THE PARASTROPHIC CRITERION FOR THE FACTORIZATION OF PRIMES

BY

FRED KIOKEMEISTER

If the rational prime p is not an extraordinary divisor of the discriminant of the irreducible polynomial $f(x)$ with coefficients in the domain of rational integers, the factorization of $f(x)$ modulo p gives the factorization of the principal ideal (p) in the maximal domain of integrity of the algebraic number field defined by $f(x)$. This criterion was given by Zolotareff[1] and discussed by Dedekind[2]. Hilbert, by relating the structure of (p) to the factorization modulo p of the minimal polynomial of the general element of the maximal domain of integrity[3], removed the necessity of separately considering the divisors of the discriminant. The parastrophic criterion here presented serves the same purpose with what is perhaps a method involving a simpler computation.

Parts 2 and 4 of the paper are related to the work of Nakayama and Nesbitt[4] on the representations of Frobenius algebras and to the study of such algebras by Nakayama[5].

1. **The parastrophic matrix.** Let A be a linear associative algebra with basis $e_1, e_2, \cdots, e_n$ over a field P. We designate the vectors of basis elements as follows:

$$u = (e_1, e_2, \cdots, e_n), \qquad u' = \begin{bmatrix} e_1 \\ e_2 \\ \cdot \\ \cdot \\ e_n \end{bmatrix},$$

so that the vector u' is the transpose of u. We shall be consistent in employing this notation for a vector and its transpose throughout the paper. From the theory[6] of the matric representations of a linear algebra, we have for an element a contained in A.

$$au = uR(a), \qquad u'a = S(a)u', \tag{1.1}$$

Presented to the Society April 12, 1941; received by the editors July 30, 1940.

(1) G. Zolotareff, *Théories des Nombres Entiers Complexes, avec une Application au Calcul Intégral*, St. Petersburg, 1874.

(2) Dedekind, Göttingen Abhandlungen, vol. 23 (1878).

(3) Hilbert, *Die Theorie der algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 4 (1894–1895), p. 195.

(4) Nakayama and Nesbitt, Annals of Mathematics, (2), vol. 39 (1938), pp. 659–668.

(5) Nakayama, Annals of Mathematics, (2), vol. 40 (1939), pp. 611–633.

(6) M. Deuring, *Algebren*, Berlin, 1935, p. 2.

where $R(a)$ and $S(a)$ are, respectively, the first and second representations of a. The elements of the vectors au and $u'a$ are linear forms in the basis elements $e_1, e_2, \cdots, e_n$ with coefficients in P; the elements of the matrices $R(a)$ and $S(a)$ are uniquely determined in P.

The multiplication table of the algebra A can be given as the outer product of the vectors u' and u:

$$u'u = \begin{bmatrix} e_1^2 & e_1e_2 \cdots e_1e_n \\ e_2e_1 & e_2^2 \cdots e_2e_n \\ \cdot & \cdot \cdots \cdot \\ \cdot & \cdot \cdots \cdot \\ e_ne_1 & \cdot \cdots e_n^2 \end{bmatrix} = \begin{bmatrix} e_1u \\ e_2u \\ \cdot \\ \cdot \\ e_nu \end{bmatrix} = (u'e_1, u'e_2, \cdots, u'e_n).$$

Employing equations (1.1), we have immediately

$$u'u = \begin{bmatrix} uR_1 \\ uR_2 \\ \cdot \\ \cdot \\ uR_n \end{bmatrix} = (S_1u', S_2u', \cdots, S_nu') \tag{1.2}$$

where $R_i = R(e_i)$, $S_i = S(e_i)$. The matrix $u'u$ has as elements linear forms in the basis elements. We shall designate $u'u$ by $Q(u)$. The array $Q(u)$ is uniquely defined by the basis u employed in the representation of the algebra A. The algebra is determined up to an isomorphic ring and isomorphic basis by $Q(u)$.

Frobenius defined the parastrophic matrix[7] of an algebra A to be that derived from $Q(u)$ by replacing each basis element e_i by the variable x_i. This replacement may be achieved by the substitution of $\xi = (x_1, x_2, \cdots, x_n)$ for u and ξ' for u' in the forms (1.2). In this notation the parastrophic matrix is

$$Q(\xi) = \begin{bmatrix} \xi R_1 \\ \xi R_2 \\ \cdot \\ \cdot \\ \xi R_n \end{bmatrix} = (S_1\xi', S_2\xi', \cdots, S_n\xi'). \tag{1.3}$$

The variables $x_1, x_2, \cdots, x_n$ range over P.

THEOREM 1.1. *If* $\xi = (x_1, x_2, \cdots, x_n)$, $\eta = (y_1, y_2, \cdots, y_n)$ *and if* α_1, α_2 *are elements of* P,

$$Q(\alpha_1\xi + \alpha_2\eta) = \alpha_1Q(\xi) + \alpha_2Q(\eta).$$

The theorem follows from equation (1.3); for

(7) Sitzungsberichte der Preussischen Akademie der Wissenschaften, 1903, p. 507.

$$Q(\alpha_1\xi + \alpha_2\eta) = \begin{bmatrix} (\alpha_1\xi + \alpha_2\eta)R_1 \\ (\alpha_1\xi + \alpha_2\eta)R_2 \\ \vdots \\ (\alpha_1\xi + \alpha_2\eta)R_n \end{bmatrix} = \alpha_1 \begin{bmatrix} \xi R_1 \\ \xi R_2 \\ \vdots \\ \xi R_n \end{bmatrix} + \alpha_2 \begin{bmatrix} \eta R_1 \\ \eta R_2 \\ \vdots \\ \eta R_n \end{bmatrix} = \alpha_1 Q(\xi) + \alpha_2 Q(\eta).$$

Let $a = \alpha_1 e_1 + \alpha_2 e_2 + \cdots + \alpha_n e_n$, $\alpha_i \in P$, be an element of A. Then $\bar{a} = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ is the unique vector representation of a with respect to the basis u. Employing the inner product of vectors, we have

$$a = \bar{a}u' = u\bar{a}'. \tag{1.4}$$

The vector representation of the elements of the algebra A has the following properties:

THEOREM 1.2. *For any elements a and b in A,*

(a) $\overline{\alpha a} = \alpha\bar{a}$, $\alpha \in P$.

(b) $\overline{a+b} = \bar{a} + \bar{b}$.

(c) $(\overline{ab})' = R(a)\bar{b}'$, $\overline{ab} = \bar{a}S(b)$.

Parts (a) and (b) of the theorem follow from the definition of an algebra.

For the proof of part (c), let a and b be two elements of A. Consider that by equation (1.4)

$$ab = a(u\bar{b}') = (au)\bar{b}'.$$

Then by (1.1)

$$ab = (uR(a))\bar{b}' = u(R(a)\bar{b}').$$

It follows from the uniqueness of the vector representation that

$$(\overline{ab})' = R(a)\bar{b}'.$$

Similarly

$$\overline{ab} = \bar{a}S(b).$$

THEOREM 1.3. *For any element a of the algebra A, the relations hold:*

$$\bar{a}Q(\xi) = \xi R(a), \qquad Q(\xi)\bar{a}' = S(a)\xi'$$

where $\xi = (x_1, x_2, \cdots, x_n)$, and $Q(\xi)$ is the parastrophic matrix of the fixed basis u.

Since $\bar{a}u' = a$,

$$\bar{a}u'u = \bar{a}Q(u) = au = uR(a),$$

so that

$$\bar{a}Q(u) = uR(a).$$

Here we have the equality of two vectors with elements which are linear forms

in the basis elements $e_1, e_2, \cdots, e_n$. The basis elements are linearly independent, and the linear forms must be identical. Since $\bar{a}$ and $R(a)$ have elements in the field P, we may replace $u=(e_1, e_2, \cdots, e_n)$ by $\xi=(x_1, x_2, \cdots, x_n)$:

$$\bar{a}Q(\xi) = \xi R(a).$$

Similarly $u\bar{a}'=a$,

$$u'u\bar{a}' = Q(u)\bar{a}' = u'a = S(a)u',$$

and

$$Q(u)\bar{a}' = S(a)u'.$$

This gives

$$Q(\xi)\bar{a}' = S(a)\xi'$$

by the same argument as above.

