$$u = (c_1, \ldots, c_n) \tag{1}$$

may be thought of as a geometric n-dimensional space. We assume the laws of combination of such sequences of Section 1.8 and call u a *point* or *vector*, of V_n. We suppose also that the quantities c_i are in a fixed field F and call c_i the ith *coordinate* of u, the quantities $c_1, \ldots, c_n$ the *coordinates* of u. The entire set V_n will then be called the n-*dimensional linear space over* F.

The properties of a field F may be easily seen to imply that

$$(u + v) + w = u + (v + w), \qquad u + v = v + u \tag{2}$$

$$a(bu) = (ab)u, \qquad (a + b)u = au + bu, \qquad a(u + v) = au + av \tag{3}$$

for all a, b in F and all vectors u, v, w of V_n. The vector which we designate by 0 is that vector all of whose coordinates are zero, and we have

$$u + 0 = u, \qquad u + (-u) = 0, \tag{4}$$

where $-u = (-c_1, \ldots, -c_n)$. Then

$$0 \cdot u = 0, \qquad 1 \cdot u = u, \qquad -u = -1 \cdot u. \tag{5}$$

Note that the first 0 of (5) is the quantity 0 of F, and the second zero is the *zero vector*. We shall use the properties just noted somewhat later in an *abstract* definition of the mathematical concept of linear space, and we leave the verification of the properties (2), (3), (4), and (5) of V_n to the reader.

2. Linear subspaces. A subset L of V_n is called a *linear subspace* of V_n if $au + bv$ is in L for every a and b of F, every u and v of L. Then it is clear that L contains all linear combinations

$$u = a_1u_1 + \ldots + a_mu_m, \tag{6}$$

for a_i in F, and u_i in L.

We observe that the set of all linear combinations (6) of any finite number m of given vectors, $u_1, \ldots, u_m$ is a linear subspace L of V_n according to this definition. If now L is so defined, we shall say that $u_1, \ldots, u_m$ *span* the space L and shall write

$$L = \{u_1, \ldots, u_m\} . \tag{7}$$

It is clear that, if e_j is the vector whose jth coordinate is unity and whose other coordinates are zero, then $e_1, \ldots, e_n$ span V_n.

The space spanned by the zero vector consists of the zero vector alone and may be called the *zero space* and designated by $L = \{0\}$. In what follows we shall restrict our attention to the nonzero subspaces L of V_n, and, for the time being, we shall indicate, when we call L a linear space over F, that L is a linear subspace over F of some V_n over F.

3. Linear independence. Our definition of a linear space L which is a subspace of V_n implies that every subspace L contains the zero vector. If $L = \{u_1, \ldots, u_m\}$, then $0 = 0u_1 + \ldots + 0u_m$. Hence the zero vector of L is expressible in the form (6) in at least this one way. We shall say that $u_1, \ldots, u_m$ are *linearly independent* in F or that $u_1, \ldots, u_m$ are a set of *linearly independent vectors* (of V_n over F), if there is *no other* such expression of 0 in the form (6). Thus, $u_1, \ldots, u_m$ are linearly independent if it is true that a linear combination $a_1u_1 + \ldots + a_mu_m = 0$ if and only if $a_1 = a_2 = \ldots = a_m = 0$. If $u_1, \ldots, u_m$ are not linearly independent in F, we shall say that they are *linearly dependent* in F.

A set of vectors $u_1, \ldots, u_m$ are now seen to be linearly independent in F *if and only if the expression of every* u *of* $\mathrm{L} = \{\mathrm{u}_1, \ldots, \mathrm{u}_m\}$ *in the form* (6) *is unique.* For this property clearly implies linear independence as the special case $u = 0$. Conversely, if $u_1, \ldots, u_m$ are linearly independent and $u = a_1u_1 + \ldots + a_mu_m = b_1u_1 + \ldots + b_mu_m$, then $0 = (a_1 - b_1)u_1 + \ldots + (a_m - b_m)u_m$, $a_i - b_i = 0$, $a_i = b_i$ as desired. We now make the

DEFINITION. *Let* $\mathrm{L} = \{\mathrm{u}_1, \ldots, \mathrm{u}_m\}$ *over* F *and* $\mathrm{u}_1, \ldots, \mathrm{u}_m$ *be linearly independent in* F. *Then we shall call* $\mathrm{u}_1, \ldots, \mathrm{u}_m$ *a* basis *over* F *of* L *and indicate this by writing*

$$\mathrm{L} = \mathrm{u}_1\mathrm{F} + \ldots + \mathrm{u}_m\mathrm{F} . \tag{8}$$

It is evident that $V_n = e_1F + \ldots + e_nF$. But we may actually show that every subspace L spanned by a finite number of vectors of V_n has a basis in the above sense. Observe, first, that the definition of linear inde-

pendence in case $m = 1$ is that $au = 0$ only if $a = 0$ and thus that $u \neq 0$. Then let $u_1, \ldots, u_r$ be linearly independent vectors of V_n and $u \neq 0$ be another vector. Then either $u_1, \ldots, u_r, u$ are linearly independent in F or $a_1u_1 + \ldots + a_ru_r + a_0u = 0$ for a_i not all zero. If $a_0 = 0$, then $a_1u_1 + \ldots + a_ru_r = 0$, from which $a_1 = \ldots = a_r = 0$, a contradiction. But then $u = (-a_0^{-1}a_1)u_1 + \ldots + (-a_0^{-1}a_n)u_r$ is in $\{u_1, \ldots, u_r\}$. It follows that, if $u_1, \ldots, u_m$ are any m distinct nonzero vectors, we may choose some largest number r of vectors in this set which are linearly independent in F and we will then have the property that all remaining vectors in the set are linear combinations with coefficients in F of these r. We state this result as

Theorem 1. *Let* L *be spanned by* m *distinct nonzero vectors* $u_1, \ldots, u_m$. *Then* L *has a basis consisting of certain* r *of these vectors,* $1 \leq r \leq m$.

EXERCISES

1. Determine which of the following sets of three vectors form a basis of the subspace they span. Hint: It is easy to see whether some two of the vectors, say u_1 and u_2 are linearly independent. To see if u_1, u_2, u_3 are linearly dependent we write $u_3 = xu_1 + yu_2$ and solve for x and y.

a) $u_1 = (1, 3, -3)$, $u_2 = (2, 5, 2)$, $u_3 = (1, 1, 6)$

b) $u_1 = (3, 1, 2)$, $u_2 = (4, 1, 3)$, $u_3 = (-1, -1, 0)$

c) $u_1 = (-1, -1, 1)$, $u_2 = (3, 2, 1)$, $u_3 = (7, 3, 9)$

d) $u_1 = (1, -2, -1, 3)$, $u_2 = (2, -1, 1, 6)$, $u_3 = (0, -1, -3, 1)$

e) $u_1 = (1, 1, 1, -1)$, $u_2 = (2, 2, 2, -2)$, $u_3 = (1, 2, 3, 4)$

f) $u_1 = (1, -1, 1, -1)$, $u_2 = (1, 1, 1, 0)$, $u_3 = (5, -1, 5, -3)$

2. Show that the space $L = \{u_1, u_2, u_3\}$ spanned by the following sets of vectors is V_3. Hint: In every case one of the vectors, say u_1, has first coordinate not zero, and L contains $u_2 - x_2u_1 = (0, b_2, c_2)$, $u_3 - x_3u_1 = (0, b_3, c_3)$. Some linear combination of these two quantities has the form $(0, 0, d)$ and L contains $e_3 = (0, 0, 1)$. It is easy to show then that L contains $e_2 = (0, 1, 0)$ and $e_1 = (1, 0, 0)$, $L = V_3$.

a) $u_1 = (1, -2, 3)$, $u_2 = (2, 3, 1)$, $u_3 = (-1, 3, 2)$

b) $u_1 = (0, 1, 8)$, $u_2 = (1, -3, 6)$, $u_3 = (1, -1, 23)$

c) $u_1 = (0, 3, 2)$, $u_2 = (0, 2, 1)$, $u_3 = (1, 5, 4)$

3. Determine whether or not the spaces spanned by the following sets of vectors u_1, u_2 coincide with those spanned by the corresponding v_1, v_2. Hint: If $L_1 =$

$\{u_1, u_2\} = L_2 = \{v_1, v_2\}$, there must exist solutions x_1, x_2, x_3, x_4 of the equations $v_1 = x_1u_1 + x_2u_2$, $v_2 = x_3u_1 + x_4u_2$ such that the determinant $x_1x_4 - x_2x_3 \neq 0$.

a) $u_1 = (3, -1, 2, 1)$, $u_2 = (1, 4, 6, 1)$,
$v_1 = (7, -11, -6, 1)$, $v_2 = (7, 2, 10, 3)$

b) $u_1 = (1, 2, -1, 2)$, $u_2 = (1, 2, 3, 4)$,
$v_1 = (1, 2, -13, -4)$, $v_2 = (0, 0, 4, 1)$

c) $u_1 = (1, -1, 2, -3)$, $u_2 = (2, -2, 4, -6)$,
$v_1 = (3, -3, 6, -9)$, $v_2 = (4, -4, 8, -9)$

d) $u_1 = (1, -1, 0, 3)$, $u_2 = (2, 1, 0, 1)$,
$v_1 = (-1, -2, 1, 2)$, $v_2 = (2, -2, 0, 6)$

e) $u_1 = (1, -2, 0, 1)$, $u_2 = (2, -1, 1, 0)$,
$v_1 = (3, -3, 1, 1)$, $v_2 = (-1, -1, -1, 1)$

f) $u_1 = (1, 0, 1, -2)$, $u_2 = (0, 1, -1, 2)$,
$v_1 = (2, -2, 4, -8)$, $v_2 = (1, 1, 0, 0)$

4. The row and column spaces of a matrix. We shall obtain the principal theorems on the elementary properties of linear spaces by connecting this theory with certain properties of matrices which we have already derived. Let us consider a set of m vectors,

$$u_i = (a_{i1}, \ldots, a_{in}) \qquad (i = 1, \ldots, m), \tag{9}$$

of V_n over F. Then we may regard u_i as being the ith row of the corresponding m by n matrix $A = (a_{ij})$ and the space $L = \{u_1, \ldots, u_m\}$ as being what we shall call the *row space* of A. Thus every m by n matrix defines a linear subspace of V_n, every subspace of V_n spanned by m vectors defines a corresponding m by n matrix.

If $P = (p_{ki})$ is any q by m matrix, the product PA is a q by n matrix. The jth coordinate of the vector

$$w_k = p_{k1}u_1 + \ldots + p_{km}u_m \tag{10}$$

is $p_{k1}a_{1j} + \ldots + p_{km}a_{mj}$, that is, the element in the kth row and jth column of PA. Hence *the* k*th row of* PA *is that linear combination of the rows of* A *whose coefficients form the* k*th row of* P.

We have now shown that every row of PA is in the row space of A. It follows that the row space of PA is contained in that of A. If P is nonsingu-

lar, then the result just derived implies that the row space of $A = P^{-1}(PA)$ is contained in the row space of PA and therefore that these two linear spaces are the same. Thus we have

LEMMA 1. *Let* P *be an* m*-rowed nonsingular matrix. Then the row spaces of* PA *and* A *coincide.*

In the proof of Theorem 3.6 we used the matrix product equivalent of the elementary transformation Theorem 2.4, and we shall now state this theorem as the useful

LEMMA 2. *Let* A *be an* m *by* n *matrix of rank* r. *Then there exist nonsingular matrices* P *and* Q *of* m *and* n *rows, respectively, such that*

$$\text{(11)} \qquad PA = \begin{pmatrix} G \\ 0 \end{pmatrix}, \qquad AQ = (H \quad 0),$$

where G *and* H *have rank* r, G *is an* r *by* n *matrix,* H *is an* m *by* r *matrix.*

We use (11) and note that the rows of G differ from those of PA only in zero rows. Then the rows of G span the row space of PA. By Lemma 1 we have

LEMMA 3. *The row spaces of* G *and* A *coincide.*

We shall use this result in the proof of

Theorem 2. *The* r *rows of* G *form a basis of the row space of* A. *Any* r + 1 *vectors of the row space of* A *are linearly dependent in* F.

For we may designate the rows of G by $v_1, \ldots, v_r$. Our definition of G implies that there is no loss of generality if we permute its rows in any desired fashion. Thus, if $b_1v_1 + \ldots + b_rv_r = 0$ for b_i in F not all zero, we may assume for convenience that $b_1 \neq 0$. The determinant of the r-rowed square matrix

$$\text{(12)} \qquad P = \begin{pmatrix} P_1 \\ P_2 \end{pmatrix}, \qquad P_1 = (b_1, \ldots, b_r), \qquad P_2 = (0, I_{r-1})$$

is clearly b_1, and hence P is nonsingular. Then PG is r-rowed and of rank r. But this is impossible since $b_1v_1 + \ldots + b_rv_r = 0$ is the first row of PG. Hence the rows of G are linearly independent in F, they span the row space of G and of A, they are a basis of the row space of A.

Assume, now, that $w_k = b_{k1}v_1 + \ldots + b_{kr}v_r$ for $k = 1, \ldots, r+1$, so that w_k are any $r+1$ vectors of the row space $L = v_1F + \ldots + v_rF$ of A. Define $B = (b_{ki})$ and obtain w_k as the kth row of the $r+1$ by n matrix BG. By Theorem 3.6 the rank of BG is at most r, and by Lemma 2 there exists a nonsingular $(r+1)$-rowed matrix $D = (d_{gk})$ for $g, k = 1, \ldots, r+1$, such that the $(r+1)$st row of $D(BG)$ is the zero vector. But then

$d_{r+1,\,1}w_1 + \ldots + d_{r+1,\,r+1}w_{r+1} = 0$, the $d_{r+1,\,k}$ form a row of the nonsingular matrix D and cannot all be zero, the vectors $w_1, \ldots, w_{r+1}$ are linearly dependent in F. This proves Theorem 2.

We now apply Theorem 1 to obtain

Theorem 3. *The matrix* G *of Lemma 2 may be taken to be a submatrix of* A. *The integer* r *of Theorem 1 is in fact the rank of the* m *by* n *matrix whose* i*th row is* u_i.

For let A be an m by n matrix whose ith row is u_i and let r be the integer of Theorem 1, the rank of A be s. After a permutation of the rows of A, if necessary, we may assume that $u_1, \ldots, u_r$ are a basis of the row space of A. Then $u_k = b_{k1}u_1 + \ldots + b_{kr}u_r$ for b_{ki} in F, and $k = r + 1, \ldots, m$. The matrix P given by

$$P = \begin{pmatrix} I_r & 0 \\ B & I_{m-r} \end{pmatrix}, \qquad B = (-b_{ki}), \tag{13}$$

is nonsingular, and it is clear that if

$$G = \begin{pmatrix} u_1 \\ \cdot \\ \cdot \\ \cdot \\ u_r \end{pmatrix}, \tag{14}$$

then PA is given by (11). It follows that s is the rank of G, $s \leq r$. If $s < r$ we apply Lemma 2 to obtain a nonsingular r-rowed matrix $D = (d_{ik})$ such that the rth row of $DG = 0$, the rth row of D is not zero, $d_{r1}u_1 + \ldots + d_{rr}u_r = 0$ contrary to our hypothesis that $u_1, \ldots, u_r$ are linearly independent. This completes our proof.

We may now obtain the principal result on linear subspaces of V_n.

Theorem 4. *Every linear subspace* L *over* F *of* V_n *over* F *has a basis. Any two bases of* L *have the same number* $r \leq n$ *of vectors, and we shall call* r *the order of* L *over* F.

For $V_n = e_1F + \ldots + e_nF$, and by Theorem 2 any $n + 1$ vectors of V_n are linearly dependent in F. Thus any linear subspace L over F of V_n contains at most n linearly independent vectors. It follows that there exists a maximum number $r \leq n$ of linearly independent vectors $u_1, \ldots, u_r$ in L, and that $u, u_1, \ldots, u_r$ are linearly dependent in F for every u of L. By the proof of Theorem 1 the vector u is in $\{u_1, \ldots, u_r\}$, $L = u_1F + \ldots + u_rF$. But if also $L = v_1F + \ldots + v_sF$, then Theorem 2 implies that $s \leq r$ and similarly that $r \leq s$, $r = s$ is unique.

In closing this section we note that the rows of the transpose A' of A are uniquely determined by the columns of A and are, indeed, their transposes. Thus we shall call the row space of A' the *column space* of A. It is a linear subspace of V_m. We call the order of the row and column spaces of A, respectively, the *row* and *column ranks* of A. By Theorem 3 the rank of A is its row rank. Also A and A' have the same rank and we have proved

Theorem 5. *The row and column ranks of a matrix are equal to its rank.*

EXERCISES

1. Solve Ex. 1 and 2 of Section 3 by the use of elementary transformations to compute the rank of the matrices whose rows are the given vectors.

2. Form the four-rowed matrices whose rows are the vectors u_1, u_2, v_1, v_2 of Ex. 3, Section 3. Show thus that $L_1 = \{u_1, u_2\} = L_2 = \{v_1, v_2\}$ if and only if the ranks of the corresponding matrices A are equal to the order of the subspace L_1, that is, the rank of the matrices formed from the first two rows of each A.

3. Find a basis of the row space of each of the following matrices, the basis to consist actually of rows of the corresponding matrix.

$$a)\begin{pmatrix} 1 & -2 & 1 & 0 \\ 2 & -4 & 2 & 0 \\ 2 & -3 & -1 & 1 \\ 4 & -7 & 1 & 1 \\ 2 & -3 & -1 & 1 \end{pmatrix} \qquad b)\begin{pmatrix} 2 & 3 & 0 & 1 \\ -2 & -1 & -1 & 1 \\ -2 & -1 & 0 & 3 \\ 0 & 4 & -1 & 2 \\ 2 & 1 & 2 & -2 \end{pmatrix}$$

$$c)\begin{pmatrix} -1 & 0 & 0 & 1 \\ 0 & -1 & 1 & 1 \\ 2 & 3 & 0 & -1 \\ 5 & 1 & 0 & 0 \\ 1 & 2 & 3 & 4 \end{pmatrix} \qquad d)\begin{pmatrix} 1 & 2 & -1 & 3 & 4 \\ 3 & 5 & 1 & 0 & 2 \\ 1 & 1 & 3 & -6 & -6 \\ 4 & 7 & 0 & 3 & 6 \\ 1 & 0 & 7 & -15 & -16 \end{pmatrix}$$

4. Let A be a rectangular matrix of the form

$$\begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix},$$

where A_1 is nonsingular. Show that then there exists a nonsingular matrix P such that

$$PA = \begin{pmatrix} A_1 & A_2 \\ 0 & A_5 \end{pmatrix}.$$

Give also a simple form for P. Hint: Show that the rows of A_3 are in the row space of A_1.

5. Let the matrix of Ex. 4 be either symmetric or skew. Show that the choice of P then implies that

$$PAP' = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}.$$

Show also that, if the order of A_1 is the rank of A, the matrix $A_2 = 0$.

5. The concept of equivalence. In discussing the properties of mathematical systems such as fields and linear spaces over F it becomes desirable quite frequently to identify in some fashion those systems behaving exactly the same with respect to the given set of definitive properties under consideration. We shall call such systems *equivalent* and shall now proceed to define this concept in terms of that of *function*.

Let G and G' be two systems and define a single-valued function f *on* G *to* G'. In elementary mathematics it is customary to call G the *range of the independent variable* and G' the *range of the dependent variable*. However, it is more convenient in general situations to say that f is a function on G to G' or that f is a *correspondence on* G *to* G'. Then f is given by

$$g \to g' = f(g) \tag{15}$$

(*read* g corresponds to g') such that every element g of G determines a unique corresponding element g' of G'. In elementary algebra and analysis the systems G and G' are usually taken to be the field of all real or all complex numbers and (15) is then given by a formula $y = f(x)$. But the basic idea there is that given above of a correspondence (15) on G to G'. This concept may be seen to be sufficiently general as to permit its extension in many directions.

Suppose now that (15) is a correspondence such that *every* element g' of G' is the corresponding element $f(g)$ of one and only one g of G. Then we call (15) a *one-to-one correspondence on* G *to* G'. It is clear that (15) then defines a second one-to-one correspondence

$$f(g) = g' \to g, \tag{16}$$

which is now on G' to G, and we may thus call (15) a *one-to-one correspondence between* G *and* G' and indicate this by writing

$$g \longleftrightarrow g'. \tag{17}$$

Note, however, that, if G and G' are the same system, the functions (15) and (16) are, in general, distinct. Thus we may let G be the field of all real

numbers and (15) be the function $x \to 2x$, so that (16) is the function $x \to \frac{1}{2}x$. Of course, if G and G' are distinct it is not particularly important whether we use (15) or (16) to define our correspondence.

We proceed to use the concept just given in constructing the fundamental definition of this section, that of equivalence. Let us consider two mathematical systems G, G' of the same kind such as two fields or two linear spaces over a fixed field F. These systems consist of sets of elements g, h, . . . closed with respect to certain operations. (Thus, for example, we might have $g + h$ in G for every g and h in G and also $g' + h'$ in G' for every g' and h' in G'.) We then call G *and* G′ *equivalent* if there exists a one-to-one correspondence between them which is preserved under the operations of their definition. We now see that we have defined two fields F and F' to be equivalent if there exists a one-to-one correspondence (15) between them such that $(g + h)' = g' + h'$, $(gh)' = g'h'$ for every g and h of F. Let us then pass to the second case which we require for our further discussion of linear spaces.

Let F be a fixed field and V consist of a set of elements such that $u + v$ and au are unique elements of V for every u and v of V and a of F. Then we shall call V *a general linear space over* F. If V_0 is a second* such space and there is a one-to-one correspondence $u \longleftrightarrow u_0$ between V and V_0 such that

$$(u + v)_0 = u_0 + v_0\,, \qquad (au)_0 = au_0$$

for every u and v of V and a of F, then we shall say that V and V_0 *are equivalent over* F. We have thus introduced two instances of what is a very important concept in all algebra.