An algebra A is said to be a *Frobenius algebra* when there exists a vector $\eta=(\delta_1, \delta_2, \cdots, \delta_n)$ with elements δ_i in P such that $Q(\eta)$ is nonsingular.

2. **Orthogonal modules.** In this section we shall assume that the algebra A has an identity e. Any linear algebra not a null algebra is homomorphic to an algebra with identity.

LEMMA 2.1. *If A has an identity e, $Q(\eta)=0$ implies that $\eta=(0, 0, \cdots, 0)$.*

Let Theorem 1.3 be applied to the element e and the vector η where $Q(\eta)=0$:

$$\bar{e}Q(\eta) = \eta R(e) = \eta.$$

Then if $Q(\eta)=0$, $\eta=0$.

Let M designate the set of all vectors $\eta=(\delta_1, \delta_2, \cdots, \delta_n)$ where $\delta_1, \delta_2, \cdots, \delta_n$ are elements of P, i.e., M is the set of all constant vectors when the variables x_i of $\xi=(x_1, x_2, \cdots, x_n)$ are allowed to run over P.

LEMMA 2.2. *If D is a set of elements d in A, the set $U(D)$ of all $\eta \in M$ such that for all $d \in D$*

$$\bar{d}Q(\eta) = 0$$

forms a P-module closed on the right under multiplication by all $S^{\tau}(x)$, $x \in A$. The set $V(D)$ of all $\eta \in M$ such that for all $d \in D$

$$Q(\eta)\bar{d}' = 0$$

forms a P-module closed on the right under multiplication by $R(x)$, $x \in A$.

Let η_1, η_2 be such that

$$\bar{d}Q(\eta_i) = 0, \qquad d \in D.$$

Then for all $d \in D$, by Theorem 1.1,

$$\bar{d}Q(\alpha_1\eta_1 + \alpha_2\eta_2) = \alpha_1\bar{d}Q(\eta_1) + \alpha_2\bar{d}Q(\eta_2) = 0$$

and $U(D)$ includes all linear forms in η_1, η_2 with coefficients in P, i.e., $U(D)$ is a P-module. Furthermore, since, for the general vector ξ, $\bar{d}Q(\xi) = \xi R(d)$ (Theorem 1.3), $\bar{d}Q(\eta) = 0$ implies that

$$\bar{d}Q(\eta S^{\mathsf{T}}(x)) = \eta S^{\mathsf{T}}(x)R(d) = \eta R(d)S^{\mathsf{T}}(x) = 0$$

for all $d \in D$, and $x \in A$ by the commutivity of $R(d)$ with $S^{\mathsf{T}}(x)$ as established by Frobenius([8]). It follows that $\eta S^{\mathsf{T}}(x)$ is an element of $U(D)$ whenever η is, and $U(D)$ is closed on the right under multiplication by all $S^{\mathsf{T}}(x)$.

The second part of the theorem is proved by applying the same argument to the relation $Q(\xi)\bar{d}' = S(d)\xi'$.

For any theorem which is proved for right ideals in the following pages there exists an analogous theorem for left ideals. Since the argument in each case is the same, we shall state the theorems in most instances only for right ideals.

LEMMA 2.3. *If N is a subset of the module M, the set $\mathfrak{a}$ of elements $a \in A$ such that*

$$\bar{a}Q(\eta) = 0$$

for all $\eta \in N$ forms a right ideal in A. Furthermore, $U(\mathfrak{a}) \subseteq N$.

Let a_1 and a_2 be elements of $\mathfrak{a}$. Then for all $\eta \in N$

$$\overline{(\alpha_1 a_1 + \alpha_2 a_2)}Q(\eta) = (\alpha_1\bar{a}_1 + \alpha_2\bar{a}_2)Q(\eta) = \alpha_1\bar{a}_1Q(\eta) + \alpha_2\bar{a}_2Q(\eta) = 0$$

where α_1, α_2 are elements of P, and $\mathfrak{a}$ is a P-module. The set $\mathfrak{a}$ is a right ideal; for let a be an element of $\mathfrak{a}$, c an element of A. Then by Lemma 1.2

$$\overline{ac} = \bar{a}S(c).$$

Frobenius established that

$$S(c)Q(\eta) = Q(\eta)R(c).$$

Employing these results, we have

$$\overline{ac}Q(\eta) = \bar{a}S(c)Q(\eta) = \bar{a}Q(\eta)R(c) = 0$$

for all c in A. Hence ac lies in $\mathfrak{a}$, and $\mathfrak{a}$ is a right ideal. By the definition of $U(\mathfrak{a})$, this set must include N.

The order of an ideal $\mathfrak{a}$ is the order with respect to the basis field P; $\mathfrak{a}$ is of order r if r linearly independent elements constitute a P-basis for $\mathfrak{a}$.

([8]) Frobenius, ibid., p. 507.

LEMMA 2.4. *If $\mathfrak{a}$ is a right ideal of order r, $U(\mathfrak{a})$ is a P-module of order $n-r$.*

If $\mathfrak{a}=A$, then $r=n$. As in the proof of Lemma 2.1, $\bar{e}Q(\eta)=0$ implies that η is the zero vector. Then $U(\mathfrak{a})=0$, and the theorem holds.

If $\mathfrak{a}=0$, then $r=0$. Let $\bar{0}$ designate the zero vector which represents the element 0 of the algebra. Every vector η satisfies the equation $\bar{0}Q(\eta)=0$, so that $U(\mathfrak{a})$ is of order n. In this special case also the theorem holds.

If $\mathfrak{a}\neq A$ and $\mathfrak{a}\neq 0$, then $\mathfrak{a}$ has a basis $v=(a_1, a_2, \cdots, a_r)$. Let $s_v=(e_1, e_2, \cdots, e_{n-r})$ be a set of elements supplementary to v so that $u=(s_v, v)$ is a basis of A. Since $\mathfrak{a}\neq A$, e is not included in $\mathfrak{a}$, so we may choose e_1 equal to the identity element of A.

If we employ $u=(s_v, v)$ to form $Q(u)$, we have

$$Q(u) = u'u = (s_v, v)'(s_v, v) = \begin{bmatrix} s_v's_v & s_v'v \\ v's_v & v'v \end{bmatrix}.$$

Since $\mathfrak{a}$ is a right ideal, every element of $v's_v$ and $v'v$ is expressible in terms of the basis v. Writing $Q(u)$ as a matrix of single elements, we have

$$Q(u) = \begin{bmatrix} e_1, & e_2, \cdots, e_{n-r}, & a_1, \cdots, a_r \\ e_2, & \cdot & \cdot \quad \cdot \quad \cdot \\ \cdot & \cdot & \cdot \quad \cdot \quad \cdot \\ e_{n-r}, & \cdot & \cdot \quad \cdot \quad \cdot \\ \cdot & \cdot & \cdot \quad \cdot \quad \cdot \\ a_1, & \cdot & \cdot \quad \cdot \quad \cdot \\ \cdot & \cdot & \cdot \quad \cdot \quad \cdot \\ a_r, & \cdot & \cdot \quad \cdot \quad \cdot \end{bmatrix}$$

where every element of $Q(u)$ in any row below the $(n-r)$th row must be expressed in the basis v. We pass by substitution of $\xi=(x_1, x_2, \cdots, x_n)$ for the basis vector u to the parastrophic matrix $Q(\xi)$ and then set $x_i=\alpha_i\in P$, $\eta=(\alpha_1, \alpha_2, \cdots, \alpha_n)$:

$$Q(\eta) = \begin{bmatrix} \alpha_1, & \alpha_2, \cdots, \alpha_{n-r}, & \alpha_{n-r+1}, \cdots, \alpha_n \\ \alpha_2, & \cdot & \cdot \quad \cdot \quad \cdot \\ \cdot & \cdot & \cdot \quad \cdot \quad \cdot \\ \alpha_{n-r}, & \cdot & \cdot \quad \cdot \quad \cdot \\ \cdot & \cdot & \cdot \quad \cdot \quad \cdot \\ \alpha_{n-r+1}, & \cdot & \cdot \quad \cdot \quad \cdot \\ \cdot & \cdot & \cdot \quad \cdot \quad \cdot \\ \alpha_n, & \cdot & \cdot \quad \cdot \quad \cdot \end{bmatrix}$$

where the elements of any row below the $(n-r)$th are linear forms in $\alpha_{n-r+1}, \cdots, \alpha_n$. Now if $a \in \mathfrak{a}$,

$$\bar{a} = (0, \cdots, 0, \beta_{n-r+1}, \cdots, \beta_n) \qquad \text{where } \beta_i \in P.$$

Obviously if we choose $\alpha_j = 0$ for $j = n-r+1, \cdots, n$, then

$$\bar{a}Q(\eta) = 0$$

for any choice of $\alpha_1, \alpha_2, \cdots, \alpha_{n-r}$. For in this case every element below the $(n-r)$th row is zero. Conversely if $\bar{a}Q(\eta) = 0$ for all $a \in \mathfrak{a}$, then in particular

$$\beta_{n-r+1}\alpha_{n-r+1} + \cdots + \beta_n\alpha_n = 0$$

for all $\beta_j \in P$. This linear form is identically zero only if the α_j involved are all zero.

It follows that $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_{n-r}, 0, \cdots, 0)$ is the most general vector such that

$$\bar{a}Q(\eta) = 0$$

for all $a \in \mathfrak{a}$. But $U(\mathfrak{a})$ is this set of vectors, and is therefore of order $n-r$.

If there exists a vector η such that $\eta R(a) = 0$, η is said to be *orthogonal on the left* to $R(a)$. Let a be an element of the right ideal $\mathfrak{a}$. From the relation

$$\bar{a}Q(\eta) = \eta R(a),$$

we see that $\eta R(a) = 0$ for all $a \in \mathfrak{a}$ implies that $\bar{a}Q(\eta) = 0$ and conversely. That is, η must lie in $U(\mathfrak{a})$. Similarly if $\mathfrak{b}$ is a left ideal, $V(\mathfrak{b})$ is the set of all vectors such that

$$Q(\eta)\bar{b}' = S(b)\eta' = 0,$$

and η is *orthogonal on the right* to all $S(b)$ where b lies in $\mathfrak{b}$.

THEOREM 2.1. *If $\mathfrak{a}$ is a right ideal, then $U(\mathfrak{a})$ is the set of vectors orthogonal on the left to all $R(a)$, $a \in \mathfrak{a}$. If $\mathfrak{b}$ is a left ideal, $V(\mathfrak{b})$ is the set of all vectors orthogonal on the right to all $S(b)$, $b \in \mathfrak{b}$.*

The vector sets $U(\mathfrak{a})$ and $V(\mathfrak{b})$ are called the *orthogonal sets* of the right ideal $\mathfrak{a}$ and the left ideal $\mathfrak{b}$, respectively.

LEMMA 2.5. (a) $U(a) = 0$, $U(0) = M$. *If $U_i = U(\mathfrak{a}_i)$, where $\mathfrak{a}_i$ is a right ideal,* (b) $\mathfrak{a}_1 \supset \mathfrak{a}_2$ *if and only if* $U_1 \subset U_2$, (c) $U(\mathfrak{a}_1, \mathfrak{a}_2) = U_1 \wedge U_2$, $U(\mathfrak{a}_1 \wedge \mathfrak{a}_2) = (U_1, U_2)$.

Part (a) follows immediately from Lemma 2.4.

Part (b): Let $a_i \in \mathfrak{a}_i$, $\eta_i \in U_i$. Then

$$\bar{a}_1 Q(\eta_1) = 0$$

for all a_1 in $\mathfrak{a}_1$. In particular

$$a_2 \in \mathfrak{a}_2 \subset \mathfrak{a}_1,$$

and hence

$$\bar{a}_2 Q(\eta_1) = 0$$

so that all η_1 are elements of U_2, or $U_1 \subset U_2$.

Part (c): If $\eta \in U_1 \wedge U_2$, then $\bar{a}Q(\eta) = 0$ for all $a \in (\mathfrak{a}_1, \mathfrak{a}_2)$ so that

$$U_1 \wedge U_2 \subseteq U(\mathfrak{a}_1, \mathfrak{a}_2).$$

By (b) above, and since $\mathfrak{a}_i \subset (\mathfrak{a}_1, \mathfrak{a}_2)$,

$$U_i \supset U(\mathfrak{a}_1, \mathfrak{a}_2), \qquad U_1 \wedge U_2 \supseteq U(\mathfrak{a}_1, \mathfrak{a}_2).$$

Finally these two relations together imply that

$$U_1 \wedge U_2 = U(\mathfrak{a}_1, \mathfrak{a}_2).$$

Similarly, let $\eta \in (U_1, U_2)$. Then $\bar{a}Q(\eta) = 0$ for all $a \in (\mathfrak{a}_1 \wedge \mathfrak{a}_2)$ so that

$$(U_1, U_2) \subseteq (\mathfrak{a}_1 \wedge \mathfrak{a}_2).$$

However, if $\mathfrak{a}_i$ is of order r_i, by Lemma 2.4

$$\begin{aligned} \text{order } (U_1, U_2) &= \text{order } U_1 + \text{order } U_2 - \text{order } (U_1 \wedge U_2) \\ &= n - r_1 + n - r_2 - \text{order } (U_1 \wedge U_2), \end{aligned}$$

From the equation $(U_1 \wedge U_2) = U(\mathfrak{a}_1, \mathfrak{a}_2)$ we have

$$\text{order } (U_1 \wedge U_2) = n - \text{order } (\mathfrak{a}_1, \mathfrak{a}_2).$$

and we know that

$$\text{order } (\mathfrak{a}_1, \mathfrak{a}_2) = r_1 + r_2 - \text{order } (\mathfrak{a}_1 \wedge \mathfrak{a}_2),$$

so that

$$\text{order } (U_1, U_2) = n - \text{order } (\mathfrak{a}_1 \wedge \mathfrak{a}_2) = \text{order } U(\mathfrak{a}_1 \wedge \mathfrak{a}_2).$$

We have proved that $U(\mathfrak{a}_1 \wedge \mathfrak{a}_2)$ contains (U_1, U_2) and that these two modules have the same order. It must be true that

$$U(\mathfrak{a}_1 \wedge \mathfrak{a}_2) = (U_1, U_2).$$

LEMMA 2.6. *Let η be a vector with elements in P, and let $Q(\eta)$ be of rank r. There exist a right ideal $\mathfrak{a}$ and a left ideal $\mathfrak{b}$, each of order $n-r$, such that $U(\mathfrak{a})$ is the set of vectors $\eta S^{(x)}$, $V(\mathfrak{b})$ is the set of vectors $\eta R(x)$ where x ranges over all elements of the algebra A.*

Let $\mathfrak{a}$ be the set of elements of A whose representation vectors are orthogonal to $Q(\eta)$ on the left. Since $Q(\eta)$ is of rank r, there must be $n-r$ linearly independent such vectors. By Lemma 2.3, $\mathfrak{a}$ is a right ideal in A. Similarly

there will exist the left ideal $\mathfrak{b}$ of order $n-r$ whose elements b are those for which $Q(\eta)\bar{b}'=0$.