The reader should observe that under our definition every mathematical system G is equivalent to itself and that if G is equivalent to a system G', then G' is equivalent to G. Finally, if G' is equivalent to G'', then G is equivalent to G''.

EXERCISES

1. Verify the statement that the field of all rational functions with rational coefficients of the complex number $\sqrt{2}$ is equivalent to the field of all matrices

$$A = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$$

for rational a and b under the correspondence $A \longleftrightarrow a + b\sqrt{2}$.

* We use the notation V_0 instead of V' to avoid confusion in the consequent usage of u' for the arbitrary vector of V' as well as for the transpose of u.

2. Verify the statement that the field of complex numbers is equivalent to the field of matrices

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

for real a and b.

3. Verify the statement that the set of all scalar matrices with elements in a field F forms a field equivalent to F.

4. Verify the statement that the mathematical system consisting of all two-rowed square matrices with elements in F and defined with respect to addition and multiplication is equivalent to the set of all matrices

$$\begin{pmatrix} a_{11} & 0 & a_{12} & 0 \\ 0 & a_{11} & 0 & a_{12} \\ a_{21} & 0 & a_{22} & 0 \\ 0 & a_{21} & 0 & a_{22} \end{pmatrix} \qquad (a_{ij} \text{ in } F)$$

under the correspondence indicated by the notation.

6. Linear spaces of finite order. We shall restrict all further study of linear spaces to linear spaces of order n over F. Then we define V to be a *linear space of order* n *over a given field* F if V is equivalent over F to V_n over F. Clearly, our definition implies that every two linear spaces of the same order n over F are equivalent over F.

Our definition also implies that, if V is a linear space of order n over F, then the properties (2), (3), (4), and (5) hold for every u, v, w, of V and a, b in F. Moreover, every quantity of V is uniquely expressible in the form

$$c_1v_1 + \ldots + c_nv_n , \tag{18}$$

where the equivalence between V and V_n is given by

$$c_1v_1 + \ldots + c_nv_n \longleftrightarrow (c_1, \ldots, c_n) . \tag{19}$$

Conversely, define $au = ua$ and $u + v$ to be in V for every u, v of V and a of F. Then it may be shown very easily that, if (2), (3), (4), and (5) hold and every u of V is uniquely expressible in the form (18) for c_i in F, then V is equivalent over F to V_n. However, we prefer instead to *define* V by its equivalence to V_n. This preference then requires the (somewhat trivial) proof of

Theorem 6. *Every linear subspace* L *of order* r *over* F *of* V_n *is equivalent over* F *to* V_r.

Thus we justify the use of the term linear *subspace* L *of order* r *over* F by proving that L is indeed what we have called a linear space of order r over F

contained in the space V_n. For proof we merely observe that every vector of $L = u_1F + \ldots + u_rF$ is uniquely expressible in the form

$$u = c_1u_1 + \ldots + c_ru_r \tag{20}$$

for c_i in F. Thus u in L uniquely determines the c_i in F and conversely. It follows that

$$u \to (c_1, \ldots, c_r) \tag{21}$$

is a one-to-one correspondence between V and V_r and it is trivial to verify that it defines an equivalence of L and V_r.

We have now seen that every linear space L of order n over F may be regarded as a linear subspace of a space M of order m over F for any $m \geq n$. *Moreover,* $\mathrm{L} = \mathrm{M}$ *if and only if* $\mathrm{m} = \mathrm{n}$.

Theorem 3 should now be interpreted for arbitrary linear spaces of order n, and we have a result which we state as

Theorem 7. *Let* $\mathrm{L} = \mathrm{u_1F} + \ldots + \mathrm{u_nF}$ *and* $\mathrm{v_1}, \ldots, \mathrm{v_m}$ *be in* L *so that there exist quantities* $\mathrm{a_{ij}}$ *in* F *for which*

$$\mathrm{v_i} = \mathrm{a_{i1}u_1} + \ldots + \mathrm{a_{in}u_n},$$

and the coefficient matrix $\mathrm{A} = (\mathrm{a_{ij}})$ *is defined. Then the number of the* $\mathrm{v_k}$ *which are linearly independent in* F *is the rank of the matrix* A. *Moreover,* $\mathrm{v_1}, \ldots, \mathrm{v_m}$ *form a basis of* L *over* F *if and only if* $\mathrm{m} = \mathrm{n}$ *and* A *is nonsingular.*

EXERCISES

1. Verify the statement that the following sets of matrices are linear spaces of finite order over F and find a basis for each.
   - *a*) The set of all m by n matrices with elements in F.
   - *b*) The set of all m by n matrices whose elements not in the first row are zero.
   - *c*) The set of all n-rowed scalar matrices.
   - *d*) The set of all n-rowed diagonal matrices.
2. Find bases for the following linear spaces of polynomials with coefficients in F.
   - *a*) All polynomials in x of degree at most three.
   - *b*) All polynomials in independent variables x and y and degree at most two (in x and y together).
   - *c*) All polynomials in $x = t^3 + t$ and $y = t^3 + t^2$ and degree at most two in x and y.
   - *d*) All polynomials in $\sqrt[3]{2}$, with F the field of all rational numbers.
   - *e*) All polynomials in a primitive cube root of unity with F the field of all rational numbers.

f) All polynomials in $w = u(i+1)$ with F the field of all rational numbers and $i^2 = -1$, $u^2 = 2$. Hint: Prove that $1, u, i, ui$ are a basis.

g) The polynomials of (*f*) but with F the field of all real numbers.

3. Let $A = \text{diag}\{1, -1, 2\}$. Show that I, A, A^2 form a basis of the set of all three-rowed diagonal matrices.

4. Show that I, A, B, AB form a basis of the set of all two-rowed square matrices if

$$a)\ A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$b)\ A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}$$

5. Show that, if

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

then $I, A, A^2, B, AB, A^2B, B^2, AB^2, A^2B^2$ form a basis of the set of all three-rowed square matrices.

7. Addition of linear subspaces. If $L_1 = \{v_1, \ldots, v_m\}$ and $L_2 = \{w_1, \ldots, w_q\}$ are linear subspaces over F of a space L of order n over F, the subspace $L_0 = \{v_1, \ldots, v_m, w_1, \ldots, w_q\}$ of L will be called the *sum* of L_1 and L_2 and will be designated generally by

$$L_0 = \{L_1, L_2\}\,. \tag{22}$$

If the only vector which is in both L_1 and L_2 is the zero vector, we shall say that L_1 and L_2 are *complementary* subspaces *of their sum* and write

$$L_0 = L_1 + L_2\,. \tag{23}$$

In this case the order of L_0 is the sum of the orders of L_1 and L_2 and in fact we shall show that, if $L_1 = v_1F + \ldots + v_mF$, $L_2 = w_1F + \ldots + w_qF$, then $L_0 = v_1F + \ldots + v_mF + w_1F + \ldots + w_qF$.

For it is clear that $a_1v_1 + \ldots + a_mv_m + b_1w_1 + \ldots + b_qw_q = 0$ if and only if $v = a_1v_1 + \ldots + a_mv_m = (-b_1)w_1 + \ldots + (-b_q)w_q$ is in both L_1 and L_2. Thus $v \neq 0$ implies that the a_i and b_j are not all zero and therefore that the vectors v_i and w_j spanning L_0 are linearly dependent in F and do not form a basis of L_0. Conversely, if necessarily $v = 0$, then the v_i and w_j do form a basis of L_0, and L_0 has order $m + q$.

If L_1 and L_0 are linear subspaces of L and if L_0 contains L_1, we may ask

whether a linear subspace L_2 of L_0 exists such that $L_0 = L_1 + L_2$. The existence of such a space is clearly a corollary of

Theorem 8. *Let* L_1 *of order* m *over* F *be a linear subspace of* L *of order* n *over* F. *Then there exists a linear subspace* L_2 *of* L *such that* L_1 *and* L_2 *are complementary subspaces of* L.

The result above may be proved by the method we used to prove Theorem 1, where we apply this method to the set $v_1, \ldots, v_m, u_1, \ldots, u_n$, in $L = u_1F + \ldots + u_nF$. However, let us give, instead, a proof using matrix theory. We put $L = V_n$, let G be the m by n matrix whose rows are the basal vectors $v_1, \ldots, v_m$ of L_1. Then G has rank m, and there exists a nonsingular matrix Q such that the columns of GQ are a permutation of those of G,

$$GQ = (G_1 \quad G_2),$$

where G_1 is nonsingular. Then the matrix

$$A_0 = \begin{pmatrix} G_1 & G_2 \\ 0 & I_{n-m} \end{pmatrix}$$

is nonsingular, and $A = A_0Q^{-1}$ is obtained by permuting the columns of A_0. But then

$$A = \begin{pmatrix} G \\ H \end{pmatrix}$$

is nonsingular, the rows of A span V_n, and the rows of H span the space L_2 which we have been seeking. Moreover, it is clear that the rows of H are certain of the vectors e_i which we defined in Section 2.

EXERCISES

1. Let L_1 be the row space of each of the m by n matrices of Section 4, Ex. 3. Use the method above to find a basis of the corresponding V_n consisting of a basis of L_1 and of a complementary space L_2.

2. Let the following vectors u_i span L_1, v_i span L_2. Find a complement in $\{L_1, L_2\}$ to L_1 and to L_2.

a) $\begin{cases} u_1 = (1, -1, 1, 1), & u_2 = (2, -2, 1, 2), & u_3 = (1, -1, 0, 1) \\ v_1 = (1, 2, 1, 0), & v_2 = (4, -1, 4, 0) \end{cases}$

b) $\begin{cases} u_1 = (1, 2, 0, 0), & u_2 = (1, -1, 1, 0), & u_3 = (1, 0, 0, 1) \\ v_1 = (4, 3, 1, 1), & v_2 = (4, -3, 3, 2), & v_3 = (1, 4, 2, -3) \end{cases}$

c) $\begin{cases} u_1 = (1, 0, 2, -1), & u_2 = (0, 1, 2, -1), & u_3 = (2, 1, 6, -3) \\ v_1 = (3, -2, 2, -1), & v_2 = (-5, 3, -4, 2), & v_3 = (-2, 1, -2, 1) \end{cases}$

8. Systems of linear equations. The set of all linear forms in $x_1, \ldots, x_n$ with coefficients in F is a linear space

$$L = x_1F + \ldots + x_nF \tag{24}$$

of order n over F. The left members

$$f_i = f_i(x_1, \ldots, x_n) = a_{i1}x_1 + \ldots + a_{in}x_n \tag{25}$$

of a system

$$a_{i1}x_1 + \ldots + a_{in}x_n = c_i \qquad (i = 1, \ldots, m), \tag{26}$$

of m linear equations in n unknowns, are such forms and are in L. Then, if r is the rank of the m by n matrix $A = (a_{ij})$ of coefficients of (26), we see by Theorem 7 that certain r of the forms f_i are linearly independent in F and the remaining $m - r$ forms are linear combinations of these r.

We may assume without loss of generality that the equations (26) have been labeled so that $f_1, \ldots, f_r$ are linearly independent in F, and

$$f_k = b_{k1}f_1 + \ldots + b_{kr}f_r \qquad (k = r + 1, \ldots, m) \tag{27}$$

for b_{kj} in F. Then

$$A = \begin{pmatrix} u_1 \\ \cdot \\ \cdot \\ \cdot \\ u_m \end{pmatrix}, \qquad u_i = (a_{i1}, \ldots, a_{in}) \qquad (i = 1, \ldots, m), \tag{28}$$

where $u_1, \ldots, u_r$ are linearly independent in F, and

$$u_k = b_{k1}u_1 + \ldots + b_{kr}u_r \quad (k = r + 1, \ldots, m). \tag{29}$$

If the system (26) is consistent, there exist quantities $d_1, \ldots, d_n$ in F such that $f_i(d_1, \ldots, d_n) = c_i$. Then (27) implies that

$$c_k = f_k(d_1, \ldots, d_n) = b_{k1}c_1 + \ldots + b_{kr}c_r \qquad (k = r + 1, \ldots, m). \tag{30}$$

Define the *augmented* matrix A^* of the system (26) to be the m by $n+1$ matrix

$$(31) \qquad A^* = \begin{pmatrix} u_1^* \\ \cdot \\ \cdot \\ \cdot \\ u_m^* \end{pmatrix}, \qquad u_i^* = (u_i, c_i) = (a_{i1}, \ldots, a_{in}, c_i) \qquad (i = 1, \ldots, m),$$

and see that (29) and (30) imply that

$$(32) \qquad u_k^* = b_{k1}u_1^* + \ldots + b_{kr}u_r^* \qquad (k = r+1, \ldots, m),$$

so that the rank of A^* is at most r. But A^* has A as a submatrix; A^* has rank r.

Conversely, if A^* has the same rank r as A and we choose $u_1, \ldots, u_r$ to be linearly independent, then $u_1^*, \ldots, u_r^*$ are clearly linearly independent. We then have (29) and may apply elementary row transformations of type 1 to A^* which add $-(b_{k1}u_1^* + \ldots + b_{kr}u_r^*)$ to u_k^* for $k = r+1, \ldots, m$. These replace the submatrix A of A^* by

$$(33) \qquad \begin{pmatrix} G \\ 0 \end{pmatrix}, \qquad G = \begin{pmatrix} u_1 \\ \cdot \\ \cdot \\ \cdot \\ u_r \end{pmatrix}$$

and replace A^* by

$$(34) \qquad \begin{pmatrix} G & C_1 \\ 0 & C_2 \end{pmatrix}, \qquad C_1 = \begin{pmatrix} c_1 \\ \cdot \\ \cdot \\ \cdot \\ c_r \end{pmatrix},$$

where the $(m-r)$-rowed and one-columned matrix C_2 has $c_{k0} = c_k - (b_{k1}c_1 + \ldots + b_{kr}c_r)$ as its elements. But, clearly, if any $c_{k0} \neq 0$, the matrix A^* has a nonzero $(r+1)$-rowed minor. This is impossible if A^* is of rank r.

We now see that *the system (26) is consistent if and only if* A* *has the same rank* r *as* A. Moreover, we have already shown that, if A^* does have the same rank as A, then $m - r$ of the equations (26) may be regarded as

linear combinations of the remaining r equations and are satisfied by the solutions of these equations. It thus remains to show that any system of r equations in $x_1, \ldots, x_n$ with matrix of rank r has solutions. We may write $x = (x_1, \ldots, x_n)$ and see that such a system may be regarded as a matrix equation

$$Gx' = v', \qquad v = (c_1, \ldots, c_r). \tag{35}$$

Before solving (35) we prove

LEMMA 4. *Let* G *be an* r *by* n *matrix of rank* r. *Then*

$$\mathrm{G} = (\mathrm{I}_r \quad 0)\mathrm{Q} \tag{36}$$

for a nonsingular n*-rowed matrix* Q.

For Lemma 2 states that $G = (H\ 0)Q_1$, where Q_1 is n-rowed and nonsingular and H is an r by r matrix of rank r. Then H is nonsingular, so is $Q_2 = \mathrm{diag}\ \{H, I_{n-r}\}$, $(I_r\ 0)Q_2 = (H\ 0)$. Thus we have (36) for $Q = Q_2Q_1$.

The system (35) may now be written as

$$(I_r \quad 0)y' = v', \qquad y = xQ' = (y_1, \ldots, y_n). \tag{37}$$

But then $y = xQ'$ is a nonsingular linear transformation and the y_i are linearly independent linear forms in $x_1, \ldots, x_n$. Evidently, (37) has the solution $y_i = c_i$ for $i = 1, \ldots, r$; the solution of (35) is then given by $x = y(Q')^{-1}$ for $y_i = c_i (i = 1, \ldots, r)$ and $y_{r+1}, \ldots, y_n$ arbitrary. Observe that, if we choose the notation of the x_i so that $G = (G_1, G_2)$ with G_1 an r-rowed nonsingular matrix, then

$$Q = \begin{pmatrix} G_1 & G_2 \\ 0 & I_{n-r} \end{pmatrix}, \qquad y = (Y_1, Y_2), \qquad x = (X_1, X_2), \tag{38}$$

where Y_1 and X_1 have r columns. From this we obtain

$$Q' = \begin{pmatrix} G_1' & 0 \\ G_2' & I_{n-r} \end{pmatrix}, \qquad xQ' = (X_1G_1' + X_2G_2', X_2),$$

so that

$$X_2 = Y_2 = (x_{r+1}, \ldots, x_n),$$

$$Y_1 = X_1G_1' + X_2G_2' = (c_1, \ldots, c_r),$$

and our solution of (35) is given by

$$X_1 = (Y_1 - X_2G_2')(G_1')^{-1} . \tag{39}$$

But then we have solved for $x_1, \ldots, x_r$ as linear functions of $x_{r+1}, \ldots, x_n$. For exercises on linear equations we refer the reader to the *First Course in the Theory of Equations.*

9. Linear mappings and linear transformations. The system of equations (3.1) of a linear mapping was expressed in (3.32) as a matrix equation $x' = y'A'$. Let us interchange the roles of m and n, A and A' in this equation. Then we see that a linear mapping may be expressed as a matrix equation

$$v = uA , \tag{40}$$

where A is an m by n matrix and

$$u = (y_1, \ldots, y_m) , \qquad v = (x_1, \ldots, x_n) . \tag{41}$$

Clearly, u is a vector of V_m over F, v is a vector of V_n over F, and (40) may be regarded as a correspondence $u \to uA$ defined by A whereby every u of V_m determines a unique vector uA of V_n. We now proceed to formulate this concept more abstractly.

Let L and M be linear spaces of respective orders m and n over F and consider a correspondence on L to M. Designate the correspondence by the symbol S, so that S is the function

$$S: \qquad u \to u^S$$

(*read* u goes to u upper S) wherein every vector u of L determines a unique u^S in M. Suppose also that

$$(au + bu_0)^S = au^S + bu_0^S \tag{42}$$

for every a and b of F, u and u_0 of L. Then we shall call S a *linear mapping* of the space L on the space M and describe (42) as the property that S is linear.

Suppose now that $L = u_1F + \ldots + u_mF$ and $M = v_1F + \ldots + v_nF$, so that we are given not only the spaces L and M but fixed bases as well. Then a linear mapping S uniquely determines u_i^S in M, and hence

$$u_i^S = a_{i1}v_1 + \ldots + a_{in}v_n \qquad (i = 1, \ldots, m) , \tag{43}$$

for a_{ij} in F. Thus S determines also an m by n matrix $A = (a_{ij})$. But, conversely, if A is an m by n matrix and we define u_i^S by (43) for the given elements a_{ij} of A, then the property that S is linear uniquely determines the mapping S. This is true since every u of L is uniquely expressible in the form

$$u = y_1 u_1 + \ldots + y_m u_m , \tag{44}$$

for y_i in F and (42) implies that

$$u^S = y_1 u_1^S + \ldots + y_m u_m^S . \tag{45}$$

It follows that to every linear mapping S of L on M and *given bases* of L and M, there corresponds a unique m by n matrix A and conversely. We shall call A *the matrix of* S *with respect to the given bases* of L and M.

We now observe that

$$u^S = \sum_{i=1}^{m} y_i u_i^S = \sum_{i=1}^{m} y_i \left(\sum_{j=1}^{n} a_{ij} v_j \right) = \sum_{j=1}^{n} x_j v_j$$

where

$$x_j = \sum_{i=1}^{m} y_i a_{ij} \qquad (j = 1, \ldots, n) .$$

But then, if we assume temporarily that $L = V_m$ and $M = V_n$ and put $v = u^S$ in (40) and (41), we see that S is the linear mapping

$$u \to u^S = uA \tag{46}$$

for the given matrix A. Thus every linear mapping which is a change of variable as in (3.1) may be regarded as a linear mapping of the space V_m on the space V_n.

Let us next observe the effect on the matrix defined by a linear mapping of a change of bases of the linear spaces. Define new bases of L and M, respectively, by

$$u_k^{(0)} = \sum_{i=1}^{m} p_{ki} u_i , \qquad v_l^{(0)} = \sum_{j=1}^{n} q_{lj} v_j , \tag{47}$$

for $k = 1, \ldots, m$ and $l = 1, \ldots, n$. Then $P = (p_{ki})$ and $Q = (q_{lj})$ are nonsingular and, as we saw in (3.33), we may also write the second set of equations of (47) in the form

$$v_j = \sum_{l=1}^{n} r_{jl} v_l^{(0)} , \tag{48}$$

where $R = (r_{jl}) = Q^{-1}$. We apply the linearity of S to (47) and obtain $(u_k^{(0)})^S = \sum_{i=1}^{m} p_{ki} u_i^S$. Substituting (43) and (48), we have

$$(u_k^{(0)})^S = \sum_{l=1}^{n} b_{kl} v_l^{(0)} , \tag{49}$$

where $b_{kl} = \Sigma p_{ki} a_{ij} r_{jl}$. Hence the matrix $B = (b_{kl})$ of the linear mapping S with respect to our new bases is given by

$$B = PAQ^{-1} . \tag{50}$$

Since P and Q^{-1} are arbitrary nonsingular matrices of m and n rows, respectively, we see that changes of basis in L and M replace A by an equivalent matrix. Thus any two equivalent m by n matrices define the *same* mapping of L on M.

If L and M are the same space we shall henceforth call a linear mapping S of L on L a *linear transformation* of L. Since we are now considering only a single space, the only possible meaning of the u_i and v_j in (43) can be that of a fixed basis $u_1, \ldots, u_n$ of L of order n over F and of a second basis $v_1, \ldots, v_n$ of L. Let us restrict our attention to the case where $v_i = u_i$. Then we define the matrix A of a linear transformation S on L with respect to a fixed basis $u_1, \ldots, u_n$ of L to be the matrix A determined by (43) with $u_i = v_i$. We have defined thereby a one-to-one correspondence between the set of all n-rowed square matrices with elements in F and the set of all linear transformations on L of order n over F. If $L = V_n$, such a correspondence is given by

$$u \to u^S = uA .$$

Clearly, we should and do call S a *nonsingular linear transformation* if A is nonsingular. Since we may then solve for $u = u^S A^{-1}$, we see that a nonsingular linear transformation defines a one-to-one correspondence of L and itself.