By Lemma 2.2, $\eta S^{\mathsf{T}}(x)\in U(\mathfrak{a})$ for every $x\in A$. If $r=0$, $\eta=(0, 0, \cdots, 0)$ by Lemma 2.1; for $Q(\eta)=0$ implies that $\eta=(0, 0, \cdots, 0)$. Then $\mathfrak{a}=\mathfrak{b}=A$, and the theorem is trivial.

If $r\neq 0$, $r\neq n$, choose a basis $b_1, b_2, \cdots, b_{n-r}$ for $\mathfrak{b}$ and let $c_1, c_2, \cdots, c_r$ be supplementary to it in A so that $u=(b_1, b_2, \cdots, b_{n-r}, c_1, c_2, \cdots, c_r)$ is a basis for A. If $r=n$, then $\mathfrak{b}=0$, and $c_1, c_2, \cdots, c_n$ is chosen as a basis for A. In either case, if $c=\sum\alpha_i c_i$, $\alpha_i\in P$, is an element of $\mathfrak{b}$, then $c=0$; for in the first case the c_i are linearly independent of the b_i and in the second case $\mathfrak{b}$ consists of the element 0 alone.

The r vectors

$$\eta S^{\mathsf{T}}(c_1), \eta S^{\mathsf{T}}(c_2), \cdots, \eta S^{\mathsf{T}}(c_r)$$

are linearly independent; for if $c=\sum\gamma_i c_i$, then $\sum\gamma_i(\eta S^{\mathsf{T}}(c_i))=\eta S^{\mathsf{T}}(c)=0$ implies that $S(c)\eta'=Q(\eta)\bar{c}'=0$ which implies that c is an element of $\mathfrak{b}$. Then $c=0$, and all γ_i are zero. We have established that the set of vectors $\eta S^{\mathsf{T}}(x)$ is at least of order r. However by Lemma 2.2 this set is contained in $U(\mathfrak{a})$, and by Lemma 2.4 $U(\mathfrak{a})$ is of order r. Therefore $U(\mathfrak{a})=\{\eta S^{\mathsf{T}}(x)\}$.

A similar proof gives $V(\mathfrak{b})=\{\eta R(x)\}$ of order r.

THEOREM 2.2. *There is a bi-unique correspondence between right ideals of A and sub-modules U of M such that $\eta\in U$ implies that $\eta S^{\mathsf{T}}(x)\in U$ for all $x\in A$. There is a bi-unique correspondence between left ideals of A and sub-modules V of M such that $\eta\in V$ implies that $\eta R(x)\in V$ for every $x\in A$.*

Lemmas 2.2 and 2.4 give the existence of $U=U(\mathfrak{a})$ for every right ideal $\mathfrak{a}$; $U(\mathfrak{a})$ is of order $n-r$ if $\mathfrak{a}$ is of order r.

Conversely let U be of order r and closed on the right under multiplication by all $S^{\mathsf{T}}(x)$. Let $\eta_1, \eta_2, \cdots, \eta_r$ be a basis for U. By Lemma 2.6 there exist right ideals $\mathfrak{a}_i$ with the orthogonal modules $U_i=\{\eta S^{\mathsf{T}}(x)\}$. Now

$$U = (U_1, U_2, \cdots, U_r).$$

From Lemma 2.5, part (c) it follows that $U=U(\mathfrak{a})$ where $\mathfrak{a}=(\mathfrak{a}_1\wedge\mathfrak{a}_2\wedge\cdots\wedge\mathfrak{a}_r)$. For each such set U there exists a right ideal $\mathfrak{a}$ and $U=U(\mathfrak{a})$. This establishes the theorem for right ideals. The proofs for left ideals can be carried through in the same way.

3. **The parastrophic form.** In the preceding section we have established the fact that the ideals of an algebra with identity e can be put into correspondence with certain sets of vectors $\eta=(\delta_1, \delta_2, \cdots, \delta_n)$, $\delta_i\in P$, i.e., with certain sets of values of $x_1, x_2, \cdots, x_n$ considered as variables over the field P. Let A be restricted to be a Frobenius algebra. This implies the existence of the identity e. Then we may define

$$\pi(\xi) = \pi(x_1, x_2, \cdots, x_n) = |Q(\xi)|$$

as the *parastrophic form* with respect to the basis $e_1, e_2, \cdots, e_n$. Since A is a Frobenius algebra, this polynomial is not identically zero. Since the elements of $Q(\xi)$ are homogeneous linear forms in $x_1, x_2, \cdots, x_n$, $\pi(\xi)$ is homogeneous of degree n in the variables.

LEMMA 3.1. *Every vector solution $\xi=\eta$ of the equation $\pi(\xi)=0$ lies in the orthogonal module of a nonzero ideal of A. Conversely if η lies in the orthogonal module of a nonzero ideal in A, $\pi(\eta)=0$.*

If $\xi=\eta$ is a solution of $\pi(\xi)=0$, then $\pi(\eta)=0$, $|Q(\eta)|=0$, and $Q(\eta)$ is of rank less than n. By Lemma 2.6 there exist both left and right ideals whose orthogonal modules contain η.

If $\mathfrak{a}$ is a right ideal of order $r\neq 0$, then by Lemma 2.4 $U(\mathfrak{a})$ is of order $n-r\neq n$, and $a\in\mathfrak{a}$ implies that

$$\bar{a}Q(\eta) = 0$$

for every η included in $U(\mathfrak{a})$. Then, for every η, $Q(\eta)$ is singular,

$$\pi(\eta) = |Q(\eta)| = 0,$$

and $\xi=\eta$ is a solution of $\pi(\xi)=0$.

THEOREM 3.1. *If A contains a right ideal $\mathfrak{a}$ or a left ideal $\mathfrak{b}$ of order 1, then*

$$\pi(\xi) = g(\xi)h(\xi)$$

where g is a linear form in $x_1, x_2, \cdots, x_n$. The orthogonal module $U(\mathfrak{a})$ or $V(\mathfrak{b})$ consists of all solutions of $g(\xi)=0$.

Let $\mathfrak{a}$ be a right ideal of order 1 in A. Then $U(\mathfrak{a})$ is of order $n-1$, i.e., $U(\mathfrak{a})$ is a linear sub-space of M defined by a linear form $g(\xi)=0$. However since every solution of $g(\xi)=0$ is a solution of $\pi(\xi)=0$, $g(\xi)$ divides $\pi(\xi)$[9].

THEOREM 3.2. *If A is a division algebra, $\pi(\xi)=0$ can have no solutions other than the zero vector. Furthermore, $\pi(\xi)$ must be of degree n in each of the variables $x_1, x_2, \cdots, x_n$.*

If A is a division algebra, $\pi(\xi)=0$ can have no solution $\eta\neq 0$ since by Lemma 3.1 a zero of $\pi(\xi)$ gives rise to an ideal other than the zero ideal in A. Suppose $\pi(\xi)$ did not contain a term $\alpha_i x_i^n$, $\alpha_i\neq 0$. Then $(0, 0, \cdots, 1, \cdots, 0)$ with 1 in the ith place and 0 elsewhere would be a solution of $\pi(\xi)=0$, by the homogeneity of $\pi(\xi)$.

4. **Commutative Frobenius algebras over a perfect field.** Let A be a commutative algebra of order n over the field P with basis $e_1, e_2, \cdots, e_n$. Every ideal $\mathfrak{a}$ is two sided, and $U(\mathfrak{a})$ is the corresponding orthogonal set.

[9] Cf. van der Waerden, B. L., *Moderne Algebra*, Berlin, Springer, 1931, vol. 2, p. 11.

LEMMA 4.1. *If A is a commutative Frobenius algebra of order n over P, the parastrophic form $\pi(\xi)$ with respect to the basis $e_1, e_2, \cdots, e_n$ is factorable into linear factors over some finite extension field Δ of P.*

If $n=1$, the theorem is trivial.

Let $n>1$, and consider A/Ω defined with basis $e_1, e_2, \cdots, e_n$ over the algebraic closure Ω of P. Since the same basis is employed, the same multiplication table results and therefore the same parastrophic form.

We define a *minimal ideal* of A to be an ideal which is not the zero ideal and which contains only the zero ideal properly. The representations of A/Ω with respect to its minimal ideals (i.e., the absolutely irreducible representations) are of order 1([10]). Then the minimal ideals themselves are of order 1.

By Theorem 3.1 each minimal ideal induces a linear factor of the parastrophic form $\pi(\xi)$. There can be, therefore, not more than n linear factors associated with the minimal ideals. By Theorem 2.5 these linear factors are distinct if and only if the minimal ideals are distinct. It follows that there can be not more than n minimal ideals. Let $g_1, g_2, \cdots, g_k$ be associated with the minimal ideals $\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_k$ where $k \leqq n$. It is true, by Theorem 3.1, that $\pi(\xi) = g_1^{\sigma_1} g_2^{\sigma_2} \cdots g_k^{\sigma_k} h$. Let $\xi=\eta$ be a solution of the equation $\pi(\xi)=0$. By Lemma 3.1 η must lie in the orthogonal module of some ideal in A. This ideal must contain a minimal ideal $\mathfrak{a}_i$ and therefore η must be a solution of $g_i=0$. Every solution of the equation $\pi(\xi)=0$ must be a solution of the equation $g_1 g_2 \cdots g_k=0$. We have immediately, by Hilbert's *Nullstellensatz*([11]) that the only factors of $\pi(\xi)$ are products of powers of the linear factors $g_1, g_2, \cdots, g_k$.

If Δ is a field defined through extending the field P by the coefficients of the g_i, Δ is a finite extension field of P in which $\pi(\xi)$ is factorable into linear factors.

As an example, let us take the linear algebra with the defining matrix

$$Q(u) = \begin{bmatrix} e & a \\ a & 5e \end{bmatrix}$$

defined over the rational field P. Then, as in Part 1,

$$Q(\xi) = \begin{bmatrix} x_1 & x_2 \\ x_2 & 5x_1 \end{bmatrix}, \qquad \pi(\xi) = |Q(\xi)| = 5x_1^2 - x_2^2.$$

The parastrophic form is irreducible over the rational field, but over $\Delta = P(5^{1/2})$, $\pi(\xi) = (5^{1/2}x_1 - x_2)(5^{1/2}x_1 + x_2)$.

As an example of the failure of the theorem for a non-commutative algebra, consider the total matric algebra of order 4 with basis $u = (e_{11}, e_{12}, e_{21}, e_{22})$ over any field P we wish to choose. In this case

([10]) M. Deuring, ibid., p. 32.

([11]) van der Waerden, ibid.

$$Q(u) = \begin{bmatrix} e_{11} & e_{12} & 0 & 0 \\ 0 & 0 & e_{11} & e_{12} \\ e_{21} & e_{22} & 0 & 0 \\ 0 & 0 & e_{21} & e_{22} \end{bmatrix}, \qquad Q(\xi) = \begin{bmatrix} x_1 & x_2 & 0 & 0 \\ 0 & 0 & x_1 & x_2 \\ x_3 & x_4 & 0 & 0 \\ 0 & 0 & x_3 & x_4 \end{bmatrix},$$

$$\pi(\xi) = |Q(\xi)| = (x_2x_3 - x_1x_4)^2.$$

Here $\pi(\xi)$ contains a factor of degree two which is irreducible over all extension fields of P.

Lemma 4.1 may be applied to a theorem of Burnside([12]) on the factorization of a certain determinant. Consider the matrix

$$\begin{bmatrix} x_1, & x_2, & \cdots, & x_n \\ x_{\alpha_1}, & x_{\alpha_2}, & \cdots, & x_{\alpha_n} \\ . & . & \cdots & . \\ x_{\sigma_1}, & x_{\sigma_2}, & \cdots, & x_{\sigma_n} \end{bmatrix}$$

where each row is a permutation of the first row, the permutations constituting a commutative group $\mathfrak{G}$ of order n. This matrix is the parastrophic matrix of the group-ring with the elements of $\mathfrak{G}$ in some order as basis elements. Since $\mathfrak{G}$ is commutative, its group-ring is commutative, and the determinant of the parastrophic matrix is factorable into linear factors in some finite extension field of the field of coefficients.

An algebra is called primary if it contains an identity element and its remainder class ring with respect to the radical is simple. A simple commutative algebra is a field; for a left ideal of a commutative algebra is a two-sided ideal. The decomposition of the identity of a commutative algebra into the sum of primitive idempotents induces a decomposition of the algebra into the direct sum of primary ideals. The remainder class ring of each component of this decomposition contains but one idempotent and is therefore a field([13]).

We choose to impose upon the field P the condition that it be perfect, i.e., that it admit no inseparable extension.

For convenience we shall define a primary commutative algebra A to be in *normal form* if it is defined over a maximal sub-field as coefficient field.

LEMMA 4.2. *A primary commutative algebra A/P defined over the perfect field P may be put in normal form. We write $A/P = B/F$ where A/P modulo its radical N is isomorphic to the field F.*

The primary commutative algebra A is defined over the perfect field P. We may write $A = F + N$ where N is the radical of A and $A/N \simeq F$([14]). The

([12]) W. Burnside, Messenger of Mathematics, vol. 23 (1894), pp. 112–114.

([13]) For this paragraph, cf. Deuring, ibid., p. 17; van der Waerden, ibid., p. 47.

([14]) M. Deuring, ibid., p. 23.

remainder class ring is a field since A/N is simple. The field F contained in A may be employed as a coefficient field. Let $e_1, e_2, \cdots, e_n$ be a P-basis for A. Consider the set of elements $\phi_1 e_1+\phi_2 e_2+\cdots+\phi_n e_n$ where the ϕ_i range over F. The set of all such numbers is contained in A, and on the other hand, since $F \supseteq P$, it contains A. Then an F-basis may be chosen for A considered as a finite F-module. To indicate this change of basis field, we write

$$A/P = B/F.$$

The field F is maximal in $A=F+N$ since any ring which contains F must also contain elements of the radical N.

LEMMA 4.3. *If $\mathfrak{a}$ is a minimal ideal of the commutative primary algebra A, then $\mathfrak{a}N=0$ where N is the radical of A. If A is written in normal form B/F, $\mathfrak{a}$ is of order 1 over F.*

Let A/P be written in normal form B/F. The same ideal $\mathfrak{a}$ and the same radical N are to be considered since the rings A/P and B/F are identical except for form of expression over different fields.

Let $\mathfrak{a}$ be a minimal ideal of B. Let $b \neq 0$ be an element of $\mathfrak{a}$. Then $\mathfrak{a}=Bb$; for $\mathfrak{a} \supseteq Bb$, and $\mathfrak{a}$ is minimal. Every element of $\mathfrak{a}$ is of the form xb where x lies in B. The correspondence $b \to cb$, c an element of B, defines an endomorphism([15]) of the ideal $\mathfrak{a}$ considered as an additive group. Let $x_1 b \to x_1 cb$, $x_2 b \to x_2 cb$, where x_1, x_2 are in B. Then $x_1 b+x_2 b=(x_1+x_2)b \to x_1 cb+x_2 cb = (x_1+x_2)cb$. Let $\mathfrak{c}$ be the set of elements of B such that $c\mathfrak{a}=0$. Then $\mathfrak{c}$ is an ideal, and $B/\mathfrak{c}$ is an absolute operator domain for $\mathfrak{a}$. However the endomorphism ring of a minimal ideal is a division algebra([16]), so that the ring $B/\mathfrak{c}$ is a field. Since every ideal of a primary commutative ring is contained in the radical([17]), $\mathfrak{c} \subseteq N$, and $B/\mathfrak{c} \sim B/N \simeq F$. However no field can be homomorphic to a second unless the homomorphism is an isomorphism. Therefore $B/\mathfrak{c} \simeq B/N$, and $\mathfrak{c}=N$, $N\mathfrak{a}=0$. It follows that $\mathfrak{a}$ is of order 1; for

$$(\alpha e + a)b = \alpha eb = \alpha b$$

where α is an element of F, a is an element of N, and $Bb=\mathfrak{a}$, $b \neq 0$ being an element of $\mathfrak{a}$.