We now observe the effect on A of a change of basis of L. We use (47) but note that $u_i = v_i$ and $u_k^{(0)} = v_k^{(0)}$, so that we have $P = Q$. Hence a change of basis* of L with matrix P replaces the matrix A of a linear transformation by

$$B = PAP^{-1}. \tag{51}$$

It is now clear that in order to study those properties of a linear transformation on L which do not depend on the basis of L over F we need only study those properties of square matrices A which are unchanged when we pass to PAP^{-1}. We shall call two matrices A and B *similar* if (51) holds for a nonsingular matrix P and shall obtain necessary and sufficient conditions that A and B be similar in our next chapter.

EXERCISES

1. Let S be the linear mapping (46) of V_3 on V_4 defined for the following matrices A. Find the vectors of V_4 into which $(-2, 3, 4)$, $(1, 0, 0)$, $(0, 1, 0)$ of V_3 are mapped by S.

$$a)\ A = \begin{pmatrix} 1 & -3 & 0 & 1 \\ 2 & -6 & -1 & 2 \\ -1 & 3 & 1 & -1 \end{pmatrix} \qquad b)\ A = \begin{pmatrix} -2 & 3 & 4 & 0 \\ -1 & 2 & 0 & 4 \\ 0 & 0 & 2 & -3 \end{pmatrix}$$

$$c)\ A = \begin{pmatrix} 2 & -1 & 2 & -5 \\ 0 & -2 & 3 & -2 \\ 1 & 1 & -1 & -1 \end{pmatrix} \qquad d)\ A = \begin{pmatrix} -2 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 1 & 1 & 1 \end{pmatrix}$$

2. Show that the linear transformations (46) of V_3 defined for the following matrices A are nonsingular and find their inverse transformations. Apply both S and S^{-1} to the vectors of Ex. 1.

$$a)\ A = \begin{pmatrix} -4 & 3 & 5 \\ 3 & 0 & 20 \\ 5 & -2 & 11 \end{pmatrix} \qquad b)\ A = \begin{pmatrix} 3 & -1 & -4 \\ 5 & -2 & -1 \\ 2 & -1 & 2 \end{pmatrix}$$

3. Define S for the matrices of Ex. 2 and let C be one or the other of the curves of all vectors (points) $u = (x_1, x_2, x_3)$ whose coordinates satisfy the following equations. Find the equation of the curves C^S into which each S carries each C.

$$a)\ 3x_1^2 - 2x_2^2 + 2x_3^2 + 4x_1x_2 - 2x_1x_3 - 2x_2x_3 = 1$$

$$b)\ -4x_1^2 + 11x_3^2 = -6x_1x_2 - 10x_1x_3 - 18x_2x_3 + 1$$

* Observe that a change of bases (47) of L defines a linear transformation of L when we put $u_i^S = u_i^{(0)}$. Thus we may regard a change of basis as being *induced* by a nonsingular linear transformation.

for $k = 1, \ldots, m$ and $l = 1, \ldots, n$. Then $P = (p_{ki})$ and $Q = (q_{li})$ are nonsingular and, as we saw in (3.33), we may also write the second set of equations of (47) in the form

$$v_j = \sum_{l=1}^{n} r_{jl} v_l^{(0)} , \tag{48}$$

where $R = (r_{jl}) = Q^{-1}$. We apply the linearity of S to (47) and obtain $(u_k^{(0)})^S = \sum_{i=1}^{m} p_{ki} u_i^S$. Substituting (43) and (48), we have

$$(u_k^{(0)})^S = \sum_{l=1}^{n} b_{kl} v_l^{(0)} , \tag{49}$$

where $b_{kl} = \Sigma p_{ki} a_{ij} r_{jl}$. Hence the matrix $B = (b_{kl})$ of the linear mapping S with respect to our new bases is given by

$$B = PAQ^{-1} . \tag{50}$$

Since P and Q^{-1} are arbitrary nonsingular matrices of m and n rows, respectively, we see that changes of basis in L and M replace A by an equivalent matrix. Thus any two equivalent m by n matrices define the *same* mapping of L on M.

If L and M are the same space we shall henceforth call a linear mapping S of L on L a *linear transformation* of L. Since we are now considering only a single space, the only possible meaning of the u_i and v_j in (43) can be that of a fixed basis $u_1, \ldots, u_n$ of L of order n over F and of a second basis $v_1, \ldots, v_n$ of L. Let us restrict our attention to the case where $v_i = u_i$. Then we define the matrix A of a linear transformation S on L with respect to a fixed basis $u_1, \ldots, u_n$ of L to be the matrix A determined by (43) with $u_i = v_i$. We have defined thereby a one-to-one correspondence between the set of all n-rowed square matrices with elements in F and the set of all linear transformations on L of order n over F. If $L = V_n$, such a correspondence is given by

$$u \to u^S = uA .$$

Clearly, we should and do call S a *nonsingular linear transformation* if A is nonsingular. Since we may then solve for $u = u^S A^{-1}$, we see that a nonsingular linear transformation defines a one-to-one correspondence of L and itself.

We now observe the effect on A of a change of basis of L. We use (47) but note that $u_i = v_i$ and $u_k^{(0)} = v_k^{(0)}$, so that we have $P = Q$. Hence a change of basis* of L with matrix P replaces the matrix A of a linear transformation by

$$B = PAP^{-1}. \tag{51}$$

It is now clear that in order to study those properties of a linear transformation on L which do not depend on the basis of L over F we need only study those properties of square matrices A which are unchanged when we pass to PAP^{-1}. We shall call two matrices A and B *similar* if (51) holds for a nonsingular matrix P and shall obtain necessary and sufficient conditions that A and B be similar in our next chapter.

EXERCISES

1. Let S be the linear mapping (46) of V_3 on V_4 defined for the following matrices A. Find the vectors of V_4 into which $(-2, 3, 4)$, $(1, 0, 0)$, $(0, 1, 0)$ of V_3 are mapped by S.

$$a)\ A = \begin{pmatrix} 1 & -3 & 0 & 1 \\ 2 & -6 & -1 & 2 \\ -1 & 3 & 1 & -1 \end{pmatrix} \qquad b)\ A = \begin{pmatrix} -2 & 3 & 4 & 0 \\ 1 & 2 & 0 & 4 \\ 0 & 0 & 2 & -3 \end{pmatrix}$$

$$c)\ A = \begin{pmatrix} 2 & -1 & 2 & -5 \\ 0 & -2 & 3 & -2 \\ 1 & 1 & -1 & -1 \end{pmatrix} \qquad d)\ A = \begin{pmatrix} -2 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 1 & 1 & 1 \end{pmatrix}$$

2. Show that the linear transformations (46) of V_3 defined for the following matrices A are nonsingular and find their inverse transformations. Apply both S and S^{-1} to the vectors of Ex. 1.

$$a)\ A = \begin{pmatrix} -4 & 3 & 5 \\ 3 & 0 & 20 \\ 5 & -2 & 11 \end{pmatrix} \qquad b)\ A = \begin{pmatrix} 3 & -1 & -4 \\ 5 & -2 & -1 \\ 2 & -1 & 2 \end{pmatrix}$$

3. Define S for the matrices of Ex. 2 and let C be one or the other of the curves of all vectors (points) $u = (x_1, x_2, x_3)$ whose coordinates satisfy the following equations. Find the equation of the curves C^S into which each S carries each C.

$$a)\ 3x_1^2 - 2x_2^2 + 2x_3^2 + 4x_1x_2 - 2x_1x_3 - 2x_2x_3 = 1$$

$$b)\ -4x_1^2 + 11x_3^2 = -6x_1x_2 - 10x_1x_3 - 18x_2x_3 + 1$$

* Observe that a change of bases (47) of L defines a linear transformation of L when we put $u_i^s = u_i^{(0)}$. Thus we may regard a change of basis as being *induced* by a nonsingular linear transformation.

10. Orthogonal linear transformations. The final topic of our study of linear spaces will be a brief introduction to those linear transformations permitted in what is called *Euclidean geometry*. Let then V_n be the n-dimensional linear space of vectors $u = (c_1, \ldots, c_n)$ over a field F. We define the *norm* of u (*square of the length of* u) to be the value $f(u) = f(c_1, \ldots, c_n)$ of the quadratic form

$$f(x_1, \ldots, x_n) = x_1^2 + \ldots + x_n^2 . \tag{52}$$

We propose to study those linear transformations S on V_n which are said to be *length preserving* and define this concept as the property that $f(u) = f(u^S)$ for every u of V_n. Such transformations S will be called *orthogonal*.

We may define S by $u^S = uA$ for an n-rowed square matrix A. Then, clearly, $f(u) = uu'$, $f(u^S) = u^S(u^S)' = uAA'u'$. Write $B = AA' = (b_{ij})$ and see that $f(u^S) = \Sigma c_i b_{ij} c_j$, $f(u) = \Sigma c_i^2$. Put $c_p = 1$, $c_j = 0$ for $j \neq p$ and have $f(u) = f(u^S)$ only if $b_{ii} = 1$ for every i. Then take $c_p = c_q = 1$, all other $c_j = 0$, from which $f(u) = 2$, $f(u^S) = 2 + 2b_{pq} = f(u)$ only if $b_{pq} = 0$ for a $p \neq q$, $B = I$ is the identity matrix. We call matrices A satisfying

$$AA' = I \tag{53}$$

orthogonal matrices and have shown that S is orthogonal if and only if its matrix is an orthogonal matrix.

We have seen that S determines A uniquely only in terms of a fixed basis of V_n. Now in Euclidean geometry the only changes of basis allowed are those obtained by an orthogonal linear transformation, that is, those for which the matrix P of (51) is orthogonal. But then $PP' = I$, $P' = P^{-1}$, $P'P = I$, so that if S is a linear transformation with orthogonal matrix A and we replace A by $PAP^{-1} = B$, then

$$BB' = (PAP')(PA'P') = PAA'P' = I ,$$

and B is also orthogonal.

EXERCISES

1. What are the possible values of the determinant of an orthogonal matrix?

2. Let I be the identity matrix, A be a skew matrix such that $I + A$ is nonsingular. Show that $(I + A)^{-1}(I - A)$ is orthogonal.

3. Show that every orthogonal two-rowed matrix A has the form

$$\begin{pmatrix} a & b \\ \pm b & \mp a \end{pmatrix} ,$$

where $a = s(s^2 + t^2)^{-1/2}$, $b = t(s^2 + t^2)^{-1/2}$, s and t range over all quantities in F such that $s^2 + t^2 \neq 0$. Hint: The result is trivial if A is a diagonal matrix. Now $a_{11}^2 + a_{12}^2 = 1$ so that $s = a_{11}$, $t = a_{12}$ are of the form above, while, conversely, $a^2 + b^2 = (s^2 + t^2)(s^2 + t^2)^{-1} = 1$. The values $a_{21} = \pm b$, $a_{22} = \mp a$ are derived from $AA' = I$.

4. The equations for rotation of axes in a real Euclidean plane through an angle h are $x = x_0 \cos h - y_0 \sin h$, $y = x_0 \sin h + y_0 \cos h$. Show that the corresponding matrix is orthogonal and that every real orthogonal two-rowed matrix is either the matrix of a rotation or its product by the matrix

$$E = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

of a reflection $x = x_0$, $y = -y_0$.

5. Find a real orthogonal matrix P for each of the following symmetric matrices A such that PAP' is a diagonal matrix. Hint: Compute $PAP' = D = (d_{ij})$ and put $d_{12} = 0$.

$$a) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad b) \begin{pmatrix} 3 & 4 \\ 4 & -3 \end{pmatrix} \qquad c) \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \qquad d) \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}$$

11. Orthogonal spaces. We shall call two vectors u and v of V_n *orthogonal* (that is, in a geometric sense, *perpendicular*) if $uv' = 0$. Then, if A is any orthogonal matrix and we define a linear transformation S of V_n by $u^S = uA$, we have

$$u^S = uA\,, \qquad v^S = vA\,, \qquad u^S(v^S)' = uAA'v' = uv' = 0$$

if and only if $uv' = 0$. Thus orthogonal transformations on V_n preserve orthogonality of vectors of V_n.

If $L = v_1F + \ldots + v_mF$ is a linear subspace of V_n, we define the set $O(L)$ to be the set of all vectors w in V_n such that $vw' = 0$ for every v of L. Then $O(L)$ is a linear subspace of V_n which we shall call the *space orthogonal* in V_n to L. For, clearly, if w_1 and w_2 are in $O(L)$ and a and b are in F, we have $v(aw_1 + bw_2)' = avw_1' + bvw_2' = 0$, $aw_1 + bw_2$ is in $O(L)$. We now prove

Theorem 9. *Let* L *be a linear subspace of order* m *of* V_n. *Then the order of* O(L) *is* n − m.

In fact we shall prove

Theorem 10. *Let* L *be the row space of the* m *by* n *matrix* G *of rank* m *so that* $G = (I_m \quad 0)Q$ *for a nonsingular* n*-rowed matrix* Q. *Then* O(L) *is the row space of* $H = (0 \quad I_{n-m})(Q')^{-1}$ *of rank* n − m.

For proof we first note that the elements of GH' are the products v_iw_j'

of the rows v_i of G by the transposes of the rows w_j of H. But $GH' = (I_m \ 0)[(0 \ I_{n-m})]$, and, clearly, then $GH' = 0$. Let then $O(L) = y_1F + \ldots + y_qF$ of order q over F so that $O(L)$ contains the row space of H. Evidently H has rank $n - m$, and we must have $q \geq n - m$. We let H_0 be the q by n matrix whose kth row is y_k, and we have $GH_0' = 0$, $0 = (I_m \ 0)QH_0'$. The rank of the n by q matrix

$$D = QH_0' = \begin{pmatrix} D_1 \\ D_2 \end{pmatrix}$$

is q since Q is nonsingular. But

$$(I_m \ 0)D = \begin{pmatrix} D_1 \\ 0 \end{pmatrix},$$

so that $D_1 = 0$, D has at most $n - m$ nonzero rows, and D must have rank $q \leq n - m$. This proves that $q = n - m$, the row space of H is $O(L)$.

Note that the row space of H is the set of all solutions $x = (x_1, \ldots, x_n)$ of the homogeneous linear system $Gx' = 0$.

The sum of the orders of L and $O(L)$ is n, and it is natural to ask whether or not they are complementary in V_n, that is, whether $V_n = L + O(L)$. This is not true in general, since if F is the field of all complex numbers and $L = vF$, $i^2 = -1$, $v = (1, i)$, then $vv' = 1 + i^2 = 0$. Hence $O(L)$ is contained in L and $O(L) = L$. However, we may prove

Theorem 11. *Let* F *be a field whose quantities are real numbers. Then* $V_n = L + O(L)$.

For by Theorem 9 it suffices to prove that the only vector w in L and $O(L)$ is the zero vector. Hence let w be in both L and $O(L)$ so that $w = dG$, where $d = (d_1, \ldots, d_m)$ has elements in F and G is an m by n matrix of rank m whose row space is L. Then $Gw' = 0$ while also $Gw' = GG'd'$. By Theorem 3.17 the matrix GG' has rank m and is nonsingular, $GG'd' = 0$ only if $d' = 0$, $d = 0$, $w = 0$ as desired.

EXERCISE

Let L be the space over the field of all real numbers spanned by the following vectors u_i. Find a basis of the space $O(L)$ in the corresponding V_n.

a) $u_1 = (1, 2, -1, 0)$, $u_2 = (0, 1, 2, 1)$

b) $u_1 = (1, 0, 1, 1)$, $u_2 = (0, 1, 0, 1)$, $u_3 = (-1, 2, 1, 0)$

c) $u_1 = (1, -1, 2, 1)$, $u_2 = (2, -1, 2, 3)$, $u_3 = (1, -2, 4, 0)$

d) $u_1 = (1, 2, -1)$, $u_2 = (-1, 1, 0)$, $u_3 = (3, 3, 3)$

CHAPTER V

POLYNOMIALS WITH MATRIC COEFFICIENTS

1. Matrices with polynomial elements. Let F be a field and designate by

$$F[x] \tag{1}$$

(*read:* F bracket x) the set of all polynomials in x with coefficients in F. We shall consider m by n matrices with elements in $F[x]$ and define elementary transformations of three types on such matrices as in Section 2.4. As we stated in that section, we assume that in the elementary transformations of type 2 the quantities c are permitted to be any quantities of $F[x]$. But those of type 3 are restricted so that the quantity a in $F[x]$ shall have an inverse in $F[x]$. Then $a \neq 0$ must be a constant polynomial, that is, a may be any nonzero quantity of F.

We now let A and B be m by n matrices with elements in $F[x]$ and call A and B *equivalent* in $F[x]$ if there exists a sequence of elementary transformations carrying A into B. The field $F(x)$ of all rational functions of x with coefficients in F contains $F[x]$, and it is thus clear that if A and B are equivalent in $F[x]$ they are also equivalent in $F(x)$. Hence we see that A and B are equivalent in $F[x]$ only if they have the same rank. We may then prove

LEMMA 1. *Every nonzero matrix* A *of rank* r *with elements in* F[x] *is equivalent in* F[x] *to*

$$\begin{pmatrix} G_1 & 0 \\ 0 & 0 \end{pmatrix}, \tag{2}$$

where $G_1 = \operatorname{diag}\{f_1, \ldots, f_r\}$ *for monic polynomials* $f_i = f_i(x)$ *such that* f_i *divides* f_{i+1}.

For the elements of all matrices equivalent in $F[x]$ to A are polynomials in x, and in the set of all such polynomials there is a nonzero polynomial $f_1 = f_1(x)$ of lowest degree. Using elementary transformations of types 3 and 1, we may assume that f_1 is monic and is the element in the first row and column of a matrix $C = (c_{ij})$ equivalent in $F[x]$ to A. By the *Division*

Algorithm for polynomials we may write $c_{i1} = q_i f_1 + r_i$ for q_i and r_i in $F[x]$ and r_i of degree less than the degree of f_1. But if we add $-q_i$ times the first row of C to its ith row, we pass to a matrix equivalent in $F[x]$ to A with r_i as the element in its ith row and first column. Our definition of f_1 thus implies that r_i is zero. Moreover, we have now shown A equivalent in $F[x]$ to a matrix $D = (d_{ij})$ with $d_{i1} = 0$ for $i \neq 1$, $d_{11} = f_1$. Similarly, we see that every d_{1i} is divisible by f_1 and hence that A is equivalent in $F[x]$ to a matrix

$$\begin{pmatrix} f_1 & 0 \\ 0 & A_2 \end{pmatrix}, \tag{3}$$

where A_2 has $m - 1$ rows and $n - 1$ columns. Then either $A_2 = 0$, or we may apply the same process to A_2. After a finite number of such steps we ultimately show that A is equivalent in $F[x]$ to a matrix (2) of our lemma such that every $f_i = f_i(x)$ is monic and is a polynomial of least degree in the set of all elements of all matrices equivalent in $F[x]$ to

$$\begin{pmatrix} G_r & 0 \\ 0 & 0 \end{pmatrix}, \qquad G_r = \operatorname{diag}\{f_1, \ldots, f_r\}. \tag{4}$$

Write $f_{i+1} = f_i s_i + t_i$, where s_i and t_i are in $F[x]$ and the degree of t_i is less than the degree of f_i. Then we add the first row of A_i to its second row so that the submatrix in the first two rows and columns of the result is

$$\begin{pmatrix} f_i & 0 \\ f_i & f_{i+1} \end{pmatrix}. \tag{5}$$

We then add $-s_i$ times the first column to the second column to obtain a matrix equivalent in $F[x]$ to A_i and with corresponding submatrix

$$\begin{pmatrix} f_i & -s_i f_i \\ f_i & t_i \end{pmatrix}. \tag{6}$$

Our definition of f_i thus implies that $t_i = 0$, f_i divides f_{i+1} as described.

We observe now that the elements of every t-rowed minor of a matrix A with elements in $F[x]$ are polynomials in x, so that these minors are also

polynomials in x. By Section 2.7 if B is obtained from A by an elementary transformation, then every t-rowed minor of B is either a t-rowed minor of A, the product of a t-rowed minor of A by a quantity a of F, or the sum $M_1 + fM_2$ where M_1 and M_2 are t-rowed minors of A and f is a polynomial of $F[x]$. If d in $F[x]$ then divides every t-rowed minor of A, it also divides every t-rowed minor of all m by n matrices B equivalent in $F[x]$ to A. But A is also equivalent in $F[x]$ to B and therefore the t-rowed minors of equivalent matrices have the same common divisors. We may state this result as

LEMMA 2. *Let* A *be an* m *by* n *matrix with elements in* F[x] *and* d_t *be the greatest common divisor of all* t*-rowed minors of* A. *Then* d_t *is also the greatest common divisor of the* t*-rowed minors of every matrix* B *equivalent in* F[x] *to* A.