THEOREM 4.1. *A necessary and sufficient condition that a commutative primary algebra defined over the perfect field P be a Frobenius algebra is that A have one and only one minimal ideal.*

Suppose that A has one and only one minimal ideal $\mathfrak{a}$. If this ideal is A, then A is a field and the theorem holds. If $\mathfrak{a}$ is a proper ideal, then $\mathfrak{a}$ is of

([15]) van der Waerden, B.L., *Moderne Algebra*, Berlin, Springer, 1936, 2d edition.
([16]) van der Waerden, *Modern Algebra*, vol. 2, p. 165.
([17]) Krull, W., *Idealtheorie*, Berlin, Springer, 1935, p. 22.

order 1 over F by Lemma 4.3 and $\mathfrak{a}$ is of order k over P where k is the order of F over P. Then if $U(\mathfrak{a})$ is defined for A/P and A is of order n over P, $U(\mathfrak{a})$ is of order $n-k$ over P. This follows from Lemma 2.4. Since $\mathfrak{a}$ is minimal, every nonzero ideal of A must contain $\mathfrak{a}$, and therefore every orthogonal module of a nonzero ideal is contained in $U(a)$ (Lemma 2.5). Then if χ is a vector of M not contained in $U(\mathfrak{a})$, $|Q(\chi)| \neq 0$; for by Lemma 3.1 $|Q(\chi)| = 0$ implies that x lies in the orthogonal module of a nonzero ideal in A.

Conversely suppose that A has at least two minimal ideals $\mathfrak{a}$ and $\mathfrak{b}$. Since $\mathfrak{a}$ and $\mathfrak{b}$ contain no ideal other than the zero ideal, they must be principal ideals. Let $\mathfrak{a}=(a)$, $\mathfrak{b}=(b)$ where $a\neq 0$, $b\neq 0$. The elements a and b must lie in the radical of A since every ideal of A lies in its radical.

Let A be written in normal form B/F. Then by Lemma 4.3, $\mathfrak{a}$ and $\mathfrak{b}$ are of order 1 over F. Choose a basis

$$v = (e, a_2, \cdots, a_{m-2}, a, b)$$

where e is the identity of B, and $a_2, \cdots, a_{m-2}$ lie in the radical of B, and m is the order of B over F. By Lemma 4.3 the product of $\mathfrak{a}$ and $\mathfrak{b}$ with any element of the radical is zero. We have

$$Q_B(v) = \begin{bmatrix} e, & a_2, \cdots, a_{m-2}, & a, & b \\ a_2, & a_2^2, \cdots, \cdot, & 0, & 0 \\ \cdot & \vdots \quad \cdots \quad \cdot & \cdot & \cdot \\ a_{m-2}, & \cdot \quad \cdots \quad \cdot, & 0, & 0 \\ a, & 0, \cdots, 0, & 0, & 0 \\ b, & 0, \cdots, 0, & 0, & 0 \end{bmatrix}.$$

Let w be a basis of F with respect to P. Then B/F may be written as A/P with basis

$$u = (ew, a_2w, \cdots, a_{m-2}w, aw, bw),$$

and the corresponding defining matrix takes the form

$$Q_A(u) = \begin{bmatrix} eQ_F(w), & a_2Q_F(w), \cdots, a_{m-2}Q_F(w), & aQ_F(w), & bQ_F(w) \\ a_2Q_F(w), & a_2^2Q_F(w), \cdots, \cdot, & 0, & 0 \\ \cdot & \cdot \quad \cdots \quad \cdot & \cdot & \cdot \\ a_{m-2}Q_F(w), & \cdot \quad \cdots \quad \cdot, & 0, & 0 \\ aQ_F(w), & 0, \cdots, 0, & 0, & 0 \\ bQ_F(w), & 0, \cdots, 0, & 0, & 0 \end{bmatrix}$$

where $Q_F(w)$ is the defining matrix for F with respect to P. The form of $Q_A(u)$

implies immediately that the parastrophic matrix $Q_A(\xi)$ is singular; A cannot be a Frobenius algebra.

COROLLARY 4.1. *If the parastrophic form $\pi(\xi)$ of the commutative primary algebra A contains a linear factor $g(\xi)$, the vector solutions of the equation $g(\xi)=0$ form the orthogonal module of an ideal of order 1 in A.*

Let $\pi(\xi)=g(\xi)h(\xi)$ where $\xi=(x_1, x_2, \cdots, x_n)$ and where $g(\xi)$ is a linear polynomial in $x_1, x_2, \cdots, x_n$. The solutions of $g(\xi)=0$ form a linear sub-space T of the set of vectors M. If M is of order n, T is of order $n-1$.

Suppose that T is not closed on the right by all $S^{\tau}(x)$. Then $\eta_1 \neq 0$ and $a \neq 0$ exist such that $\eta_1 S^{\tau}(a)$ is not an element of T, and

$$M = T + P\eta_1 S^{\tau}(a).$$

If $\eta \in M$, there exist $\eta_2 \in T$ and $\alpha \in P$ such that $\eta = \eta_2 + \alpha\eta_1 S^{\tau}(a)$. Since η_1 and η_2 are solutions of $g(\xi)=0$ and therefore solutions of $\pi(\xi)=0$ each of these vectors must, by Lemma 3.1 lie in the orthogonal module of some nonzero ideal of A. Let $\eta_1 \in U(\mathfrak{a}_1)$, $\eta_2 \in U(\mathfrak{a}_2)$. Then by Lemma 2.2 $\eta_1 S^{\tau}(a) \in U(\mathfrak{a}_1)$. The theorem gives the existence of an unique minimal ideal $\mathfrak{b} \neq 0$, and $\mathfrak{b} \subseteq (\mathfrak{a}_1 \wedge \mathfrak{a}_2)$. But $\eta \in U(\mathfrak{a}_1 \wedge \mathfrak{a}_2)$ which is contained in $U(\mathfrak{b})$. It follows that $|Q(\eta)| = 0$, and A is not a Frobenius algebra.

This contradiction gives the closure of T. By Theorem 2.2 T is the orthogonal module of an ideal of order 1 in A.

THEOREM 4.2. *If the commutative algebra A has only principal ideals, A is a Frobenius algebra.*

Suppose that a primary component B of A were not a Frobenius algebra. Then, by Theorem 4.1, B must have at least two minimal ideals. Since a minimal ideal is principal, these must have the form (a) and (b), $a \neq 0$, $b \neq 0$. Every element of (a) is of the form ca where $c \in B$, and every element of (b) is of the form cb.

Consider the ideal (a, b) with elements $c_1a + c_2b$ where $c_i \in B$. Now every element of B can be written as $\phi + d$ where ϕ is an element of the field F, d is an element of the radical N, and $B = F + N$. By assumption the ideal (a, b) is principal and is therefore generated by a fixed element $c_1a + c_2b$, $c_1, c_2 \in B$. By Lemma 4.3 $aN = 0$; and $bN = 0$. It follows that

$$(\phi + d)(c_1a + c_2b) = \phi(c_1a + c_2b).$$

However (a, b) contains the ideals (a) and (b), so that the equations

$$\phi_1(c_1a + c_2b) = a, \qquad \phi_2(c_1a + c_2b) = b$$

must have a solution for ϕ_1 and ϕ_2 as elements of F. Since F is a field, this implies that $c_1 = c_2 = 0$ and that $a = b = 0$ contradictory to hypothesis.