Every $(k+1)$-rowed minor M_{k+1} of A may be expanded according to a row and is then a linear combination, with coefficients in $F[x]$, of k-rowed minors of A. Hence d_k divides every M_{k+1} so that d_k divides d_{k+1}. We observe also that in (2) the only nonzero k-rowed minors are the k-rowed minors $|\mathrm{diag}\,\{f_{i_1}, \ldots, f_{i_k}\}|$ for $i_1 < i_2 < \ldots < i_k$, and since clearly every f_i divides f_{i+i} we see that the g.c.d. of all k-rowed minors of (2) is $f_1 \ldots f_k$. We thus have $d_k = f_1 \ldots f_k$, whence

$$\frac{d_k}{d_{k-1}} = f_k. \tag{7}$$

It is customary to relabel the polynomials f_i and thus to write $f_r = g_1$, $f_{r-1} = g_2, f_1 = g_r$. We call g_j the jth *invariant factor* of A and see that if we define $d_0 = 1$ we have the formula

$$g_j = \frac{d_{r-j+1}}{d_{r-j}} \qquad (j = 1, \ldots, r). \tag{8}$$

Moreover, g_j is now divisible by g_{j+1} for $j = 1, \ldots, r-1$. We apply elementary transformations of type 1 to (2) and see that if A has invariant factors $g_1, \ldots, g_r$, then A is equivalent in $F[x]$ to

$$\begin{pmatrix} G & 0 \\ 0 & 0 \end{pmatrix}, \qquad G = \mathrm{diag}\,\{g_1, \ldots, g_r\}. \tag{9}$$

If, then, B is equivalent in $F[x]$ to A, it has the same greatest common divisors d_k and hence the same g_j of (8), while, if the converse holds, B is equivalent in $F[x]$ to (9) and to A. We have proved

Theorem 1. *Two* m *by* n *matrices with elements in* F[x] *are equivalent in* F[x] *if and only if they have the same invariant factors. Every* m *by* n *matrix of rank* r *with invariant factors* $g_1, \ldots, g_r$ *is equivalent in* F[x] *to* (9).

As in our theory of the equivalence of matrices on a field we may obtain a theory of equivalence in $F[x]$ using matrix products instead of elementary transformations. We thus define a matrix P to be an *elementary matrix* if both P and P^{-1} have elements in $F[x]$. Then, if $a = |P|$ and $b = |P^{-1}|$, the quantities a and b are in $F[x]$, $ab = |I| = 1$, so that a and b are nonzero quantities of F. But if P has elements in $F[x]$ so does adj P. Hence so will $P^{-1} = |P|^{-1}$ adj P if $|P|$ is in F. Thus we have proved that *a square matrix* P *with polynomial elements is elementary if and only if its determinant is a constant* (that is, in F) *and not zero.*

We now observe that, in particular, the determinant of any elementary transformation matrix is in F. Hence, if A and B are square matrices with elements in $F[x]$ and are equivalent in $F[x]$, their determinants differ only by a factor in F. Moreover, if $|A|$ and $|B|$ are monic polynomials, then the equivalence of A and B in $F[x]$ implies that $|A| = |B|$ and, in fact, that when A is a nonsingular matrix with $g_1, \ldots, g_n$ as invariant factors its determinant is the product $g_1 \cdots g_n$.

It is clear now that a square matrix P with elements in $F[x]$ is elementary if and only if P is equivalent in $F[x]$ to the identity matrix, and thus the invariant factors of P are all unity. We may now redefine equivalence. We call *two* m *by* n *matrices* A *and* B *with elements in* F[x] *equivalent in* F[x] *if there exist elementary matrices* P *and* Q *such that* PAQ = B. Then we again have the result that A *and* B *are equivalent in* F[x] *if and only if they have the same invariant factors.* For under our first definition P and Q are equivalent in $F[x]$ to identity matrices and hence *may be expressed as products of elementary transformation matrices.* But, if P_0 and Q_0 are elementary transformation matrices, the products P_0A, AQ_0 are the matrices resulting from the application of the corresponding elementary transformations to A. Hence, PAQ must have the same invariant factors as A. The converse is proved similarly, and we have the result desired.

In closing let us note a rather simple polynomial property of invariant factors. The invariant factors of a matrix A with elements in $F[x]$ and rank r are certain monic polynomials $g_i(x)$ such that $g_{i+1}(x)$ divides $g_i(x)$ for $i = 1, \ldots, r-1$. If $g_k(x) = 1$, then $g_j(x) = 1$ for larger $j = k+1, \ldots, r$. Let us then call those $g_i(x) \neq 1$ the *nontrivial invariant factors*

of A, the remaining $g_i(x) = 1$ the *trivial invariant factors* of A. Thus there exists an integer t such that $g_i(x)$ has positive degree for $i = 1, \ldots, t$, $g_{t+1}(x) = \ldots = g_r(x) = 1$.

EXERCISES

1. Express the following matrices as polynomials in x whose coefficients are matrices with constant elements.

$$a)\ \begin{pmatrix} 1+2x & x^3+4x^2+x+2 & x^3+4x+2 \\ 0 & x^2+x & x^2 \\ 1-2x & x^3+3x^2-3x-1 & x^3-x^2+4x-2 \end{pmatrix}$$

$$b)\ \begin{pmatrix} x^2 & x & x^2-2x \\ x^2-1 & 1+x & x^2-2x-3 \\ x^3+2x^2-2 & x^2+2x+2 & x^3-4x-6 \end{pmatrix}$$

$$c)\ \begin{pmatrix} x^3+x^2-2x & x^2-x^3 & x^3+x \\ x^3 & x-x^3 & x^3 \\ 2x^3+x^2-2x+1 & x^2-x-1 & x+1 \end{pmatrix}$$

$$d)\ \begin{pmatrix} x^2+x & x & x^2+x \\ x^2+x & x+1 & x^2+x \\ x^2-1 & 2x & 2x^2+2 \end{pmatrix}$$

2. Let A be an m by n matrix whose elements are in $F[x]$. Describe a process by means of which we may use elementary row transformations involving only the ith and kth rows of A to replace A by a matrix with the g.c.d. of a_{ij} and a_{kj} in its ith row and jth column. Hint: Use the g.c.d. process of Section 1.6 with $f = a_{ij}$, $g = a_{kj}$.

3. Use elementary transformations to carry the following matrices into the form (9).

$$a)\ \begin{pmatrix} x & 0 \\ 0 & x+1 \end{pmatrix} \qquad b)\ \begin{pmatrix} x(x-1) & 0 \\ 0 & x(x+1) \end{pmatrix} \qquad c)\ \begin{pmatrix} x^2+x-2 & 0 \\ 0 & x^2+2x-3 \end{pmatrix}$$

4. Describe a process for reducing a matrix A with elements in $F[x]$ to an equivalent diagonal matrix. How, then, may we use the process of Ex. 3 to carry this preliminary diagonal matrix into the form (9)?

5. Reduce the matrices of Ex. 1 to the form (9) by the use of elementary transformations.

6. Determine the invariant factors of the matrices of Ex. 1 by the use of (8).

7. Use elementary transformations to reduce the following matrices to the form (9).

a) $\begin{pmatrix} x^2 & 1 & x^2 - x^3 & x - x^2 - 2 \\ 0 & 1 & x^2 & x - 2 \\ x^3 & -x & 2 + x - x^3 - x^4 & 1 + 2x - x^2 - x^3 \\ 2x^3 & 1 & 2 + x + x^2 - 2x^4 & -1 + x - 2x^3 \end{pmatrix}$

b) $\begin{pmatrix} x^2 & -2x & 2x - 2 & x^2 - 2 \\ 4x + 4 & 3x + 2 & -3x & 4x + 6 \\ x & x & 1 - x & x + 1 \\ 4x^2 + 4x & 2x^2 & -2x^2 + x - 2 & 4x^2 + 5x - 2 \end{pmatrix}$

c) $\begin{pmatrix} x + 3 & 3x^2 + 3x & 2x + 3 & x + 3 \\ x & 2x^2 & 2x & x \\ 1 + x - x^3 & 3x^2 + x & 2x + 1 & x + 1 \\ x^3 - x + 1 & x - 2x^2 & 1 - 2x & 1 - x \end{pmatrix}$

d) $\begin{pmatrix} -x & 2x + 1 & x - 1 & x + 1 \\ 2 - x & x - 1 & x + 2 & x - 2 \\ -3 - 2x & 3x + 4 & x & 2x + 4 \\ -x^2 + x - 1 & x^2 + x + 2 & x^2 + 3x - 1 & x^2 - x + 2 \end{pmatrix}$

e) $\begin{pmatrix} 2x^2 + 4x + 2 & -x & 2x^2 + 3x + 1 & x^2 - x - 1 \\ x^2 + x - 3 & 5x^2 + 2x & x^2 - 1 & 6x^2 + 5x + 2 \\ 3x + 6 & -2x^2 + x & 3x + 3 & -2x^2 + 2x + 1 \\ x + 2 & -x^2 & x + 1 & -x^2 \end{pmatrix}$

2. Elementary divisors. Let K be the field of all complex numbers so that

$$g_1(x) = (x - c_1)^{e_1} \dots (x - c_s)^{e_s},$$

where $c_1, \dots, c_s$ are the distinct complex roots of the first invariant factor of a matrix A with elements in $K[x]$. Since $g_{i+1}(x)$ divides $g_i(x)$, it is clear that every $g_i(x)$ divides $g_1(x)$, and thus

$$g_i(x) = (x - c_1)^{e_{i1}} \dots (x - c_s)^{e_{is}} \qquad (i = 1, \dots, r). \tag{10}$$

Here r is the number of invariant factors of A, $e_{1j} = e_j$, $e_{ij} \geqq 0$ for $i = 2, \dots, r$. We shall call the rs polynomials

$$f_{ij} = (x - c_j)^{e_{ij}}$$

the *elementary divisors* of A. Those for which $e_{ij} > 0$ will be called the *nontrivial elementary divisors* of A.

The invariant factors of A clearly determine its elementary divisors uniquely as certain rs powers f_{ij} of linear functions $x - c_j$ where r is the rank of A, and s is the number of distinct roots of the invariant factors of A. Conversely, the elementary divisors of A uniquely determine its invariant factors. In fact, let us consider a set of q polynomials each a power with positive integral exponent of a monic linear factor with a complex root. The distinct roots in our set may then be labeled $c_1, \ldots, c_s$ and our polynomials have the form $h_{kj} = (x - c_j)^{n_{ij}}$ for $n_{ij} > 0$. For each c_j let t_j be the number of h_{kj} in our set, t be the maximum t_j. Then, clearly, $q = t_1 + \ldots + t_s \leqq ts$, and our set of polynomials may be extended to a set of exactly ts polynomials by adjoining $t - t_j$ polynomials $(x - c_j)^{n_{ij}}$ with $n_{ij} = 0$. Let us then order the t exponents n_{ij} to be integers e_{ij} satisfying $e_{1j} \geqq e_{2j} \geqq \ldots \geqq e_{tj} \geqq 0$. Define $g_i(x)$ as in (10) for $i = 1, \ldots, t$ and obtain a set of polynomials $g_i(x)$ such that $g_{i+1}(x)$ divides $g_i(x)$ for $i = 1, \ldots, t - 1$, the $g_i(x)$ are the nontrivial invariant factors of a matrix A whose nontrivial elementary divisors are the given h_{kj}. If A has rank r, we have $r \geqq t$, and we adjoin $(r - t)s$ new trivial elementary divisors f_{ij} to obtain the complete set of r invariant factors $g_i(x)$ of A.

It is now evident that *two* m *by* n *matrices with elements in* K[x] *are equivalent in* K[x] *if and only if they have the same elementary divisors.*

The matrix (9) has prescribed invariant factors and hence prescribed elementary divisors. However, it is desirable to obtain a matrix of a form exhibiting the elementary divisors explicitly. We shall do this. Let us prove first

Theorem 2. *Let* $\mathrm{f}_1, \ldots, \mathrm{f}_s$ *be monic polynomials of* F[x] *which are relatively prime in pairs. Then the only nontrivial invariant factor of the matrix* $\mathrm{A} = \mathrm{diag}\,\{\mathrm{f}_1, \ldots, \mathrm{f}_s\}$ *is its determinant* $\mathrm{g} = \mathrm{f}_1 \ldots \mathrm{f}_s$.

The result is trivial for $s = 1$. If $s = 2$, the g.c.d. of the elements f_1 and f_2 of $A_2 = \mathrm{diag}\,\{f_1, f_2\}$ is unity, $d_1 = 1, f_1 f_2$ is the only nontrivial invariant factor of A_2, and A_2 is equivalent in $F[x]$ to $\mathrm{diag}\,\{\mathrm{f}_1\mathrm{f}_2, 1\}$. Assume, then, that $A_{s-1} = \mathrm{diag}\,\{f_1, \ldots, f_{s-1}\}$ is equivalent in $F[x]$ to $B_{s-1} = \mathrm{diag}\,\{g_{s-1}, 1, \ldots, 1\}$, where $g_{s-1} = f_1 \ldots f_{s-1}$. Then $A = \mathrm{diag}\,\{f_1, \ldots, f_s\}$ is equivalent in $F[x]$ to $\mathrm{diag}\,\{g_{s-1}, f_s, 1, \ldots, 1\}$. But g_{s-1} is prime to f_s, $\mathrm{diag}\,\{g_{s-1}, f_s\}$ is equivalent in $F[x]$ to $\mathrm{diag}\,\{g, 1\}$. Hence A is equivalent to $\mathrm{diag}\,\{g, 1, \ldots, 1\}$. Then g is the only nontrivial invariant factor of A, and our theorem is proved.

We see now that if $g_i(x)$ is defined by (10) for distinct complex numbers c_j, the corresponding elementary divisors $f_{i1}, \ldots, f_{is}$ are relatively prime in pairs. By Theorem 2 the matrix $A_i = \mathrm{diag}\,\{f_{i1}, \ldots, f_{is}\}$ is equivalent in $F[x]$ to $\mathrm{diag}\,\{g_i, 1, \ldots, 1\}$. But then $A = \mathrm{diag}\,\{A_1, \ldots, A_t\}$ is equiv-

alent in $F[x]$ to diag $\{g_1, \ldots, g_t, 1, \ldots, 1\}$, and hence the nontrivial invariant factors of A are $g_1, \ldots, g_t$. We examine the form of A to see that we have proved

Theorem 3. *Let* $c_1, \ldots, c_r$ *be complex numbers and* $f_i = (x - c_i)^{n_i}$ *for integers* $n_i \geqq 0$. *Then the matrix*

$$A = \text{diag } \{f_1, \ldots, f_r\}$$

has the f_i *as its elementary divisors.*

EXERCISES

1. The following polynomials are the nontrivial invariant factors of a matrix. What are its nontrivial elementary divisors?

a) $x^5 + 2x^4 + x^3, \quad x^3 + x^2, \quad x^2 + x$

b) $x^6 + x^5 + 2x^4 + 2x^3 + x^2 + x, \quad x^3 + x, \quad x$

c) $x(x-1)^2 \quad (x^2 - 2x + 1), \quad x^3 - 2x^2 + x, \quad x - 1$

d) $x^4 - 5x^3 + 9x^2 - 7x + 2, \quad x^3 - 4x^2 + 5x - 2, \quad x^2 - 3x + 2$

e) $(x^2 - 1)^3, \quad (x^2 - 1)^2, \quad (x^2 - 1), \quad x - 1$

f) $(x^2 + 1)^4, \quad (x^2 + 1)^3, \quad x^2 + 1$

2. The following polynomials are the nontrivial elementary divisors of a matrix whose rank is six. What are its invariant factors?

a) $(x-1)^3, \quad (x-1)^2, \quad (x-1), \quad (x+1)^2, \quad (x+1)$

b) $(x-2)^4, \quad (x-2)^3, \quad (x-2), \quad x, \quad (x+1)^2, \quad x^2$

c) $(x-3), \quad (x-3)^3, \quad (x-3)^5, \quad x^2, \quad x^4, \quad x^6$

d) $x, \quad (x-1), \quad (x-2), \quad (x-3), \quad (x-4), \quad (x-5)$

e) $(x+1)^3, \quad (x+1)^2, \quad (x-1), \quad x, \quad x^2, \quad x^3, \quad x^3$

f) $x, \quad (x-1), \quad x^2, \quad (x-1)^2, \quad x^3, \quad (x+1)^4, \quad x^2$

3. Find elementary transformations which carry the following matrices into the form (9).

$$a) \begin{pmatrix} (x-1)^3 & 0 & 0 \\ 0 & x-2 & 0 \\ 0 & 0 & x-1 \end{pmatrix} \qquad b) \begin{pmatrix} x^3 & 0 & 0 \\ 0 & x+1 & 0 \\ 0 & 0 & x+2 \end{pmatrix}$$

$$c) \begin{pmatrix} x^3 & 0 & 0 \\ 0 & (x-1)^2 & 0 \\ 0 & 0 & x+1 \end{pmatrix}$$

3. Matric polynomials. Let the elements a_{ij} of an m by n matrix A be in $F[x]$ and let s be a positive integer not less than the degree of any of the a_{ij}. Then every a_{ij} has s as a virtual degree and we may write

$$a_{ij} = a_{ij}^{(0)}x^s + a_{ij}^{(1)}x^{s-1} + \ldots + a_{ij}^{(s)} \tag{11}$$

for $a_{ij}^{(k)}$ in F. Define $A_k = (a_{ij}^{(k)})$ and obtain an expression of A in the form

$$f(x) = A_0x^s + \ldots + A_s \tag{12}$$

for m by n matrices A_k. Thus $f(x)$ is a polynomial in x of virtual degree s *with* m *by* n *matrix coefficients* A_k and virtual leading coefficient A_0. Moreover, we say that $f(x)$ has *degree* s and *leading coefficient* A_0 if $A_0 \neq 0$.

In order to be able to multiply as well as to add our matrices we shall henceforth restrict our attention to n-rowed square matrices with elements in $F[x]$ and thus to the set of all polynomials in x with coefficients n-rowed square matrices having elements in F. Let us call these polynomials n-rowed matric polynomials. If all the A_k in (11) are zero matrices, the polynomial $f(x)$ is the zero polynomial, and we again designate it by 0. Evidently we have

LEMMA 3. *The degree of* $f(x) + g(x)$ *is not greater than the degree of* $f(x)$ *or* $g(x)$.

LEMMA 4. *Let* $f(x)$ *have degree* n *and leading coefficient* A_0, $g(x)$ *have degree* m *and leading coefficient* B_0 *such that* $A_0B_0 \neq 0$. *Then the degree of* $f(x)g(x)$ *is* $m + n$ *and the leading coefficient of* $f(x)g(x)$ *is* A_0B_0.

As in Chapter I we use Lemma 4 in the derivation of the *Division Algorithm* for matric polynomials which we state as

Theorem 4. *Let* $f(x)$ *and* $g(x)$ *be* n*-rowed matric polynomials of respective degrees* s *and* t *such that the leading coefficient of* $g(x)$ *is nonsingular. Then there exist unique polynomials* $q(x)$, $Q(x)$, $r(x)$, $R(x)$ *such that* $r(x)$ *and* $R(x)$ *have virtual degree* $t - 1$ *and*

$$f(x) = q(x)g(x) + r(x) = g(x)Q(x) + R(x)\,. \tag{13}$$

Moreover, if $s < t$, *then* $q(x) = Q(x) = 0$, *while if* $s \geqq t$, *then* $q(x)$ *and* $Q(x)$ *have degree* $s - t$.

While the proof is very much the same as that in Theorem 1.1, let us give it in some detail. We assume first that $s \geqq t$ and let $A_0 \neq 0$ and B_0 be the respective leading coefficients of $f(x)$ and $g(x)$. Then B_0^{-1} exists, and if $q_1(x) = A_0B_0^{-1}x^{s-t}$ the polynomial $f_1(x) = f(x) - q_1(x)g(x)$ has virtual de-

gree $s-1$. This implies a finite process by means of which we begin with a polynomial $f_i(x)$ of virtual degree $s-i \geqq t$ and leading coefficient $A_0^{(i)}$ and then form $f_{i+1}(x) = f_i(x) - q_{i+1}(x)g(x)$ of virtual degree $s-i-1$ for $q_{i+1}(x) = A_0^{(i)}B_0^{-1}x^{s-i-t}$. The process terminates when we obtain an $f_j(x)$ of virtual degree $t-1$. Thus we have the first equation of (13) with $q(x) = 0$, $r(x) = f(x)$ if $s < t$, and otherwise with $q(x)$ of degree $s-t$ and leading coefficient $A_0B_0^{-1}$ and $r(x)$ the $f_j(x)$ above. If also $f(x) = q_0(x)g(x) + r_0(x)$ for $q_0(x) - q(x) \neq 0$, the degree of this polynomial is $h \geqq 0$, and its leading coefficient is $C_0 \neq 0$. Also $C_0B_0 \neq 0$ since B_0 is nonsingular. But then by Lemma 4 the degree of $[q_0(x) - q(x)]g(x) = r(x) - r_0(x)$ is $t+h$, whereas its virtual degree is $t-1$, a contradiction. This proves the uniqueness of $g(x)$ and $r(x)$. The existence and uniqueness of $Q(x)$ and $R(x)$ is proved in exactly the same way except that we begin by forming $f(x) - g(x)B_0^{-1}A_0x^{s-t}$.

Let us regard the first equation of (13) as the *right division* of $f(x)$ by $g(x)$, the second as the *left division* of $f(x)$ by $g(x)$. Then we shall speak correspondingly of $q(x)$ and $r(x)$ as *right quotient* and *remainder*, of $Q(x)$ and $R(x)$ as *left quotient* and *remainder*. If $r(x) = 0$, we have $f(x) = q(x)g(x)$, and $g(x)$ is a *right divisor* of $f(x)$. Similarly, we call $g(x)$ a *left divisor* of $g(x)$ if $f(x) = g(x)Q(x)$, so that $R(x) = 0$ in (13).