Over the perfect field P it is possible to consider the polynomial algebras

of the form

$$A \simeq P[x]/f(x)$$

where $P[x]$ is the polynomial domain in the indeterminant x, and $P[x]/f(x)$ is the remainder class ring with respect to the polynomial $f(x)$. The basis of A may be chosen as $1, x, x^2, \cdots, x^{n-1}$, and reduction modulo $f(x)$ of degree n follows any multiplication. In this case the polynomial ideal theories may be employed([18]). The factorization of $f(x)$ into distinct factors gives a corresponding reduction of A into the direct sum of ideals. If $f(x) = g_1(x)g_2(x)$ where the two factors are relatively prime, then

$$A \simeq P[x]/f(x) \simeq P[x]/g_1(x) + P[x]/g_2(x).$$

If $f(x)$ is the power of an irreducible polynomial, then $P[x]/f(x)$ is primary.

LEMMA 4.4. *If $A \simeq P[x]/f(x)$, A has an ideal of order 1 if and only if $f(x)$ has a linear factor.*

Let $f(x) = g_1(x)g_2(x) \cdots g_r(x)$ where $g_1(x), g_2(x), \cdots, g_r(x)$ are irreducible. Then

$$A = C_1 + C_2 + \cdots + C_r,$$

and $C_i \simeq P[x]/g_i^{\sigma_i}(x)$ is a primary ideal. Now

$$C_i \supseteq F_i \simeq P[x]/g_i(x)$$

so that F_i is a field whose order is the degree of $g_i(x)$. Let $\mathfrak{a}$ be a minimal ideal of C_i in case $\sigma_i > 1$ and C_i itself in case $\sigma_i = 1$. Then $\mathfrak{a}$ is a minimal ideal of A. However, since $\mathfrak{a} \supseteq \mathfrak{a}F_i$, $\mathfrak{a}$ is of order at least that of F_i so that if $\mathfrak{a}$ is of order 1, F_i is of order 1, and $g_i(x)$ is of degree 1.

Conversely if $g_i(x)$ is linear, $C_i \simeq P[x]/g_i^{\sigma_i}(x)$ is isomorphic with $P[y]/y^{\sigma_i}$ where $y = g_i(x)$. The transformation $y = g_i(x)$ has an inverse since $g_i(x)$ is linear. We may choose as a basis of C the elements $1, y, y^2, \cdots, y^{\sigma_i - 1}$. Then, as in the proof of Lemma 4.2, the maximal field contained in C_i is isomorphic with P, and C_i contains an ideal of order 1, or C itself is of order 1.

THEOREM 4.3. *If F is an algebraic extension field of the perfect field P, the parastrophic form of F with respect to its basis over P is irreducible.*

Since P is perfect, $F \simeq P[x]/f(x)$ where $f(x)$ is irreducible over P; for F is generated by a single element satisfying the irreducible polynomial equation $f(x) = 0$. Suppose that for some basis of F

$$\pi(\xi) = g_1(\xi)g_2(\xi)$$

where g_i is of degree $m_i < n$, n being the order of F with respect to P. By Theo-

([18]) Cf. van der Waerden, loc. cit.; Krull, loc. cit.

rem 3.2 $\pi(\xi)$ is a polynomial of degree n in x_1, g_1 is a polynomial of degree m_1 in x_1 over the polynomial field

$$\Gamma = P(x_2, x_3, \cdots, x_n).$$

Let a root μ of g_1 be adjoined to Γ. Then g_1 (and therefore $\pi(\xi)$ has a linear factor in $\Gamma(\mu)$. It follows (Lemma 4.4) that $f(x)$ must have a linear factor over $\Gamma(\mu)$ since $F/\Gamma(\mu)$ must by Corollary 4.1 have an ideal of order 1. However $\pi(\xi)$ is uniquely factorable into linear factors over a finite extension field Δ of P (Lemma 4.1), so that

$$\Gamma(\mu) = P(\theta)(x_2, x_3, \cdots, x_n)$$

where θ is algebraic of degree m_1 with respect to P. Then $f(x)$ has a zero in $P(\theta)$. However $f(x)$ is of degree n over P while m_1 was assumed to be less than n. This contradiction gives the irreducibility of $\pi(\xi)$.

LEMMA 4.5. *If the primary commutative Frobenius algebra A is defined over the perfect field P, and if the maximal field F contained in A is of degree k over P, then A/Ω, where Ω is the algebraic closure of P, has exactly k minimal ideals.*

If F is the maximal field contained in A, then $F \simeq A/N$ where N is the radical of A, and we may write A as the direct sum of F and N([19]);

$$A/P = F/P + N/P$$

where the direct sum is in the sense of P-modules.

Consider that P is perfect and that F is a finite extension field of P. It follows that F is obtained from P by the adjunction of a single element and that this element satisfies an irreducible algebraic equation $f(x) = 0$ of degree k with coefficients in P. Then

$$F/P \simeq P[x]/f(x).$$

If we extend P to its algebraic closure Ω, then

$$A/\Omega = F/\Omega + N/\Omega$$

and, furthermore,

$$F/\Omega \simeq \Omega[x]/f(x).$$

Over Ω, however, $f(x)$ factors into linear factors, and F/Ω decomposes into the direct sum of primary ideals, each containing an unique idempotent. There can be but k idempotents in A/Ω, and each induces a primary component of A/Ω.

Since A/P is a Frobenius algebra, A/Ω is a Frobenius algebra. Each primary component of A/Ω is a Frobenius algebra, and each, by Theorem 4.1,

([19]) M. Deuring, loc. cit., p. 23.

can contain one and only one minimal ideal. We have proved that the number of these components is k since each contains a primitive idempotent of F/Ω. Therefore there are just k distinct minimal ideals in A/Ω.

THEOREM 4.4. *If the primary commutative algebra A is a Frobenius algebra, the parastrophic form is $\pi(\xi)=g^m(\xi)$ where $g(\xi)$ may be chosen as the parastrophic form of $F\simeq A/N$ where N is the radical of A.*

Let A/P be written in normal form B/F with basis $v=(b_1=e, b_2, \cdots, b_m=b)$ where e is the identity element and b is the basis element with respect to F of the unique minimal ideal of B (cf. Lemmas 4.1, 4.3) and $b_2, \cdots, b_m$ lie in the radical of B. The defining matrix of B/F under these conditions is

$$Q_B(v) = \begin{bmatrix} e, & b_2, & \cdots, & b \\ b_2, & b_2^2, & \cdots, & 0 \\ \cdot & \cdot & \cdots & \cdot \\ b, & 0, & \cdots, & 0 \end{bmatrix}.$$

The product of b with any element of the radical is zero by Lemma 4.3. Column m and row m of $Q_B(v)$ consist of zeros except in the first place of each.

Let w be a basis of F with respect to P. Then a basis of $A/P=B/F$ with respect to P will be given by

$$u = (ew, b_2w, \cdots, bw),$$

and the defining matrix of A/P on the basis u is

$$Q_A(u) = \begin{bmatrix} eQ_F(w), & b_2Q_F(w), & \cdots, & bQ_F(w) \\ b_2Q_F(w), & b_2^2Q_F(w), & \cdots, & 0 \\ \cdot & \cdot & \cdots & \cdot \\ bQ_F(w), & 0, & \cdots, & 0 \end{bmatrix}$$

where $Q_F(w)$ is the defining matrix of F with respect to P.