It is natural now to try to prove a *Remainder Theorem* for matric polynomials. However, the theorem in usual form is ambiguous since, for example, if C is an n-rowed square matrix and $f(x) = A_0x^2 = x^2A_0 = xA_0x$, the polynomial $f(C)$ might mean any one of A_0C^2, C^2A_0, CA_0C, and these matrices might all be different. Thus we must first define what we shall mean by $f(C)$. We shall do this and obtain a *Remainder Theorem* which we state as

Theorem 5. *Let* $\mathrm{f(x)}$ *be an* n*-rowed square matric polynomial* (12), C *be an* n*-rowed square matrix with elements in* F. *Define* $\mathrm{f_R(C)}$ (*read:* f *right of* C), *and* $\mathrm{f_L(C)}$ (*read:* f *left of* C) *by*

$$\mathrm{f_R(C) = A_0C^s + A_1C^{s-1} + \ldots + A_{s-1}C + A_s}, \tag{14}$$

and

$$\mathrm{f_L(C) = C^sA_0 + C^{s-1}A_1 + \ldots + CA_{s-1} + A_s}. \tag{15}$$

Then the right and left remainders on division of $\mathrm{f(x)}$ *by* $\mathrm{xI - C}$ *are* $\mathrm{f_R(C)}$ *and* $\mathrm{f_L(C)}$, *respectively.*

To make our proof as in the case of polynomials with coefficients in a field we use Theorem 4 with $g(x) = xI - C$ and have $f(x) = q(x)g(x) + r(x)$ where $q(x)$ has degree $s - 1$ and $r(x) = B$ has elements in F. We then wish to draw our conclusion from $f_R(C) = q_R(C)(C - C) + B$. This statement is correct, but let us examine it more closely. We write $q(x) = C_0x^{s-1} + \ldots + C_{s-1}$ and have

$$h(x) = q(x)(xI - C)$$
$$= (C_0x^s + C_1x^{s-1} + \ldots + C_{s-1}x) - (C_0Cx^{s-1} + \ldots + C_{s-1}C).$$

Then, if D is any n-rowed square matrix with elements in F, we have

$$h_R(D) = C_0D^s + (C_1 - C_0C)D^{s-1} + \ldots + (C_{s-1} - C_{s-2}C)D - C_{s-1}C,$$

while

$$q_R(D)(DI - C) = C_0D^s + (C_1D^{s-1} - C_0D^{s-1}C) + \ldots$$
$$+ (C_{s-1}D - C_{s-2}DC) - C_{s-1}C,$$

and these matrices are equal in general* if and only if D and C are commutative. They are equal if $D = C$, and thus $f(x) = h(x) + B$ implies that $f_R(C) = h_R(C) + B = q_R(C)(C - C) + B = B$. The second part of our theorem is proved similarly.

As a consequence of the result just proved we have the *Factor Theorem* for matric polynomials which we state as

Theorem 6. *The matric polynomial* f(x) *has* xI − C *as a right divisor if and only if* $f_R(C) = 0$; *it has* xI − C *as a left divisor if and only if* $f_L(C) = 0$.

For Theorem 5 implies that, if $f_R(C) = 0$, then in (12) the polynomial $r(x) = 0$, $f(x) = q(x)(xI - C)$. Conversely, if $f(x) = q(x)(xI - C)$, we have seen that $f_R(C) = q_R(C)(CI - C) = 0$. The results on the left follow similarly.

Our principal use of the result above is precisely what is usually called the trivial part of Theorem 5, that is, if $f(x)$ has $x - C$ as a factor, then C is a root of $f(x)$. However, it is nontrivial that $f_R(C) = 0$ and follows only from the study above where we showed that if D is any square matrix such that $DC = CD$, then $h(x) = q(x)(xI - C)$ implies that $h_R(D) = q_R(D)(D - C)$.

* E.g., if $q(x) = x$ so that $h(x) = x^2 - Cx$, then $h_R(D) = D^2 - CD$, $q_R(D)(D - C) = D^2 - DC \neq D^2 - CD$ unless $DC = CD$.

EXERCISES

1. Express the following matrices as polynomials $f(x)$ and $g(x)$ with matric coefficients and compute $q(x)$, $Q(x)$, $r(x)$, $R(x)$ of (13).

a) $f(x) = \begin{pmatrix} x^3+5x+1 & 3x^3+x-1 \\ 2x^3+x^2+2 & 4x^3+2x+2 \end{pmatrix}$, $\quad g(x) = \begin{pmatrix} 2x^2-1 & x^2 \\ 3x^2 & 2x^2 \end{pmatrix}$

b) $f(x) = \begin{pmatrix} x^4+3x^2-1 & x^3-1 \\ x^2+1 & x^3+1 \end{pmatrix}$, $\quad g(x) = \begin{pmatrix} 3x^2+x & -2x^3+x+1 \\ -x^2+2x & x^2+x \end{pmatrix}$

c) $f(x) = \begin{pmatrix} 2x^4-x^2+2 & -x^3+x-1 & 1-x^2 \\ x^3-x+1 & -x^4+x^2-2 & 1+x \\ x^2-1 & -1-x & x^4+x^2-1 \end{pmatrix}$,

$$g(x) = \begin{pmatrix} x^2+2x+1 & x^2-1 & x^2+1 \\ 1-x & 2x^2+x & x^2-1 \\ 2x & x^2+1 & x^2+2x \end{pmatrix}$$

d) $f(x) = \begin{pmatrix} x+2 & 2x^2+1 & x^3 & 3x^3 \\ x & 2x & 2x^3 & 5x^3 \\ 2x^3-1 & x^3+x & 3 & -2 \\ x^3-1 & x^3+1 & -2 & 1 \end{pmatrix}$,

$$g(x) = \begin{pmatrix} -1 & 2 & 2x^2-x & 3x^2+1 \\ 3 & 4 & x^2-1 & x^2+x \\ 2x^2+x & 3x^2 & 1 & 2 \\ x^2 & 2x^2-x & 3 & 5 \end{pmatrix}$$

2. Use $f(x)$ of Ex. 1(c) and find $f_R(C)$ and $f_L(C)$ by the use of the division process as well as by substitution if

a) $C = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 0 \end{pmatrix}$ $\quad$ b) $C = \begin{pmatrix} 0 & 2 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ $\quad$ c) $C = \begin{pmatrix} 1 & 2 & 0 \\ 2 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

4. The characteristic matrix and function. If $f(x)$ is a matric polynomial (12) with n-rowed scalar matrix coefficients A_k, then we shall call $f(x)$ a *scalar polynomial*. Thus $A_k = a_k I$ for the a_k in F, and

$$f(x) = (a_0 x^s + \ldots + a_s) I \,, \tag{16}$$

where I is the n-rowed identity matrix. We call $f(x)$ *monic* if $a_0 = 1$. If now $g(x)$ is also a scalar polynomial, the quotients $q(x)$ and $Q(x)$ in (13) are the same scalar polynomials and also $r(x) = R(x)$ is scalar. For obviously this case of Theorem 4 is now the result of multiplying all the polynomials of Theorem 1.1 by the n-rowed identity matrix.

If A is any n-rowed square matrix, the polynomials $f_R(A)$ and $f_L(A)$ are equal for every scalar polynomial $f(x)$, and we shall designate their common value by

$$f(A) = a_0A^s + \ldots + a_{s-1}A + a_sI\,. \tag{17}$$

We now say that either the polynomial $f(x)$ or the equation $f(x) = 0$ has A as a root if $f(A) = 0$. By Theorem 6 the matrix A is a root of $f(x)$ if and only if $f(x)$ has $xI - A$ as either a right- or a left-hand factor.

We shall call the matrix $xI - A$ the *characteristic matrix* of A, the determinant $|xI - A|$ the *characteristic determinant* of A, the scalar polynomial

$$f(x) = |xI - A| \cdot I \tag{18}$$

the *characteristic function* of A, and the corresponding equation $f(x) = 0$ the *characteristic equation* of A. We now apply (3.27) to $xI - A$ to obtain

$$(xI - A)[\text{adj } (xI - A)] = [\text{adj } (xI - A)](xI - A) = |xI - A| \cdot I\,. \tag{19}$$

Then the elements of adj $(xI - A)$ are the cofactors of the elements of $xI - A$, and adj $(xI - A)$ is a matric polynomial (in general, nonscalar). By the argument above we have

Theorem 7. *Every square matrix is a root of its characteristic equation.*

The g.c.d. of the elements of adj $(xI - A)$ is clearly the polynomial $d_{n-1}(x)$ defined for $xI - A$ and $d_n(x) = |xI - A|$. But then adj $(xI - A) = d_{n-1}(x)B(x)$, where $B(x)$ is an n-rowed square matrix with elements in $F[x]$. Hence $B(x)$ is a matric polynomial. The invariant factors of $xI - A$ were defined in (8), and by (19) $|xI - A|I = g_1(x)d_{n-1}(x)I = (xI - A)B(x)d_{n-1}(x)$. By the uniqueness of quotient in Theorem 4 we have

$$g(x) = g_1(x)I = (xI - A)B(x)\,. \tag{20}$$

Hence, clearly, $g(A) = 0$. Observe also that the g.c.d. of the elements of $B(x)$ is unity so that if $B(x) = Q(x)q(x)$ for a monic scalar polynomial $q(x)$, then $q(x) = 1$.

We now define the *minimum function* of a square matrix A to be the *monic scalar polynomial of least degree with* A *as a root.* The remark just made above then implies

Theorem 8. *Let* $g_1(x)$ *be the first invariant factor of the characteristic matrix of* A. *Then* $g(x) = g_1(x)I$ *is the minimum function of* A.

For if $h(x)$ is the minimum function of A we may write $g(x) = h(x)q(x) + r(x)$ for scalar polynomials $h(x)$ and $r(x)$ such that the degree of $r(x)$ is less than that of $h(x)$. But $h(A) = 0$, and $g(A) = 0$ so that $r(A) = 0, r(x) = 0$. Hence $g(x) = h(x)q(x)$, and since $g(x)$ and $h(x)$ are monic so is $q(x)$. By Theorem 6 we have $h(x) = (xI - A)Q(x)$, and by (20) we have $g(x) = (xI - A)Q(x)q(x) = (xI - A)B(x)$. The uniqueness in Theorem 4 then states that $B(x) = Q(x)q(x)$, $q(x) = 1$, from which $g(x) = h(x)$ as desired.

We see now that $|xI - A|$ is a monic polynomial of degree n and is not zero, $r = m = n$ in (9), and

$$P(x) \cdot (xI - A) \cdot Q(x) = \text{diag}\,\{g_1, \ldots, g_n\} \tag{21}$$

for elementary matrices $P(x)$ and $Q(x)$. But then, as we have already observed in an earlier discussion,

$$c \cdot |xI - A| \cdot d = g_1 \ldots g_n \tag{22}$$

for $c = |P(x)|$ and $d = |Q(x)|$ in F. Hence $cd = 1$, and we have proved

Theorem 9. *The characteristic function of a square matrix* A *is the product by* I *of the product of the invariant factors of the characteristic matrix of* A.

This result implies that $|xI - A|$ is the product of $g_1(x)$ by divisors $g_i(x)$ of $g_1(x)$. It follows that every root of $|xI - A|$ in any field K containing F is a root of $g_1(x)$. But in fact we have already seen that if F is the field of all complex numbers, the elementary divisors of $xI - A$ are polynomials $(x - c_i)^{e_{ij}}$ whose product is $|xI - A|$. Then the c_i are the distinct roots of $g_1(x)$ as well as of $|xI - A|$. They are called the *characteristic roots* of A.

In closing this section we note that if we write $f(x) = |xI - A| \cdot I = (x^n + a_1x^{n-1} + \ldots + a_n)\,I$, then $f(0) = |-A| \cdot I = (-1)^n|A| \cdot I$, so that $|A| = (-1)^n a_n$. It follows that, if $|A| \neq 0$, then

$$A^{-1} = -a_n^{-1}(A^{n-1} + a_1A^{n-2} + \ldots + a_{n-1} \cdot I)\,, \tag{23}$$

and hence it is obvious that $AA^{-1} = A^{-1}A$. Moreover, if $|A| = 0$, then A^{-1} does not exist. If, then, $A \neq 0$ and $g_1(x) = x^m + b_1x^{m-1} + \ldots + b_m$, the polynomial $g(x) = g_1(x)I$ can be the minimum function of A only if $b_m = 0$. Since $A \neq 0$, we have $m > 1$, and $G = A^{m-1} + b_1A^{m-2} + \ldots + b_{m-1}I$ is a nonzero matrix with the property

$$AG = GA = 0\,. \tag{24}$$

EXERCISES

1. When is the minimum function of a matrix linear?

2. What, then, are the minimum functions of the following matrices?

$$a)\ \begin{pmatrix} 2 & 3 \\ 1 & -2 \end{pmatrix} \qquad b)\ \begin{pmatrix} 0 & 1 \\ b & a \end{pmatrix} \qquad c)\ \begin{pmatrix} 2 & 3 \\ 4 & 1 \end{pmatrix} \qquad d)\ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

3. Let $A = \operatorname{diag}\{A_1, A_2\}$ where A_1 and A_2 are square matrices of m and n rows respectively. Show that if $f(x)$ is any polynomial in $F[x]$ and we define $f_t(x) = f(x)I_t$ for any t, then $f_{m+n}(A) = \operatorname{diag}\{f_m(A_1), f_n(A_2)\}$. Hint: Prove first by induction that $A^k = \operatorname{diag}\{A_1^k, A_2^k\}$.

4. Let A have the form of Ex. 3 and let $g(x)I_{m+n}$, $g_1(x)I_m$, and $g_2(x)I_n$ be the respective minimum functions of A, A_1, A_2. Prove that $g(x)$ is the least common multiple of $g_1(x)$ and $g_2(x)$.

5. Apply Ex. 4 in the case where A_1 is nonsingular and $A_2 = 0$.

6. Compute the characteristic functions of the following matrices.

$$a)\ \begin{pmatrix} 1 & 2 & 3 \\ 2 & -1 & 4 \\ 3 & 1 & 1 \end{pmatrix} \qquad b)\ \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 1 \\ 0 & 0 & -4 \end{pmatrix}$$

$$c)\ \begin{pmatrix} 0 & -1 & 2 & -3 \\ 1 & 0 & 3 & -2 \\ -2 & -3 & 0 & 1 \\ 3 & 2 & -1 & 0 \end{pmatrix} \qquad d)\ \begin{pmatrix} 1 & 2 & 3 & 1 \\ 3 & 2 & 1 & 0 \\ 2 & 1 & -1 & -2 \\ -1 & 0 & -2 & -5 \end{pmatrix}$$

7. It may be shown that the characteristic function $f(x) = x^n - a_1x^{n-1} + \ldots + (-1)^i a_i x^{n-i} + \ldots + (-1)^n a_n$ of an n-rowed square matrix A has the property that a_i is the sum of all i-rowed principal minors of A. Verify this for the matrices of Ex. 6.

5. Similarity of square matrices. We have defined two n-rowed square matrices A and B with elements in a field F to be *similar* in F if there exists a nonsingular matrix P with elements in F such that

$$PAP^{-1} = B\,.$$

The principal result on the similarity of square matrices is then given by

Theorem 10. *Two matrices are similar in* F *if and only if their characteristic matrices have the same invariant factors.*

For if $PAP^{-1} = B$, then $P(xI - A)P^{-1} = xPIP^{-1} - B = xI - B$. But P has elements in F, $|P| \neq 0$ is in F, P is elementary. Hence $xI - A$

and $xI - B$ are equivalent in $F[x]$ and have the same invariant factors. Conversely, let $xI - A$ and $xI - B$ have the same invariant factors, so that

$$P(x)[xI - A]Q(x) = xI - B \tag{25}$$

for elementary matrices $P(x)$ and $Q(x)$. We define

$$P = P_L(B), \qquad Q = Q_R(B) \tag{26}$$

as in Theorem 5 and have

$$P(x) = (xI - B)P_0(x) + P, \qquad Q(x) = Q_0(x)(xI - B) + Q. \tag{27}$$

Then

$$\begin{aligned} P(x)[(xI - A)]Q(x) &= (xI - B)P_0(x)(xI - A)Q(x) + \\ &\quad P \cdot (xI - A) \cdot Q_0(x)(xI - B) + P \cdot (xI - A) \cdot Q = xI - B. \end{aligned}$$

We now use (25) and the fact that $P(x)$ and $Q(x)$ are elementary to write $[P(x)]^{-1} = C(x)$, $Q(x)^{-1} = D(x)$ for matrix polynomials $C(x)$ and $D(x)$ such that

$$(xI - A)Q(x) = C(x)(xI - B), \qquad P(x)(xI - A) = (xI - B)D(x). \tag{28}$$

But then from (27) and (28)

$$P \cdot (xI - A) = (xI - B)[D(x) - P_0(x)(xI - A)]$$

and thus

$$(xI - B) - P \cdot (xI - A) \cdot Q = (xI - B)R(xI - B), \tag{29}$$

where $R = R(x) = P_0(x)C(x) + D(x)Q_0(x) - P_0(x)(xI - A)Q_0(x)$. By Lemma 4 the degree in x of the right member of (29) is at least two unless $R(x) = 0$. But the degree in x of the left member of (29) is at most one, $R(x) = 0$,

$$P \cdot (xI - A) \cdot Q = xI - B. \tag{30}$$

It follows that $PAQ = B$, $PIQ = I$, $Q = P^{-1}$, $PAP^{-1} = B$ as desired.

Observe that the degree of $|xI - A|$ is n and hence that if n_i is the degree of the ith nontrivial invariant factor $g_i(x)$ the property $|xI - A| = g_1(x) \ldots g_t(x)$ implies that

$$n_1 + n_2 + \ldots + n_t = n, \qquad n_1 \geqq n_2 \geqq \ldots \geqq n_t = 0. \tag{31}$$

Obviously, this is an important restriction on the possible degrees of the invariant factors of the characteristic matrix of an n-rowed square matrix.

EXERCISES

1. What are all possible types of invariant factors of the characteristic matrices of square matrices having 1, 2, 3, or 4 rows?

2. Give the possible elementary divisors of such matrices.

3. Use the proof of Theorem 10 to show that if A_1, A_2, B_1, and B_2 are n-rowed square matrices such that A_1 and B_1 are nonsingular, then $A_1x + A_2$ and $B_1x + B_2$ are equivalent in $F[x]$ if and only if there exist nonsingular matrices P and Q with elements in F such that $PA_1Q = B_1$ and $PA_2Q = B_2$. Hint: Take $A = -A_1^{-1}A_2$, $B = -B_1^{-1}B_2$ in (25).

4. Show that the hypothesis that A_1 is nonsingular in Ex. 3 is essential by proving that $A_1x - I$ and $B_1x - I$ are equivalent in $F[x]$, yet P and Q do not exist, if

$$A_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad B_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

6. Characteristic matrices with prescribed invariant factors. If $g_1(x)$, $\ldots$, $g_t(x)$ are the nontrivial invariant factors of a matrix $xI - A$ and n_i is the degree of $g_i(x)$, then by Theorem 1 the n-rowed square matrix

$$B = \text{diag}\,\{B_1, \ldots, B_t\}$$

will be similar in F to A if B_i is an n_i-rowed square matrix such that the only nontrivial invariant factor of the characteristic matrix of B_i is $g_i(x)$. For then $xI - B = \text{diag}\,\{xI_{n_1} - B_1, \ldots, xI_{n_t} - B_t\}$ is equivalent in $F[x]$ to diag $\{G_1, \ldots, G_t\}$, where $G_i = \text{diag}\,\{g_i, 1, \ldots, 1\}$, and we conclude that $xI - B$ has the same invariant factors as $xI - A$. Thus the problem of constructing an n-rowed square matrix A whose characteristic matrix has prescribed invariant factors is completely solved by the result we state as

Theorem 9. *Let* $\mathrm{g(x)} = \mathrm{x^n} - (\mathrm{b_1x^{n-1}} + \ldots + \mathrm{b_n})$ *and*

$$\mathrm{A} = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ . & . & . & \ldots & . \\ 0 & 0 & 0 & \ldots & 1 \\ \mathrm{b_n} & \mathrm{b_{n-1}} & \mathrm{b_{n-2}} & \ldots & \mathrm{b_1} \end{pmatrix}. \tag{32}$$

Then $\mathrm{g(x)I}$ *is both the characteristic and the minimum function of* A, $\mathrm{g(x)}$ *is the only nontrivial invariant factor of* $\mathrm{xI - A}$.

For

$$xI - A = \begin{pmatrix} x & -1 & 0 & \ldots & 0 & 0 \\ 0 & x & -1 & \ldots & 0 & 0 \\ . & . & . & \ldots & . & . \\ 0 & 0 & 0 & \ldots & x & -1 \\ -b_n & -b_{n-1} & -b_{n-2} & \ldots & -b_2 & x - b_1 \end{pmatrix}. \tag{33}$$

The complementary submatrix of the element $-b_n$ of (33) is an $(n-1)$-rowed square triangular matrix with diagonal elements all -1 and its determinant is $(-1)^{n-1}$. Thus the cofactor of $-b_n$ is $(-1)^{n+1}(-1)^{n-1} = 1$ and hence $d_{n-1}(x) = 1$. It remains to prove that $d_n(x) = |xI - A| = g(x)$. This is true if $n = 1$, since then $A = A_1 = (b_1)$, and $|xI - A| = x - b_1$. Let it be true for matrices A_{n-1} of the form (33) and of $n-1$ rows, so that $|xI - A_{n-1}| = x^{n-1} - (b_1x^{n-2} + \ldots + b_{n-1})$ is the cofactor of the element x in the first row and column of (33). We now expand (33) according to its first column and obtain $|xI - A| = x[x^{n-1} - (b_1x^{n-2} + \ldots + b_{n-1})] - b_n = g(x)$ as desired. This proves our theorem.

The construction of square matrices A with complex number elements whose characteristic matrices have prescribed elementary divisors has a simple solution, and we shall see that the argument preceding Theorem 9 reduces the solution to the proof of

Theorem 10. *Let* c *be a complex number,* A *be the* n*-rowed square matrix*

$$\mathrm{A} = \begin{pmatrix} \mathrm{c} & 1 & 0 & \ldots & 0 & 0 \\ 0 & \mathrm{c} & 1 & \ldots & 0 & 0 \\ \cdot & \cdot & \cdot & \ldots & \cdot & \cdot \\ 0 & 0 & 0 & \ldots & \mathrm{c} & 1 \\ 0 & 0 & 0 & \ldots & 0 & \mathrm{c} \end{pmatrix}. \tag{34}$$

Then the only nontrivial invariant factor of $\mathrm{xI} - \mathrm{A}$ *is* $(\mathrm{x} - \mathrm{c})^{\mathrm{n}}$.