To form the parastrophic matrix $Q_A(\xi)$ from $Q_A(u)$ we substitute $\xi=(x_1, x_2, \cdots, x_n)$ for u in $Q_A(u)$. This substitution will also take place in the upper right-hand corner of the matrix, namely within the matrix $bQ_F(w)=Q_F(bw)$. Since b is linearly independent of the elements of the basis w, $Q_F(bw)$ will be the same except for notation as $Q_F(w)$. Substitution of variables $x_1, x_2, \cdots, x_n$ in $Q_F(bw)$ will, therefore, give the same result as substitution in $Q_F(w)$.

Then $|Q_F(\xi)|=g(\xi)$ must be the parastrophic form of F for the basis w. In the expansion of $|Q_A(\xi)|$ by minors as indicated by the matrix $Q_A(u)$, $g(\xi)$ must enter as a factor. The parastrophic form of A is $\pi(\xi)=g(\xi)f(\xi)$ where $g(\xi)$ is, by Theorem 4.3, irreducible.

We now extend the basis field P to its algebraic closure Ω. Over Ω, how-

ever, $g(\xi)=h_1(\xi)h_2(\xi)\cdots h_k(\xi)$ where k is the order of F over P and the $h_i(\xi)$ are distinct linear polynomials in $x_1, x_2, \cdots, x_n$ (cf. Lemma 4.1). By Lemma 4.5, A/Ω has exactly k minimal ideals. Suppose that $f(\xi)$ contained a linear factor distinct from the $h_i(\xi)$. Then by Corollary 4.1 this factor would give rise to a $(k+1)$st minimal ideal distinct from the rest. Since this is impossible, $f(\xi)$ must contain only the $h_i(\xi)$ as factors. Since $g(\xi)$ is irreducible over P, $f(\xi)$ must be a power of $g(\xi)$, and $\pi(\xi)=g^m(\xi)$ where m is the order of B over F.

5. **Factorization of the rational prime number p.** Let H be a finite extension field of degree n over the rational field R. Let G be the ring of rational integers, and let K be a domain of integrity in H with G-basis $e_1, e_2, \cdots, e_n$. If p is a rational prime number, $\mathfrak{a}=Kp$ is the corresponding principal ideal in K. Then

$$\mathfrak{a} = \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_s$$

where $\mathfrak{q}_i$ is a primary ideal belonging to the prime ideal $\mathfrak{p}_i$, and

$$C = K/\mathfrak{a} \simeq K/\mathfrak{q}_1 + K/\mathfrak{q}_2 + \cdots + K/\mathfrak{q}_s$$

is the direct sum of the primary ideals $K/\mathfrak{q}_i$([20]). This ring is composed of linear combinations of the elements e_i with coefficients in G taken modulo p, and is therefore a linear algebra over the field $P=G/p$, which is a perfect field([21]). Furthermore, C has the same multiplication table as K. If $\pi(\xi)$ is the parastrophic form in the basis $e_1, e_2, \cdots, e_n$,

$$\pi^*(\xi) = \pi(\xi) \pmod{p}$$

is that of the algebra C.

The additive components of C induce a factorization of $\pi^*(\xi)$ into distinct factors. Each component is primary, and the corresponding factor of the parastrophic form is the power of an irreducible factor or is identically zero (Theorem 4.4), i.e., if $\pi(\xi)\not\equiv 0 \pmod{p}$, then

$$\pi(\xi) = g_1^{\sigma_1}g_2^{\sigma_2}\cdots g_s^{\sigma_s} \pmod{p}$$

where the degree of g_i is the degree of the field $K/\mathfrak{p}_i$ over P, and the radical of $K/\mathfrak{q}_i$ is of index at most σ_i.

Two ideals are said to be divisor prime in K if their greatest common divisor is the unit ideal.

LEMMA 5.1. *If the ideal $\mathfrak{a}$ is divisor prime to the conductor $\mathfrak{f}$ of K, then $K/\mathfrak{a}$ is a principal ideal ring.*

By Krull([22]) if $\mathfrak{a}$ is divisor prime to $\mathfrak{f}$, $\mathfrak{a}=\mathfrak{p}_1^{\alpha_1}\mathfrak{p}_2^{\alpha_2}\cdots\mathfrak{p}_s^{\alpha_s}$. Let $\mathfrak{b}\supset\mathfrak{a}$. Then

([20]) Cf. van der Waerden, loc. cit., vol. 2, pp. 47–50.

([21]) van der Waerden, loc. cit., vol. 1, first edition, p. 118.

([22]) Krull, ibid.

$(\mathfrak{b}, \mathfrak{f}) \supseteq (\mathfrak{a}, \mathfrak{f}) \supseteq K$, and every ideal which contains $\mathfrak{a}$ is divisor prime to $\mathfrak{f}$. Then $\mathfrak{b} = \mathfrak{p}_1^{\beta_1}\mathfrak{p}_2^{\beta_2} \cdots \mathfrak{p}_s^{\beta_s}$ where $\beta_i \leqq \alpha_i$.

Consider that the ideals of $K/\mathfrak{a}$ are the rings $\mathfrak{b}/\mathfrak{a}$ where $\mathfrak{b} \supset \mathfrak{a}$. Then if $\mathfrak{c} = \mathfrak{p}_1^{\beta_1+1}\mathfrak{p}_2^{\beta_2+1} \cdots \mathfrak{p}_s^{\beta_s+1}$, $\mathfrak{c}_i = \mathfrak{p}_1^{\beta_1+1}\mathfrak{p}_2^{\beta_2+1} \cdots \mathfrak{p}_i^{\beta_i} \cdots \mathfrak{p}_s^{\beta_s+1}$, we may choose d_i in $\mathfrak{c}_i$ and not in $\mathfrak{c}$. Then d_i is contained in every $\mathfrak{p}_j^{\beta_j+1}$ except $\mathfrak{p}_i^{\beta_i+1}$. Furthermore d_i is contained in all $\mathfrak{p}_j^{\beta_j}$. Therefore d_i and $d = d_1 + d_2 + \cdots + d_s$ are contained in $\mathfrak{b}$. It follows that the ideal $(\mathfrak{a}, d)$ which contains $\mathfrak{a}$ is contained in $\mathfrak{b}$. Since $(\mathfrak{a}, d)$ is a divisor of $\mathfrak{a}$, $(\mathfrak{a}, d) = \mathfrak{p}_1^{\gamma_1}\mathfrak{p}_2^{\gamma_2} \cdots \mathfrak{p}_s^{\gamma_s}$, where $\gamma_i \geqq \beta_i$. Then $d \in \mathfrak{p}^{\gamma_i}$. However d is not divisible by $\mathfrak{p}_i^{\beta_i+1}$ so that $\gamma_i \leqq \beta_i$. It follows that $\gamma_i = \beta_i$, and

$$(\mathfrak{a}, d) = \mathfrak{p}_1^{\beta_1}\mathfrak{p}_2^{\beta_2} \cdots \mathfrak{p}_s^{\beta_s} = \mathfrak{b}.$$

The ideal $\mathfrak{b}/\mathfrak{a}$ of $K/\mathfrak{a}$ is generated by the element d, i.e., $K/\mathfrak{a}$ is a principal ideal ring[23].

When K is the maximal domain of integrity of H, the conductor $\mathfrak{f}$ is the unit ideal, and $K/\mathfrak{a}$ is principal for every ideal in K.

THEOREM 5.1. *If* $\pi(\xi) \equiv g_1^{\sigma_1}g_2^{\sigma_2} \cdots g_s^{\sigma_s} \pmod{p}$, *then*

$$\mathfrak{a} = Kp = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s$$

where the $\mathfrak{q}_i$ *are primary ideals belonging to the prime ideals* $\mathfrak{p}_i$ *of degree that of* g_i. *If* $\pi(\xi) \equiv 0 \pmod{p}$, p *is not prime to the conductor of* K.

The theorem follows immediately from the above conclusions and from Theorem 4.2.

UNIVERSITY OF WISCONSIN,
MADISON, WIS.

---

[23] The proof of Lemma 5.1 is taken from van der Waerden, loc. cit.