For $xI - A$ is a triangular matrix with diagonal elements all $x - c$, $|xI - A| = (x - c)^n$. The complementary minor of the element in the nth row and first column of $xI - A$ is a triangular matrix with diagonal elements all unity, $d_{n-1}(x) = 1$, and $d_n(x) = (x - c)^n$ is the only nontrivial invariant factor of A.

Thus if $c_1, \ldots, c_t$ are complex numbers and $n_1, \ldots, n_t$ are positive integers, we construct matrices A_i of the form (34) for $c = c_i$ and with n_i rows. The matrix $A = \text{diag}\,\{A_1, \ldots, A_t\}$ then has n rows, and its characteristic matrix $xI - A = \text{diag}\,\{B_1, \ldots, B_t\}$, where $B_i = xI_{n_i} - A_i$ is equivalent in $F[x]$ to $\text{diag}\,\{f_i, 1, \ldots, 1\}$ such that $f_i = (x - c_i)^{n_i}$. But then $xI - A$ is equivalent in $F[x]$ to $\text{diag}\,\{f_1, \ldots, f_t, 1, \ldots, 1\}$, and by Theorem 3 the nontrivial elementary divisors of $xI - A$ are $f_1, \ldots, f_t$ as desired.

EXERCISES

1. Compute the invariant factors and elementary divisors of the characteristic matrices of the following matrices.

$$a)\ \begin{pmatrix} -1 & -1 & 1 \\ -2 & 5 & -1 \\ -1 & -1 & -1 \end{pmatrix} \qquad b)\ \begin{pmatrix} 1 & -1 & -1 \\ 1 & 0 & -1 \\ 2 & -2 & -2 \end{pmatrix}$$

$$c)\ \begin{pmatrix} 1 & -1 & -1 \\ 2 & -1 & -2 \\ 1 & 1 & -1 \end{pmatrix} \qquad d)\ \begin{pmatrix} 1 & -1 & 0 \\ 2 & -1 & -1 \\ 6 & -2 & -2 \end{pmatrix}$$

$$e)\ \begin{pmatrix} -4 & 6 & 3 \\ -3 & 5 & 4 \\ 4 & -5 & 3 \end{pmatrix} \qquad f)\ \begin{pmatrix} 0 & -2 & 1 & 0 \\ 2 & 0 & 0 & 0 \\ 1 & -1 & 2 & -1 \\ 0 & -1 & 1 & 0 \end{pmatrix}$$

$$g)\ \begin{pmatrix} -2 & 1 & 3 & -2 \\ -1 & 0 & 3 & 0 \\ 1 & -1 & 0 & -1 \\ -3 & 0 & 8 & 0 \end{pmatrix} \qquad h)\ \begin{pmatrix} -6 & 2 & -5 & -19 \\ 2 & 0 & 1 & 5 \\ -2 & 1 & 0 & -5 \\ 3 & -1 & 2 & 9 \end{pmatrix}$$

2. Find a matrix $B = \operatorname{diag}\{B_1, \ldots, B_t\}$ similar in $F(\lambda)$ to each of the matrices of Ex. 1, respectively, where B_i has the form (32), and the characteristic function of B_i is the ith nontrivial invariant factor of A.

3. Solve Ex. 2 with the characteristic function of B_i now the ith nontrivial elementary divisor of A, B_i of the form (34).

7. Additional topics. There are many important topics of the theory of matrices other than those we have discussed, and we leave their exposition to more advanced texts. Let us mention some of these topics here, however.

The quantities of the field K of all complex numbers have the form

$$c = a + bi \qquad (a, b \text{ in } R,\ i^2 = -1),$$

where R is the field of all real numbers, a subfield of K. The *complex conjugate* of c is

$$\bar{c} = a - bi,$$

and the correspondence $c \longleftrightarrow \bar{c}$ defines a *self-equivalence* or *automorphism* of K, a fact verified in Section 6.9. This automorphism of K leaves the elements of its subfield R unaltered, that is, $\bar{a} = a$ for every real a. We then may call it an *automorphism* over R.

If A is any m by n matrix with elements a_{ij} in K, we define $\bar{A}$ to be the m by n matrix whose element in its ith row and jth column is $\bar{a}_{ij}$. It is then a simple matter to verify that

$$\overline{AB} = \bar{A}\bar{B}\,, \qquad (\bar{A})' = \overline{A'}\,, \qquad \overline{C^{-1}} = (\bar{C})^{-1}\,,$$

for every A, B, and nonsingular C. Moreover, then $(\overline{AB})' = \overline{B'}\overline{A'}$. We now define a matrix A to be *Hermitian* if $\overline{A'} = A$, *skew-Hermitian* if $\overline{A'} = -A$. Two matrices A and B are said to be *conjunctive* in K if there exists a nonsingular matrix P with elements in K such that

$$PA\overline{P'} = B\,.$$

The results of this theory are almost exactly the same as those of the theory of congruent matrices, and it is, in fact, possible to obtain a general theory including both of the theories above as special cases.

Two symmetric matrices A and B with elements in a field F are said to be *orthogonally equivalent* in F if there exists an orthogonal matrix P with elements in F such that $PAP' = B$. But $PP' = P'P = I$ so that $B = PAP^{-1}$ is both similar and congruent to A. Analogously, we call a matrix P with complex elements such that $P\overline{P'} = \overline{P'}P = I$, a *unitary matrix*. Then we say that two Hermitian matrices A and B are *unitary equivalent* if $PA\overline{P'} = B$, where P is a unitary matrix. Both of these concepts may also be shown to be special cases of a more general concept.

Finally, let us mention the topic of the equivalence and congruence of pairs of matrices. Let A, B, C, D be matrices of the same numbers of rows and columns. Then we call the pairs A, B and C, B *equivalent* pairs* if there exist nonsingular square matrices P and Q such that simultaneously $PAQ = C$ and $PBQ = D$. Similarly, if A, B, C, D are n-rowed square matrices, we call A, B and C, D *congruent pairs* if simultaneously $PAP' = C$ and $PBP' = D$ for a nonsingular matrix P.

References to treatments of the topics mentioned above as well as others will be found in the final bibliographical section of Chapter VI. We shall not state any of the results here.

* In this connection see Exs. 3 and 4 of Section 5.

CHAPTER VI

FUNDAMENTAL CONCEPTS

1. Groups. These pages were written in order to bridge the gap between the intuitive function-theoretic study of algebra, as presented in the usual course on the theory of equations, and the abstract approach of the author's *Modern Higher Algebra*. The objective of our exposition has now been attained. For our study of matrices with constant elements led us naturally to introduce the concepts of field, linear space, correspondence, and equivalence, and we are ready now to begin the study of abstract algebra. However, we believe it desirable to precede the serious study of material such as that of the first two chapters of the *Modern Higher Algebra* by a brief discussion of this subject matter, without proofs (or exercises). We shall give this discussion here and shall therewith not only leave our readers with an acquaintance with the basic concepts of algebraic theory but with a knowledge of how these concepts may lead into those branches of mathematics called the *Theory of Numbers* and the *Theory of Algebraic Numbers*.

Our first new concept is that of a set G of elements closed with respect to a single operation, and we wish to define the concept that G forms a *group* with respect to this operation. It should be clear that if we do not state the nature either of the elements of G or of the operation, it will not matter if we indicate the operation as *multiplication*. If we wish later to consider special sets of elements with specified operations we shall then replace "product" in our definition by the operation desired. Thus we shall make the

DEFINITION. *A set* G *of elements* a, b, c, . . . *is said to form a group with respect to multiplication if for every* a, b, c *of* G

I. *The product* ab *is in* G;

II. *The associative law* a(bc) = (ab)c *holds;*

III. *There exist solutions* x *and* y *in* G *of the equations*

$$ax = b, \qquad ya = b.$$

The reader is already familiar with the groups (with respect to ordinary multiplication) of all nonzero rational numbers, all nonzero real numbers,

and, indeed, all nonzero elements of any field. These are all examples of groups G such that for every a and b of G we have

IV. *The products* $ab = ba$.

Such groups are called *commutative* or *abelian* groups. An example of a *nonabelian* (*noncommutative*) group is the group, with respect to matrix multiplication, of all nonsingular n-rowed square matrices with elements in a field.

Every group G contains a *unique* element e called its *identity element*, such that for every a of G

$$ae = ea = a . \tag{1}$$

Moreover, every element a of G has a *unique inverse* a^{-1} in G such that

$$aa^{-1} = a^{-1}a = e , \tag{2}$$

Then the solutions of the equations of Axiom III are the *unique* elements

$$x = a^{-1}b , \quad y = ba^{-1} . \tag{3}$$

A set H of elements of a group G is called a *subgroup* of G if the product of any two elements of H is in H, H contains the identity element of G and the inverse element h^{-1} of every h of H. Then H forms a group with respect to the same operation as does G.

The *equivalence* of two groups is defined as an instance of the general definition of equivalence which we gave in Section 4.5. The concept of equivalence of two mathematical systems of the same kind as well as the concept of subsystem (e.g., subgroup of a group, subfield of a field, linear subspace over F of a linear space over F) are two concepts of evident fundamental importance which are given in algebraic theory whenever any new mathematical system is defined.

The number of elements in a group G is called its *order*. This number is either infinity, and we call G an *infinite group;* or it is a finite number n, and we call G a *finite group of order* n. For finite groups we have the important result which we shall state without proof.*

LEMMA 1. *Let* H *be a subgroup of a finite group* G. *Then the order of* H *divides the order of* G.

A simple example of a finite abelian group is the set of all nth roots of unity. The reader may verify that an example of a finite nonabelian group

* The proof is given in Chapter VI of my *Modern Higher Algebra.*

is given by the quaternion group of order 8 whose elements are the two-rowed matrices with complex elements,

$$(4)\qquad \begin{cases} I, & A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, & B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \\ AB, & -I, & -A, & -B, & -AB. \end{cases}$$

The set of all powers

$$(5)\qquad a^0 = e,\ a,\ a^{-1},\ a^2,\ a^{-2},\ \ldots$$

of an element a of a group G forms a subgroup of G which we shall designate by

$$(6)\qquad [a]$$

and shall call the *cyclic group generated by* a. Its order is called the *order of the element* a and it can be shown that either all the powers (5) are distinct and a has infinite order, or a has finite order m, and $[a]$ consists of the m distinct powers

$$(7)\qquad e,\ a,\ a^2,\ \ldots,\ a^{m-1},$$

where e is the identity element of $[a]$, $a^m = e$. Then *the order* m *of* a *is the least integer* t *such that* $a^t = e$. Moreover, it can be shown that $a^t = e$ *if and only if* m *divides* t.

The order m of an element of a finite group G divides the order of G, since m is the order of the subgroup $[a]$, and we may apply Lemma 1. Thus $n = mq$, $a^n = (a^m)^q = e^q = e$. We therefore have

LEMMA 2. *Let* e *be the identity element of a group* G *of order* n. *Then*

$$(8)\qquad a^n = e$$

for every a *of* G.

2. Additive groups. In any field and in the set of all n-rowed square matrices there are *two* operations. Thus we have said that the set of all nonzero elements of a field and the set of all nonsingular n-rowed square matrices form multiplicative groups. But the elements of any field, the set of all m by n matrices with elements in a field, the elements of any linear space, all form *additive* groups, that is, groups with respect to the operation of addition as defined for each of these mathematical systems. The reader will observe that the axioms for an additive abelian group G are those axioms

for addition which we gave in Section 3.12 for a field. Additive groups are normally assumed to be abelian, that is, the use of addition to designate the operation with respect to which a group G is defined is usually taken to connote the fact that G is abelian.

The identity element of an additive group is usually called its *zero* element, that is, the element 0 such that $a + 0 = a = 0 + a$. The inverse with respect to addition of a is designated as $-a$ and is such that $a + (-a) = (-a) + a = 0$. Thus the solutions of the additive formulation

$$a + x = b\,, \qquad y + a = b\,, \tag{9}$$

of the equations of our group Axiom III are

$$x = (-a) + b\,, \qquad y = b + (-a)\,. \tag{10}$$

When G is abelian, we have $x = y$ and designate their common value by $b - a$. Thus we define the operation of *subtraction* in terms of that of addition.

In a cyclic additive group $[a]$ the elements are always designated by

$$0, a, 2a, (2 + a), \ldots, \tag{11}$$

where, clearly, if m is any positive integer $-(m \cdot a) = m \cdot (-a)$, and we define $(-m) \cdot a = -(m \cdot a)$. Here $m \cdot a$ does *not* mean the *product* of a by the positive integer m but means the *sum* $a + \ldots + a$ with m summands. If $[a]$ is a finite group of order m, the elements of $[a]$ are 0, a, $2a$, $\ldots$, $(m - 1) \cdot a$, and m is least positive integer such that the sum of m summands all equal to a is zero. However, if $[a]$ is infinite, then it may be seen that $n \cdot a = q \cdot a$ for any integers n and q if and only if n and q are equal.

3. Rings. The set consisting of all n-rowed square matrices with elements in a field F is an instance of certain type of mathematical system called a *ring*. Many other systems which are known to the reader are rings and we shall make the

DEFINITION. *A ring is an additive abelian group of at least two distinct elements such that, for every* a, b, c, *of* R,

I. *The product* ab *is in* R;

II. *The associative law* a(bc) = (ab)c *holds;*

III. *The distributive laws* a(b + c) = ab + ac, (b + c)a = ba + ca *hold.*

We leave to the reader the explicit formulation of the definitions of subring and equivalence of rings. They may be found in the first chapter of the *Modern Higher Algebra.* The reader should also verify that all nonmodular fields are rings, the set of all ordinary integers is a ring.

The *zero element* of a ring R is its identity element with respect to addition. Observe that by making the hypothesis that R contains at least two elements we exclude the mathematical system consisting of zero alone from the systems we have called rings.

Rings may now be seen to be mathematical systems R whose elements have all the ordinary properties of numbers except that possibly the products ab and ba might be *different* elements of R, the equations $ax = b$ of $ya = b$ might not have solutions in R if $a \neq 0$, b are in R. A ring may also contain *divisors of zero*, that is, elements $a \neq 0$, $c \neq 0$ such that $ac = 0$. In particular, the ring of all n-rowed square matrices has already been seen to have such elements as well as the other properties just mentioned.

A ring is said to possess a *unity element* e if e in R has the property $ea = ae = a$ for every a of R. The element e then has the properties of the ordinary number 1 and is usually designated by that symbol. The unity element of the set of all n-rowed square matrices is the n-rowed identity matrix, and the unity element was always the number 1 in the other rings we have studied. However, the set of all two-rowed square matrices of the form

$$\begin{pmatrix} 0 & r \\ 0 & 0 \end{pmatrix} \tag{12}$$

with r rational may easily be seen to be a ring without a unity element. In fact, all nonzero elements of this ring are divisors of zero.

A ring R is said to be *commutative* if $ab = ba$ for every a and b of R. The ring of all integers is a commutative ring, the ring of all n-rowed square matrices with elements in a field F is a noncommutative ring.

4. Abstract fields. If R is any ring, we shall designate by

$$R^*$$

the set of all nonzero elements of R. Then we shall call R a *division ring* if R^* is a multiplicative group. This occurs clearly if and only if the equations $ax = b$, $ya = b$ have solutions in R^* for every a and b of R^*. The set of all n-rowed square matrices is not a division ring. However, let c and d range

over all complex numbers, $\bar{c}$ and $\bar{d}$ be the complex conjugate of c and d. Then the set Q of all two-rowed matrices

$$A = \begin{pmatrix} c & -d \\ \bar{d} & \bar{c} \end{pmatrix} \tag{13}$$

is a noncommutative division ring. The reader should verify this, noting in particular that every $A \neq 0$ is nonsingular since $A \neq 0$ implies that $c \neq 0$ or $d \neq 0$ and $|A| = c\bar{c} + d\bar{d} > 0$. The ring Q is a linear space of order 4 over the field of all real numbers and it has the matrices I, A, B, AB of (4) as a basis over that field. It is usually called the ring of *real quaternions.*

Until the present we have restricted the term "field" to mean a field containing the field of all rational numbers. We now define fields in general.

DEFINITION. *A field is a ring* F *such that* F* *is a multiplicative abelian group.*

The identity element of the multiplicative group F^* is then the unity element 1 of F. The whole set F is an additive group with identity element 0, and 1 generates an additive cyclic subgroup [1]. If this cyclic group has infinite order, it may be shown to be equivalent to the set of all ordinary integers. But F is closed with respect to rational operations, and [1] then generates a subfield of F equivalent to the field of all rational numbers. We call all such fields *nonmodular fields.*

The group [1] might, however, be a finite group. Its elements are then the *sums*

$$0 \cdot 1 = 0, 1, 2, \ldots, p - 1, \tag{14}$$

where p is the order of this group, and we have the property that the *sum* $1 + 1 + \ldots + 1$ with p summands is zero. It is easy to show that p *is a prime,* and it follows that if a is in F, then the sum $a + a + \ldots + a$ with p summands is equal to the product $(1 + 1 + \ldots + 1)a = 0$. We call such fields F *modular fields of characteristic* p. It may easily be shown that the characteristic of all subfields of a field F is the same as that of F, and, in fact, every subfield of F contains the subfield generated by the unity element of F under rational operations.

5. Integral domains. A commutative ring with a unity element and without divisors of zero is called an *integral domain.* Any field forms a somewhat trivial example of an integral domain. Less trivial examples are the set $F[x]$ of all polynomials in x, the set $F[x_1, \ldots, x_q]$ of all polynomials in $x_1, \ldots, x_q$ and coefficients (in both cases) in a field F, the set of all ordinary

integers. The set of all integers may be extended to the field of all rational numbers by adjoining quotients a/b, $b \neq 0$. In a similar fashion we adjoin quotients a/b for a and $b \neq 0$ in J to imbed any integral domain J in a field.

When we studied polynomials in Chapter I we studied questions about divisibility and greatest common divisor. We may also study such questions about arbitrary integral domains. Let us then formulate such a study.

Let J be an integral domain and a and b be in J. Then we say that a *is divisible by* b (or that b *divides* a) if there exists an element c in J such that $a = bc$. If u in J divides its unity element 1, then u is called a *unit* of J. Thus u is a unit of J if it has an inverse in J. The inverse of a unit is clearly also a unit.

Two quantities b and b_0 are said to be *associated* if each divides the other. Then b and b_0 are associated if and only if $b_0 = bu$ for a unit u. Moreover, if b divides a so does every associate of b. Every unit of J divides every a of J. Thus we are led to one of the most important problems about an integral domain, that of determining its units.

A quantity p of an integral domain J is called a *prime* or *irreducible quantity* of J if $p \neq 0$ is not a unit of J and the only divisors of p in J are units and associates of p. Every associate of a prime is a prime. A *composite quantity* of J is an $a \neq 0$ which is neither a prime nor a unit of J. It is natural then to ask whether or not every composite a of J may be written in the form

$$a = p_1 \ldots p_r \tag{15}$$

for a finite number of primes p_i of J. We may also ask if it is true that whenever also $a = q_1 \ldots q_s$ for primes q_i, then necessarily $s = r$ and the q_i are associates of the p_j in some order. When these properties hold we may call J a *unique factorization integral domain.* The reader is familiar with the fact that the set of all ordinary integers is such an integral domain. This fact, as well as the corresponding property for the set of all polynomials in $x_1, \ldots, x_n$ with coefficients in a field F are derived in Chapter II of the author's *Modern Higher Algebra.*

The problem of determining a g.c.d. (greatest common divisor) of two elements a and b of a unique factorization domain is solvable in terms of the factorization of a and b. However, we saw that in the case of the set $F[x]$ the g.c.d. may be found by a Euclidean process. Let us then formulate the problem regarding g.c.d.'s. We define a g.c.d. of two elements a and b not both zero of J to be a common divisor d of a and b such that every common divisor of a and b divides d. Then all g.c.d.'s of a and b are associates. We call a and b *relatively prime* if their only common divisors are units of J,

that is, they have the unity element of J as a g.c.d. We now see that one of the questions regarding an integral domain J is the question as to whether every a and b of J have a g.c.d. Moreover, we must ask whether there exist x and y in J such that

$$d = ax + by$$

is a common divisor and hence a g.c.d. of a and b; and finally whether or not d may be found by the use of a *Euclidean Division Algorithm.*

6. Ideals and residue class rings. A subset M of a ring R is called an *ideal* of R if M contains $g - h$, ag, ga, for every g and h of M and a of R. Then M either consists of zero alone and will be called the *zero ideal* of R, or M may be seen to be a subring of R with the property that the products am, ma of any element m of M and any element a of R are in M.

If H is any set of elements of a ring R, we may designate by $\{H\}$ the set consisting of all finite sums of elements of the form xmy for x and y in R, m in H. It is easy to show that $\{H\}$ is an ideal. If H consists of finitely many elements $m_1, \ldots, m_t$ of R, we write $\{H\} = \{m_1, \ldots, m_t\}$, and if H consists of only one element m of R, we write

(16) $$M = \{m\}$$

for the corresponding ideal. This most important type of an ideal is called a *principal* ideal. It consists of all finite sums of elements of the form amb for a and b in R. When R is a commutative ring, $M = \{m\}$ consists of all products am for a in R.

The ring R itself is an ideal of R called the *unit ideal.* This term is derived from the fact that in the case where R has a unity quantity $R = \{1\}$. Evidently $\{0\}$ is the zero ideal.

Let M be an ideal of R and define

(17) $$a \equiv b \ (M)$$

(*read*: a congruent b modulo M) if $a - b$ is in M. We may then define what we shall call a residue class $\underline{a}$ of M for every a of R. We put into the class every b in R such that $a \equiv b \ (M)$. Clearly $a \equiv b \ (M)$ if and only if $b \equiv a \ (M)$. Moreover, if $a - b$ is in M and $b - c$ in M, then $(a - b) + (b - c) = a - c$ is in M. It follows that $\underline{a} = \underline{b}$ (a and b are the same residue class) if and only if b is in $\underline{a}$.

Let us now define the sum and product of residue classes by

(18) $$\underline{a} + \underline{b} = \underline{a + b}, \qquad \underline{a} \cdot \underline{b} = \underline{a \cdot b}.$$

It may be verified readily that if $\underline{a_1} = \underline{a}$, $\underline{b_1} = \underline{b}$, then $\underline{a_1 + b_1} = \underline{a + b}$, $\underline{a_1 b_1} = \underline{ab}$. It follows that our definitions of sum and product of residue classes are unique. Then it is easy to show that if M is not R the set of all the residue classes forms a ring with respect to the operations just defined. We call this ring the *residue class* or *difference ring* R − M (*read:* R minus M). When $M = R$ the residue classes are all the zero class, and we have not called this set a ring.

When the residue class ring $R - M$ is an integral domain, we call the ideal M a *prime ideal* of R. We call M a *divisorless ideal* of R if $R - M$ is a field. These concepts coincide in the case where $R - M$ has only a finite number of elements since it may be shown that any integral domain with a finite number of elements is a field. This coincidence occurs in most of the topics of mathematics (in particular the *Theory of Algebraic Numbers*) where ideals are studied.

7. The ring of ordinary integers. The set of all ordinary integers is a ring which we shall designate henceforth by E. It is easily seen to be an integral domain, and we shall prove that it has the property of unique factorization.

We observe first that the units of E are those ordinary integers u such that $uv = 1$ for an integer v. But then 1 and -1 are the only units of E. Thus the primes of E are the ordinary positive prime integers 2, 3, 5, etc., and their associates -2, -3, -5, etc. Every integer a is associated with its absolute value $|a| \geqq 0$. We note now that if b is any integer not zero, the multiples

$$0,\ |b|,\ -|b|,\ 2|b|,\ -2|b|,\ \ldots \tag{19}$$

are clearly a set of integers one of which exceeds* any given integer a. Then let $(g + 1)|b|$ be the least multiple of $|b|$ which exceeds a so that $g|b| \leq a$, $(g + 1)|b| > a$, $a - g|b| = r$ such that $0 \leq r < |b|$. We put $q = g$ if $b > 0$, $q = -g$ otherwise, and have $g|b| = qb$, $a = bq + r$. If also $a = bq_1 + r_1$ with $0 \leq r_1 < |b|$, then $b(q - q_1) = r_1 - r$ is divisible by b, whereas $|r - r_1| < |b|$. This is possible only if $r_1 = r$ and $q_1 = q$. We have thus proved the *Division Algorithm* for E, a result we state as

Theorem 1. *Let* a *and* b ≠ 0 *be integers. Then there exist unique integers* q *and* r *such that* $0 \leq r < |b|$, a = bq + r.

We now leave for the reader the application of the Euclidean process, which we used to prove Theorem 1.5, to our present case. The process yields

* We use the concept of *magnitude* of integers throughout our study of the ring E.

Theorem 2. *Let* f *and* g *be nonzero integers. Then there exist integers* a *and* b *such that*

$$\mathrm{d} = \mathrm{af} + \mathrm{bg} \tag{20}$$

is a positive divisor of both f *and* g. *Then* d *is the unique positive g.c.d. of* f *and* g.

The result above implies

Theorem 3. *Let* f, g, h *be integers such that* f *divides* gh *and is prime to* g. *Then* f *divides* h.

For by Theorem 2 we have $af + bg = 1$, $afh + bgh = h$. But by hypothesis $gh = fq$, $h = (ah + bq)f$ is divisible by f.

We then have

Theorem 4. *Let* p *be a prime divisor of* gh. *Then* p *divides* g *or* h.

For if p does not divide g, the g.c.d. of p and g is either 1 or an associate of p. The latter is impossible, and therefore p is prime to g.

We also have

Theorem 5. *Let* m *be an integer. Then the set of integers prime to* m *is closed with respect to multiplication.*

For let a and b be prime to m and d be the g.c.d. of ab and m. If ab is not prime to m we have $d > 1$, and by Theorem 3 if d is prime to a it divides b. But then a divisor $c > 1$ of d divides a or b as well as m contrary to hypothesis.

We may now conclude our proof of what is sometimes called the Fundamental Theorem of Arithmetic.

Theorem 6. *Every composite integer* a *is expressible in the form*

$$\mathrm{a} = \pm \mathrm{p}_1 \ldots \mathrm{p}_r \tag{21}$$

uniquely apart from the order of the positive prime factors $\mathrm{p}_1, \ldots, \mathrm{p}_r$.

For if $a = bc$, every divisor of b or of c is a divisor of a. If a is composite, it has divisors b such that $1 < b < |a|$, and there exists a least divisor $p_1 > 1$ of a. But then p_1 is a positive prime, $a = p_1a_2$ for $|a_2| < |a|$. If a_2 is a prime, we write $a_2 = \pm p_2$ with p_2 a positive prime and have (21) for $r = 2$. Otherwise a_2 is composite and has a prime divisor p_2 by the proof above, $a_2 = p_2a_3$ and $a = p_1p_2a_3$ for $|a_3| < |a_2|$. After a finite number of stages the sequence of decreasing positive integers $|a| > |a_2| > |a_3| > \ldots$ must terminate, and we have (21). If also $a = \pm q_1 \ldots q_s$ for positive primes $q_1, \ldots, q_s$, the sign is uniquely determined by a, and $p_1 \ldots p_r = q_1 \ldots q_s$. Then either we may arrange the q_i so that $q_1 = p_1$, or $p_1 \neq q_j$ for $j = 1, \ldots, s$. But if the divisor p_1 of $q_1 \ldots q_s$ is not equal to q_1, it does

not divide q_1 and by Theorem 4 must divide $q_2 \ldots q_s$. By our hypothesis it does not divide q_2 and must divide $q_3 \ldots q_s$. This finite process leads to a contradiction. Thus $p_1 = q_1$, $p_2 \ldots p_r = q_2 \ldots q_s$, and the proof just completed may be repeated, and we may take $p_2 = q_2$. Proceeding similarly, we ultimately obtain $r = s$, the $p_i = q_i$ for an appropriate ordering* of the q_i.

8. The ideals of the ring of integers. Let M be a nonzero ideal of the set E of all integers and m be the least positive integer in M. Then M contains every element qm of the principal ideal $\{m\}$. If h is in M, we may use Theorem 1 to write $h = mq + r$ where $0 \leq r < m$. But mq and h are in M, $h - mq = r$ is in M. Our definition of m implies that $r = 0$ and thus that every element of M is in $\{m\}$. We have proved

Theorem 7. *The ideals of* E *are principal ideals* {m}, m *a positive integer.*

The residue classes of E modulo $\{m\}$ are now the classes

$$\underline{0}, \underline{1}, \ldots, \underline{m-1}. \tag{22}$$

For if a is any integer, we have $a = mq + r$ for $r = 0, 1, \ldots, m-1$. Then $a - r$ is in $\{m\}$, $\underline{a} = \underline{r}$. Thus the elements of the residue class ring

$$E - \{m\}$$

defined for $m > 1$ are given by (22). Then $E - \{m\}$ is a ring whose zero element is the class $\underline{0}$ of all integers divisible by m and whose unity element is the class $\underline{1}$ of all integers whose remainder in Theorem 1 on division by m is 1.

If a is an integer prime to m, the elements of the residue class $\underline{a}$ are all prime to m. For by Theorem 2 there exist integers c and d such that

$$ac + md = 1. \tag{23}$$

If b is in $\underline{a}$, then $b = a + mq$, $bc + m(d - qc) = ac + m(qc + d - qc) = ac + md = 1$, and therefore b and m are relatively prime. But $\underline{a} \cdot \underline{c} = \underline{1}$, and Theorem 7 implies

Theorem 8. *The residue classes* a *in* E − {m} *defined for* a *prime to* m *form a multiplicative abelian group.*

If m is a composite integer cd where $c > 1$, $d > 1$, then $m > c$, $m > d$, and $\underline{c}$ and $\underline{d}$ are both not the zero class. But $\underline{c} \cdot \underline{d} = \underline{cd} = \underline{m} = \underline{0}$, $E - \{m\}$ has divisors of zero and is not an integral domain. If m is a prime, then

* We may order the p_i so that $p_1 \leq p_2 \leq \ldots \leq p_r$ and similarly assume that $q_1 \leq q_2 \leq \ldots \leq q_s$. Then we obtain $r = s$, $p_i = q_i$ for $i = 1, \ldots, r$.

every a not in $\underline{m}$ is prime to m, and Theorem 8 states that $E - \{m\}$ is a field. We have proved

Theorem 9. *An ideal* M *of* E *is a prime ideal if and only if* M = {p} *for a positive prime* p, M *is a divisorless ideal.*

We observe now that $a \equiv b\ (M)$ for $M = \{m\}$ means that $a - b = mq$, that is, $a - b$ is divisible by m. Thus it is customary in the *Theory of Numbers* to write

$$a \equiv b \pmod{m} \tag{24}$$

(*read*: a congruent b modulo m) if $a - b$ is divisible by m. But then $\underline{a} = \underline{b}$, and if we also have $\underline{c} = \underline{d}$, we will have $\underline{a} + \underline{c} = \underline{b} + \underline{d}$ as well as $\underline{a} \cdot \underline{c} = \underline{b} \cdot \underline{d}$. Hence if (24) and

$$c \equiv d \pmod{m} \tag{25}$$

hold, we have

$$a + c \equiv b + d \pmod{m}\,, \qquad ac \equiv bd \pmod{m}\,. \tag{26}$$

Thus the rules (26) for combining congruences are equivalent to the definitions of addition and multiplication in $E - \{m\}$.

We next state the number-theoretic consequence of Theorem 8 and Lemma 2 which is called *Euler's Theorem* and which we state as

Theorem 10. *Let* f(m) *be the number of positive integers not greater than* m > 0 *and prime to* m. *Then if* a *is prime to* m *we have*

$$\mathrm{a}^{\mathrm{f(m)}} \equiv 1 \pmod{\mathrm{m}}\,. \tag{27}$$

For $f(m)$ is clearly the order of the multiplicative group defined in Theorem 8. Our result then follows from Lemma 2.

We next have the *Fermat Theorem.*

Theorem 11. *Let* p *be a prime. Then*

$$\mathrm{a}^{\mathrm{p}} \equiv \mathrm{a} \pmod{\mathrm{p}} \tag{28}$$

for every integer a.

For (28) holds if a is divisible by p. Otherwise a is prime to p, and $\underline{a}$ is one of the residue classes $\underline{1}, \underline{2}, \ldots, \underline{p-1}$. Thus $f(p) = p - 1$ and by Theorem 10 $a^{p-1} - 1$ is divisible by p, $a(a^{p-1} - 1) = a^p - a$ is also divisible by p.

The ring $E - \{p\}$ defined by a positive prime p is a field* P whose

* This field is equivalent to the subfield generated by its unity quantity of any field of characteristic p.

nonzero elements form an abelian group P^* of order $p - 1$. The elements of P^* are the distinct roots of the equation $x^{p-1} = \underline{1}$ and are not all roots of any equation of lower degree. Then it may be shown that P^* is a cyclic multiplicative group $[\underline{r}]$ where r is an integer such that $\underline{1}, \underline{r}, \underline{r^2}, \ldots, \underline{r^{p-2}}$ are a complete set of nonzero residue classes modulo $\{p\}$. Such an integer r is called a *primitive root modulo* p. We then have

Theorem 12. *Let* p *be a prime of the form* $4n + 1$. *Then there exists an integer* t *such that*

$$t^2 + 1 \equiv 0 \pmod{p}. \tag{29}$$

For $p - 1 = 4n$, and we let r be a primitive root modulo p, $t = r^n$. Then $t^4 = r^{p-1}$, $t^4 - 1 = (t^2 + 1)(t^2 - 1)$, $(\underline{t^2} + \underline{1})(\underline{t^2} - \underline{1}) = \underline{0}$ in the field $E - \{p\}$. However, $\underline{t^2} = \underline{r^{2n}} \neq \underline{1}$ since r is primitive, $\underline{t^2} + \underline{1} = \underline{0}$ as desired.

There is a number of other results on congruences which are corollaries of theorems on rings and fields. However, we shall not mention them here.

9. Quadratic extensions of a field. If F is a subfield of a field K which is a linear space $u_1F + \ldots u_nF$ over F, we say that K is a field *of degree* n *over* F. The theory of linear spaces of Chapter IV implies that u_1 may be taken to be any nonzero element of K. Hence we may take u_1 to be the unity element 1 of F. Then if $n = 1$, the field K is F. We call K a quadratic, cubic, quartic, or quintic field over F according as $n = 2, 3, 4$, or 5.

Let $n = 2$ so that K has a basis $u_1 = 1$, u_2 over F. The quantities of K are then uniquely expressible in the form $k = c_1 + c_2u_2$ for c_1 and c_2 in F, and k is in F, $k = k \cdot 1 + 0u_2$, if and only if $c_2 = 0$. Clearly, if k is in F, then 1, k do not form a basis of K over F. We now say that a quantity u in K *generates* K over F if 1, u are a basis of K over F. Then u generates K over F if and only if u is not in F. For if 1, u are linearly dependent in F we have $a_1 + a_2u = 0$ for $a_2 \neq 0$, $u = -a_2^{-1}a_1$ is in F.

The elements k of a quadratic field have the property that 1, k, k^2 are linearly dependent in F, $c_2k^2 + c_1k + c_2 = 0$ for c_0, c_1, c_2 not all zero and in F. If $c_0 = 0$, then c_1 cannot be zero, and $k = -c_1c_2^{-1}$ is in F, k is a root of the monic polynomial $(x - k)^2$ with coefficients in F. If k is not in F, then $c_0 \neq 0$, k is a root of a monic polynomial of degree two. Thus every element k of a quadratic field is a root of an equation

$$f(x, k) = x^2 - T(k)x + N(k) = 0 \tag{30}$$

with $T(k)$ and $N(k)$ in F. In particular, if u generates K over F we have

$$u^2 - bu + c = 0 \tag{31}$$

for b and c in F, and we propose to find the value of $T(k)$ and $N(k)$ as polynomials in b, c and the coordinates k_1 and k_2 in F of $k = k_1 + k_2u$.

Define a correspondence S on K to K by

$$k = k_1 + k_2u \longrightarrow k^S = k_1 + k_2u^S\,, \tag{32}$$

for all k_1 and k_2 in F where u^S is in K. Then (32) is a one-to-one correspondence of K and itself if and only if u^S generates K over F. If $k_0 = k_3 + k_4u$ for k_3 and k_4 in F we have $k_0^S = k_3 + k_4u^S$, $k + k_0 = (k_1 + k_3) + (k_2 + k_4)u$, so that $(k + k_0)^S = k_1 + k_3 + (k_2 + k_4)u^S$, and we have

$$(k + k_0)^S = k^S + k_0^S\,. \tag{33}$$

Also $kk_0 = k_1k_3 + (k_1k_4 + k_2k_3)u + k_2k_4u^2 = (k_1k_3 - k_2k_4c) + (k_1k_4 + k_2k_3 + k_2k_4b)u$, while $k^Sk_0^S = k_1k_3 + (k_1k_4 + k_2k_3)u^S + k_2k_4(u^S)^2$. But then

$$(kk_0)^S = k^Sk_0^S \tag{34}$$

if and only if $(u^S)^2 = bu^S - c$, that is, u^S is a root in K of the quadratic equation $x^2 - bx + c = 0$. But the quadratic equation can have only two distinct roots in a field K, the sum of the roots is b,

$$u^S = u \quad \text{or} \quad b - u\,. \tag{35}$$

In the former case S is the *identity* correspondence $k \longleftrightarrow k$. In either case S defines a self-equivalence of K leaving the elements of F unaltered and is called an *automorphism over* F *of* K.

If K were any field of degree n over F and if S and T were automorphisms over F of K, we would define ST as the result $k \longrightarrow k^{ST} = (k^S)^T$ of applying first $k \longrightarrow k^S$ and then $k^S \longrightarrow (k^S)^T$. It is easy to show that the set of all automorphisms over F of K is a group G with respect to the operation just defined. In case G has order equal to the degree n of K over F it is called the *Galois group of* K *over* F, and that branch of algebra called the *Galois Theory* is concerned with relative properties of K and G. In our present case $u^{S^2} = (u^S)^S = (b - u)^S = b - (b - u) = u$ so that S^2 is the identity automorphism. But $b - u = u$ if and only if $2u = b$, which is not possible since u is not in F unless K is a modular field in which $u + u = 0$. Hence if K is a nonmodular quadratic field over F, the automorphism group of K over F is the cyclic group $[S]$ of order 2 and is the Galois group of K.

We see now that if $k = k_1 + k_2u$, then $kk^S = (k_1 + k_2u)[k_1 + k_2(b - u)] = k_1^2 + k_1k_2b + k_2^2u(b - u)$. But $bu - u^2 = c$. Hence if

$$T(k) = k + k^S\,, \qquad N(k) = kk^S\,, \tag{36}$$

we have

$$T(k) = 2k_1 + k_2 b\,, \qquad N(k) = k_1^2 + k_2^2 c + k_1 k_2 b\,, \tag{37}$$

and the polynomial of (30) is

$$f(x, k) = (x - k)(x - k^S)\,. \tag{38}$$

The function $T(k)$ is called the *trace* of k, and $N(k)$ is called the *norm* of k. Moreover, we may show that

$$T(a_1 k + a_2 k_0) = a_1 T(k) + a_2 T(k_0)\,, \qquad N(kk_0) = N(k) \cdot N(k_0) \tag{39}$$

for every a_1 and a_2 of F and k and k_0 of K. For $T(a_1 k + a_2 k_0) = (a_1 k + a_2 k_0) + (a_1 k + a_2 k_0)^S = a_1 k + a_2 k_0 + a_1 k^S + a_2 k_0^S = a_1(k + k^S) + a_2(k_0 + k_0^S)$ as desired. Similarly,* $N(kk_0) = kk_0(kk_0)^S = kk_0 k^S k_0^S = (kk^S)(k_0 k_0^S)$. Note that if k is in F, then $N(k) = k^2$.

Let us now assume that the field K is nonmodular so that $K = F + uF$ where u satisfies (31). Then K is also generated by the root $u - \frac{1}{2}b$ of the equation

$$x^2 = a \qquad (a \text{ in } F)\,, \tag{40}$$

if $a = (u - b/2)^2 = u^2 - bu + b^2/4 = -c + b^2/4$. Let us then assume without loss of generality that u is a root of (40) so that in (31) we have $b = 0$, $c = -a$. Then (37) has the simplified form given by

$$T(k) = 2k_1\,, \qquad N(k) = k_1^2 - k_2^2 a\,. \tag{41}$$

Now if $a = d^2$ for d in F, we have $u^2 = d^2$, $(u + d)(u - d) = 0$, whereas u is not in F and $u + d \neq 0$, $u - d \neq 0$. This is impossible in a field.

The quantities of K now consist of all polynomials in u with coefficients in F. For if $k(x)$ is any polynomial in $F[x]$, we may write $k(x) = k_1(x^2) + k_2(x^2)x$, $k(u) = k_1(a) + k_2(a)u$. Thus *every nonmodular quadratic field is the ring* F[u] *of all polynomials with coefficients in* F *in an algebraic root* u *of an equation* $x^2 = a$ *where* a *is in* F, a *is not the square root of any quantity of* F, *and* F *is nonmodular*. Since K is a field, it is actually the field $F(u)$ of all rational functions in u with coefficients in F.

Conversely, if the nonmodular field F and the equation $x^2 = a$ in F are given, then K is defined. For we may take

$$u = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}, \qquad u^2 = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \tag{42}$$

* The trace function is thus called a *linear* function and the norm function a *multiplicative* function.

and identify F with the set of all two-rowed scalar matrices with elements in F (so as to make K contain F). Then every polynomial in u has the form $k = k_1 + k_2u$ and $N(k) = k_1^2 - k_2^2a = 0$ if and only if $k_1 = k_2 = k = 0$. For otherwise $k_2 \neq 0$, $a = (k_1k_2^{-1})^2$ contrary to hypothesis. But then we take $K = F + uF$ and have $k^{-1} = (k_1^2 - k_2^2a)^{-1}(k_1 - k_2u)$ for every k of K. Hence K is the field $F(u)$. That K is nonmodular is evident since the unity element of K is that of F. We have thus constructed all quadratic fields K over a nonmodular field F in terms of equations $x^2 = a$ for a in F, $a \neq d^2$ for any d of F.

Observe in closing that if $K = F(u)$, then $K = F(v)$ for every $v = bu$ such that $b \neq 0$ is in F. But v is a root of

$$x^2 = b^2a\,. \tag{43}$$

Thus we may replace the defining quantity a in F by any multiple b^2a for $b \neq 0$ in F. It is also shown easily that if K is defined by a and K_0 by a_0, then K and K_0 are fields equivalent over F if and only if $a_0 = b^2a$.

10. Integers of quadratic fields. The *Theory of Algebraic Numbers* is concerned principally with the integral domain consisting of the elements called *algebraic integers* in a field K of degree n over the field of all rational numbers. We shall discuss somewhat briefly the case $n = 2$.

Let, then, K be a quadratic field over the rational field so that K is generated by root u of $u^2 = a$ where a is rational and not a rational square. By the use of (43) we may multiply a by an integer and hence take a integral. Write $a = c^2d$ where d has no square factor and c and d are ordinary integers. If we take $b = c^{-1}$ in (43) we replace a by d. Hence every quadratic field is generated by a root u of the quadratic equation

$$x^2 = a = \pm p_1 \ldots p_r\,, \tag{44}$$

where the p_i are distinct positive primes and $r \geq 1$ for $a > 0$, while if $a = -1$ we interpret (44) as the case a negative and $r = 0$.

The quantities k of K have the form $k = k_1 + k_2u$ where k_1 and k_2 are ordinary rational numbers. We call k an integer of K if the coefficients $T(k)$, $N(k)$ of (30) are integers. Thus k is an integer of K if and only if $2k_1$ and $k_1^2 - k_2^2a$ are both ordinary integers. We shall determine all integers of K stating our final results as

Theorem 13. *The integers of a quadratic field* K *form an integral domain* J *containing the ring* E *of all ordinary integers. Then* J *consists of all linear combinations*

$$c_1 + c_2w \tag{45}$$

for c_1 *and* c_2 *in* E, *where* $w = u$ *if* $a \equiv 2 \pmod 4$ *or* $a \equiv 3 \pmod 4$ *but*

$$w = \frac{1+u}{2} \tag{46}$$

if $a \equiv 1 \pmod 4$.

Note that $a \not\equiv 0 \pmod 4$ since a has no square factor. We write

$$k_1 = \frac{b_1}{b_0}, \qquad k_2 = \frac{b_2}{b_0}, \qquad k = \frac{b_1 + b_2 u}{b_0}$$

for b_0, b_1, b_2 in E and b_0 the positive least common denominator of k_1 and k_2. Then 1 is the g.c.d. of b_0, b_1, b_2. Now $2k_1$ is an integer, b_0 divides $2b_1$, $k_1^2 - k_2^2 a = b_0^{-2}(b_1^2 - b_2^2 a)$, so that b_0^2 divides $b_1^2 - b_2^2 a$. If p were an odd prime factor of b_0, it would divide $2b_1$ only if it divided b_1. But then p^2 would divide b_1^2, and p^2 would divide $b_1^2 - b_2^2 a$ as well as $-b_2^2 a$. Since a has no square factors this is possible only if p divides b_2, a contradiction. Hence b_0 is a power of 2. If $b_0 \geq 4$ divides $2b_1$, then 2 divides b_1, 4 divides b_1^2 and $-b_2^2 a$, and thus 2 divides b_2. We have a contradiction and have proved that $b_0 = 1, 2$. If $b_0 = 2$ and b_1 is even, then 4 divides $-b_2^2 a$, and hence 2 divides b_2 contrary to the definition of b_0. Similarly, if b_2 were even, then 4 would divide b_1^2, a contradiction. Hence $b_1 = 2m_1 + 1$, $b_2 = 2m_2 + 1$ for ordinary integers m_1 and m_2, and $b_1^2 - b_2^2 a = 4[m_1^2 + m_1 - a(m_2^2 + m_2)] + 1 - a$ is divisible by 4 if and only if $a \equiv 1 \pmod 4$. Thus we have proved that J consists of the elements (45) with $w = u$ if $a \equiv 2, 3 \pmod 4$. But if $a \equiv 1 \pmod 4$, then we have shown that either $k = b_1 + b_2 u$ with b_1 and b_2 in E, $b_0 = 1$, or $k = m_1 + m_2 u + w$ for w in (46). However, $u = 2w - 1$, and in either case k has the form (45) with c_1 and c_2 in E.

It remains to show that J is an integral domain. The elements of J are in the field K, and thus it suffices to show that $k + h$, kh are in J for every k and h of J. But the sum of k and h of the form (45) is clearly of that form, the product

$$(c_1 + c_2 w)(d_1 + d_2 w) = c_1 d_1 + (c_1 d_2 + c_2 d_1)w + c_2 d_2 w^2$$

is of the form (45) if w^2 is of that form. But this condition holds since if $w = u$ then $w^2 = a + 0w$, while otherwise $u^2 = a = 4m + 1$ for an integer m, $T(w) = \frac{1}{2} + \frac{1}{2} = 1$, $N(w) = \frac{1}{4}(1 - a) = -m$, $w^2 - w - m = 0$,

$$w^2 = m + w\,. \tag{47}$$

This completes the proof.

The units of J are elements k such that $kh = 1$ for h also in J. Then $N(kh) = N(k)N(h) = 1$, $N(k)$ is an ordinary integer which divides unity,

$$N(k) = \pm 1 . \tag{48}$$

Conversely, if (48) holds, k has the property $kk^S = 1$ or -1. But k^S is in J when k is in J since $T(k^S) = T(k)$ and $N(k^S) = N(k)$. Hence $k^S = k^{-1}$ or $-k^S = k^{-1}$. Thus (48) is a necessary and sufficient condition that k be a unit of J.

If $a \equiv 2, 3 \pmod 4$ so that $k = c_1 + c_2 u$, then (48) is equivalent to

$$c_1^2 - c_2^2 a = \pm 1 . \tag{49}$$

However, if $a \equiv 1 \pmod 4$, then (48) becomes $N(k) = c_1^2 + c_1 c_2 - c_2^2 m = \pm 1$ so that $4N(k) = 4c_1^2 + 4c_1 c_2 + c_2^2 - (4m + 1)c_2^2 = \pm 4$. But this is equivalent to

$$(2c_1 + c_2)^2 - c_2^2 a = \pm 4 . \tag{50}$$

We may determine the units of J completely and simply in case a is negative. For both (49) and (50) have the form $x_1^2 + x_2^2 g = \pm 1, \pm 4$ for $g = -a > 0$, and this is possible for ordinary integers x_1 and x_2 and $g > 4$ only if $x_2 = 0$, $c_1 = 1, -1$. Now a has no square factors, and hence $g \neq 4$, the only possible remaining cases are $g = 1, 2, 3$. If $g = 2$ we have $x_1^2 + 2x_2^2 = 1$ only if $x_2 = 0$. Hence we have proved that the units of J are $1, -1$ for every $a < 0$ save only $a = -1, -3$.

Now let $a = -1$ so that (49) becomes $c_1^2 + c_2^2 = 1$. Then one of c_1 and c_2 is zero, the other is 1 or -1, and the units of J are

$$1, u, -u, u^2 = -1 . \tag{51}$$

In the remaining case $a = -3$ we use (50) and have $(2c_1 + c_2)^2 + 3c_2^2 = 4$, and if $c_2 \neq 0$ we must have $c_2 = \pm 1$, $2c_1 + c_2 = \pm 1$ with any choice of signs. Then $c_2 = 1$ gives $c_1 = 0$ or -1, while $c_2 = -1$ gives 0 or 1 for c_1. Clearly, the units of J are

$$1, -1, w, -w, w^S, -w^S . \tag{52}$$

The units of J form a multiplicative group, and we have shown that if a is negative this group is a finite group.

If $a = 2$, then $h = 3 + 2u$ has norm $9 - 4u^2 = 9 - 8 = 1$. Hence h is a unit of J, and so is h^t for every integer t. If $h^t = h^s$ for $s \neq t$, we may take $t > s$ and have $h^{t-s} = 1$. But we may regard u as the ordinary positive $\sqrt{2}$

and have $h > 5$, $h^{t-s} > 5^{t-s} > 1$. Hence the multiplicative group of the units of J is an *infinite* group. *It may similarly be shown to be infinite for every positive* a.

We shall not study the units of quadratic fields further but shall pass on to some results on primes and prime ideals in two special cases.

11. Gauss numbers. The complex numbers of the form $x + yi$ with rational x and y are called the *Gauss complex numbers*, and those for which x and y are integers are called the *Gauss integers*. Then the Gauss complex numbers are the elements of a quadratic field K of our study with

$$u^2 = -1,$$

and the Gauss integers comprise its integral domain J. We have determined the units ± 1, $\pm u$ of J and shall now study its divisibility properties. Our first result is the *Division Algorithm* which we state as

Theorem 14. *Let* f *and* g $\neq 0$ *be in* J. *Then there exist elements* h *and* r *in* J *such that*

$$\mathrm{f} = \mathrm{gh} + \mathrm{r} \tag{53}$$

and $0 \leq \mathrm{N(r)} < \mathrm{N(g)}$.

For fg^{-1} is in K, $fg^{-1} = k_1 + k_2 u$ with rational k_1 and k_2. Every rational number t lies in an interval $s \leq t < s + 1$ for an ordinary integer s. If $s \leq t < s + \frac{1}{2}$ then $(t - s) \leq \frac{1}{2}$, while if $s + \frac{1}{2} \leq t < s + 1$ then $|t - (s + 1)| \leq \frac{1}{2}$. Hence there exist ordinary integers h_1 and h_2 such that

$$s_1 = k_1 - h_1, \quad s_2 = k_2 - h_2, \quad |s_1| \leq \tfrac{1}{2}, \quad |s_2| \leq \tfrac{1}{2}. \tag{54}$$

Put $h = h_1 + h_2 u$, $s = s_1 + s_2 u$, $r = sg$ so that $fg^{-1} = h + s$, $f = gh + sg = gh + r$. Then $N(s) = s_1^2 + s_2^2 \leq \frac{1}{2}$, $N(r) = N(s)N(g) < N(g)$ as desired.

We observe that the quotient h and the remainder r *need not be unique* in our present case. For example, if $f = 2 + u$ and $g = 1 + u$, we have $N(g) = 2$. Then $f = 1 \cdot g + 1 = 2 \cdot g - u$ with $N(1) = N(-u) = 1$.

We shall use the *Division Algorithm* to prove the existence of a g.c.d. Our proof will be different and simpler than that we gave in the case of polynomials and indicated in the case of integers but has the defect of being merely existential and not constructive. We first prove

Theorem 15. *Every ideal* M *of* J *is a principal ideal.*

For the norms of the nonzero elements of M are positive integers, and there exists an $m \neq 0$ in M such that $N(m) \leq N(f)$ for every f of M. By

Theorem 14 we have $f = mh + r$ for h and r in J and $N(r) < N(m)$. But f, m and mh are in M, so is $r = f - mh$, and it follows that r must be zero. Thus $f = mh$, $M = \{m\}$.

The above result then implies

Theorem 16. *Let* f *and* g *be nonzero elements of* J. *Then there exist* b *and* c *in* J *such that*

$$\mathrm{d} = \mathrm{bf} + \mathrm{cg} \tag{55}$$

is a common divisor of f *and* g. *Thus* d *is a g.c.d. of* f *and* g.

For the set of all elements of the form $xf + yg$ with x and y in J is an ideal M of J. By Theorem 15 we have $M = \{d\}$, d in M has the form (55) and divides $f = 1 \cdot f + 0g$, and $g = 0 \cdot f + 1 \cdot g$ in M.

The above result may now be seen to imply that if f divides gh and is prime to g, then f divides h, and also if p is a prime of J dividing gh, then p divides g or h. Moreover, if f is a composite integer of J, then $f = gh$ for nonunit g and h, $N(g) < N(f)$. Then if p is a divisor of f of least positive norm it is a prime divisor of f, and we continue the proof of Theorem 6 to obtain

Theorem 17. *Every composite Gauss integer is expressible as a product*

$$\mathrm{f} = \mathrm{p}_1 \cdots \mathrm{p}_r \tag{56}$$

of primes p_i *which are determined uniquely by* f *apart from their order and unit multipliers.*

We observe that Theorem 17 implies that an ideal M of J is a prime ideal (and, in fact, a divisorless ideal) if and only if $M = \{d\}$ for a prime d of J. Let us then determine the prime quantities $d = d_1 + d_2 u$ of J. We see first that if d is a prime of J, so is $d^S = d_1 - d_2 u$. For if $d^S = gh$ with $N(g) \neq 1$, $N(h) \neq 1$, we have $d = g^S h^S$ for $N(g^S) = N(g)$, $N(h^S) = N(h)$, and d is composite. We now prove

Theorem 18. *A positive prime* p *of* E *is either a prime of* J *or the product* $\mathrm{N(d)} = \mathrm{dd}^S$, *where* d *is a prime of* J. *Every prime* d *of* J *is either associated with a positive prime of* E *or arises from the factorization in* J *of a positive prime* $\mathrm{p} = \mathrm{dd}^S$ *of* E *which is composite in* J.

For if p is a positive prime of E and is composite in J, then $p = dk$ for $N(d) > 1, N(k) > 1, N(p) = p^2 = N(d)N(k)$. But then $p = N(d)$. If $d = gh$ with $N(g) > 1$, then $N(d) = p = N(g)N(h)$ so that $N(h) = 1$, h is a unit, d is a prime. Conversely, let d be a prime of J. Then $c = N(d)$ is a positive integer of E and is either a prime or is composite. But $c = dd^S$ can have at most two prime factors in E, $c = pp_0$ for positive primes p and p_0

of E. We may assume that p is associated with d and p_0 with d^S so that $p_0^S = p_0$ is associated with d and with p. Since p and p_0 are both in E, we have $p_0 = \pm p$. But p and p_0 are positive and must be equal, $N(d) = p^2$. Therefore d is associated with the prime p of E which is prime in J.

We now clearly complete our study of the primes of J by proving

Theorem 19. *A positive prime* p *of* E *is a prime of* J *if and only if* p *has the form* 4m + 3.

To prove this result we observe first that if t is an odd integer of E we have $t = 2s + 1$, $t^2 = 4s^2 + 4s + 1 = 4s(s + 1) + 1$. One of s and $s + 1$ is even, $t^2 = 8r + 1 \equiv 1 \pmod 8$. If t is even, we have $t^2 \equiv 0 \pmod 4$ and $t^2 \equiv 0, 4 \pmod 8$. Thus a sum of two squares is congruent to 0, 1, 2, 4, or 5 *modulo* 8 while $4n + 3$ is congruent 3 or 7 *modulo* 8. It follows that $p = 4n + 3 \neq x^2 + y^2$. We now assume that $p = gh$ for g and h in J and have $p^2 = N(p) = N(g)N(h)$. If neither g nor h were a unit, we would have $N(g) > 1$, and both of these integers would be divisors of p^2. But then $N(g) = N(h) = p = x^2 + y^2$, which is impossible. Hence, $p = 4n + 3$ is prime in J. We note that $2 = 1 + 1 = (1 + u)(1 - u)$ is composite in J and that it remains to show that $p = 4n + 1$ is composite in J. We know by Theorem 12 that there exists an integer b in E such that $b^2 + 1$ is divisible by p. If p divides $b + u$ or $b - u$, then $b \pm u = p(k_1 + k_2 u)$, and $\pm 1 = pk_2$, which is impossible. But a prime p of J cannot divide the product $(b + u)(b - u) = b^2 + 1$ without dividing one of its factors $b + u$, $b - u$. Hence p is not a prime of J. This completes the proof.

We use the result above to derive an interesting theorem of the *Theory of Numbers*. We call a positive integer c a sum of two squares if $c = x^2 + y^2$ for x and y in E. Then we have

Theorem 20. *Write* c = f²g *where* f *and* g *are positive integers and* g *has no square factors. Then* c *is a sum of two squares if and only if no prime factor of* g *has the form* 4n + 3.

For if $c = x^2 + y^2 = (x + yu)(x - yu)$, we may write $x + yu = d_1 \ldots d_r$ for primes d_i in J, $c = N(d_1) \ldots N(d_r)$. Then $N(d_i) = p_i$ is a prime of E if and only if $p_i \neq 4n + 3$ and otherwise $N(d_i) = p_i^2$. Thus the prime factors of c of the form $4n + 3$ occur to even powers and are not factors of g. Conversely, if $g = p_1 \ldots p_r$ for positive primes p_i of E not of the form $4n + 3$, we have $p_i = N(d_i)$ for d_i in J, $g = N(d_1) \ldots N(d_r) = N(d_1 \ldots d_r)$, and $c = N(fd_1 \ldots d_r) = N(k) = x^2 + y^2$ for $k = x + yu$ in J.

Note in closing that a positive prime p of the form $4n + 3$ divides $x^2 + y^2$ if and only if p divides both x and y. For p is a prime of J and divides $(x + yu)(x - yu)$ if and only if p divides either $x + yu$ or $x - yu$. Then

$x \pm yu = p(k_1 \pm k_2 u)$, $x = pk_1$, $y = pk_2$ for integers k_1 and k_2 of E. It follows, then, that if x, y, z are ordinary integers such that

$$x^2 + y^2 = z^2, \tag{57}$$

every prime divisor $p = 4n + 3$ of z divides both x and y. Then let x, y, z, have g.c.d. unity. It follows that the odd prime divisors of z have the form $4n + 1$. We may show readily also that x and y cannot both be even or be odd and that z must be odd.*

12. An integral domain with nonprincipal ideals. We shall close our exposition with a discussion of some properties of the ring J of integers of the field K defined by $a = u^2 = -5$. Since $-5 \equiv 3 \pmod 4$, the elements of J have the form $k_1 + k_2 u$ for k_1 and k_2 in the set E of all integers. Observe that if b is an integer of E which is a divisor in J of $k_1 + k_2 u$, then b must divide both k_1 and k_2. For $k_1 + k_2 u = b(h_1 + h_2 u)$, $k_1 = bh_1$, $k_2 = bh_2$. We now prove

Theorem 22. *The elements* 3, 7, $1 + 2u$, $1 - 2u$ *are primes of* J *no two of which are associated.*

For if k is a composite of J we have $k = gh$, $N(k) = N(g)N(h)$ for ordinary integral proper divisors $N(g)$ and $N(h)$ of $N(k)$. The norms of the integers of our theorem are 9, 49, 21, 21, respectively, and the only positive proper divisors of these norms are 3, 7. But if $g = g_1 + g_2 u$, we have $N(g) = g_1^2 + 5g_2^2 > 0$, $g_1^2 + 5g_2^2 = 3, 7$. Evidently $g_2 \neq 0$, $g_2^2 \leq 1$. But $g_2^2 = 1$ is impossible since $g_1^2 \neq -2, 2$. Thus 3, 7, $1 + 2u$, $1 - 2u$ are primes of J. The units of J are 1, -1, and clearly no two of them are associated.

We see now that $21 = 3 \cdot 7 = (1 + 2u)(1 - 2u)$, and we have factored 21 into prime factors in J in two distinct ways. Moreover, the principal ideal $\{3\}$ of J defined for the prime 3 is not a prime ideal. For 3 does not divide $1 + 2u$ and $1 - 2u$ in J yet does divide their product, and therefore the residue class ring $J - \{3\}$ contains $\underline{1 + 2u}$ and $\underline{1 - 2u}$ as divisors of zero.

The ring J contains nonprincipal ideals one of which we shall exhibit. We let M be the ideal of J consisting of all elements of J of the form

$$3x + y(1 + 2u) \qquad (x, y \text{ in } J). \tag{58}$$

If this ideal were a principal ideal $\{d\}$, there would exist a common divisor d of 3 and $1 + 2u$. Since these are nonassociated primes, d must be a unit

* For further results see L. E. Dickson's *Introduction to the Theory of Numbers*, pp. 40–42.

1 or -1 of J, and $\{d\} = \{1\}$. Then $1 = 3b + (1 + 2u)c$ for b and c in J, $7 = 21b + (1 + 2u)7c = (1 + 2u)[b(1 - 2u) + 7c]$. But $1 + 2u$ does not divide 7, a contradiction. We now proceed to prove that M is a divisorless ideal of J and hence is a prime ideal of J.

We have shown that M is not a principal ideal and does not contain 1. Since M contains 3 but not 1 it cannot contain 2. For otherwise $3 - 2 = 1$ would be in M. Let c be an integer of E in M so that $c = 3q + r$ where $r = 0, 1, 2$. Since M contains $3q$ it contains $c - 3q = r$, $r = 0$. Hence the ordinary integers in M are divisible by 3.

The ideal M contains 3 and $1 + 2u$ and so contains

$$w_1 = 3\,, \qquad w_2 = 3u - (1 + 2u) = u - 1\,, \tag{59}$$

If h is in M, then $h = h_0 + h_2 u$ for h_0 and h_2 in E, $h - h_2 w_2 = h_0 + h_2$ in E and in M. By the proof above $h_0 + h_2 = 3h_1$ for h_1 in E,

$$h = h_1 w_1 + h_2 w_2\,. \tag{60}$$

We have thus proved that M consists of all quantities of the form (60) for h_1 and h_2 ordinary integers. Thus we may call w_1, w_2 a *basis of* M *over* E. Note that $\{1\}$ has a basis 1, u over E in this sense. It may be shown that every ideal of J has a basis of two elements over E.

Every integer of J has the form $k = k_1 + k_2 u = k_1 + k_2 w_2 + k_2$. Write $k_1 + k_2 = 3c + r$ for c in E and $r = 0, 1, 2$. Then $k = cw_1 + k_2 w_2 + r \equiv r\,(M)$, the elements of $J - M$ are the residue classes $\underline{0}$, $\underline{1}$, $\underline{2}$ such that $\underline{3} = \underline{0}$. We have proved that $J - M$ is equivalent to $E - \{3\}$ and is a field, M is a divisorless ideal of J.

This completes our discussion of ideals and of quadratic fields. We shall conclude our text with the following brief bibliographical summary.

Let us begin with references to standard topics on matrices not covered in our introductory exposition. The theory of orthogonal and unitary equivalence of symmetric matrices is contained with generalizations in Chapter V of the *Modern Higher Algebra* and is further generalized and connected with the theory of equivalence of pairs of matrices in the author's paper entitled "Symmetric and Alternate Matrices in an Arbitrary Field," in *Transactions of the American Mathematical Society*, XLIII (1938), 386–436. See also pages 74–76 and Chapter VI of L. E. Dickson's *Modern Algebraic Theories*, and Chapter VI of J. M. H. Wedderburn's *Lectures on Matrices*. Both of these texts as well as Chapters III, IV, and V of the *Modern Higher Algebra* include, of course, all the material of our Chapters II–V. For a discussion

without details but with complete references of many other topics on matrices see C. C. MacDuffee, *The Theory of Matrices* ("Ergebnisse der Mathematik und ihrer Grenzgebiete," Vol. II, No. 5 [pp. 110]).

The theory of rings as given here is contained in the detailed discussion of Chapters I and II of the *Modern Higher Algebra*, and the theory of ideals in Chapter XI. See also the much more extensive treatment in Van der Waerden's *Moderne Algebra*. The units of the ring of integers of a quadratic field are discussed on page 233 of R. Fricke's *Algebra*, Volume III, and its ideals on pages 106–10 of H. Hecke's *Theorie der algebräischen Zahlen*. We close with a reference to the only recent book in English on algebraic number theory, H. Weyl's *Algebraic Theory of Numbers* (Princeton, 1940).

INDEX

PRINTED IN U.S.A.