THEORY OF FINITE ALGEBRAS*

BY

H. S. VANDIVER

1. The object of this paper is to develop an abstract theory of finite algebras which is applicable to various familiar and important concrete algebras, such as the m classes of residues of integers modulo m, the classes of residues of polynomials in x with respect to the moduli m and $P(x)$, the classes of residues of integral algebraic numbers of a given algebraic field with respect to any ideal as modulus, and the classes of residues with respect to certain modular systems. We consider an algebra composed of a finite set of elements which may be combined by addition, subtraction and multiplication, subject to the commutative, associative and distributive laws, and such that the sum, difference or product of any two elements is uniquely determined as an element of the set, while, moreover, there occurs an element playing the rôle of unity under multiplication. It is not assumed that division is always possible; a product may vanish when neither factor vanishes.

While the field $R(\alpha_1, \cdots, \alpha_n)$ defined by the algebraic numbers $\alpha_1, \cdots, \alpha_n$ is identical with a field $R(u)$ defined by a single algebraic number u, a similar theorem does not hold for finite algebras (§ 6).

As regards their units, primes, etc., the theory of finite algebras presents analogies with the theory of integral algebraic numbers.

I am indebted to Professor L. E. Dickson for valuable suggestions.

2. **Definition of a Finite Algebra.** Let the elements $u_0, u_1, \cdots, u_{s-1}$ form a commutative group under addition. The unique element u_0 such that $u_i + u_0 = u_i$ $(i = 0, \cdots, s-1)$ is called the zero element. It is assumed that the elements may be combined by multiplication, subject to the commutative, associative and distributive laws, and that the product of any two elements is an element of the set. We shall discard the assumption, made in the theory of finite fields, that division by every element other than u_0 is possible and unique. However, we shall assume that there exists at least one element u_k, called a *unit element,* such that $u_k x = u_0$ has the unique solution $x = u_0$. Elements which are not units are called *non-units* and denoted by $N_1, N_2, \cdots$.

Theorem I. *Division by a unit U_k is always possible and unique.*

Since the products $u_i U_k$ $(i = 0, 1, \cdots, s-1)$ are distinct, they form a permutation of the u_i. Thus $xU_k = u_l$ has one and but one solution x.

[*] Presented to the Society (Chicago), December 29, 1911.

The solution x of $xU_k = U_k$ plays the rôle of *unity*. For, if y is the solution of $yU_k = u_l$, then

$$xu_l = (xU_k)\, y = U_k\, y = u_l.$$

Theorem II. *The product of two or more units is a unit.*

For, if $U_1 U_2 \cdots U_k = N_1$, we can determine a non-unit $N_2 \neq u_0$ such that $N_1 N_2 = u_0$. Then

$$U_1 (N_2 U_2 \cdots U_k) = u_0,$$

so that

$$N_2 U_2 \cdots U_k = u_0.$$

A repetition of the process gives $N_2 = u_0$.

Theorem III. *A product is a non-unit if any factor is.*

By Theorem II such a product may be given the form

$$P = UN_1 N_2 \cdots N_e \qquad (U \text{ a unit}).$$

Set $N_1 N_k = u_0$, $N_k \neq u_0$. Then $PN_k = u_0$, so that P is a non-unit.

Theorem IV. *The totality of units $U_1, \cdots, U_k$ forms a commutative group under multiplication; the kth power of any unit is unity.*

The products $U_i U_1, \cdots, U_i U_k$ are distinct and each is a unit (Theorem II). Hence they form a permutation of $U_1, \cdots, U_k$, so that $U_i x = U_j$ has as its unique solution a unit.

By Thorems I and III, every element is divisible by each unit, and no unit is divisible by a non-unit. But a given non-unit may or may not be divisible by another given non-unit. Accordingly, we shall make the

Definitions. If N is a non-unit, any element UN is called an *associate* of N, where U is a unit. A non-unit is called a *prime* if it has no non-unit divisor other than itself and its associates. Two or more non-units are called *prime to each other* if no two of them have a common non-unit divisor.

3. Consider the algebra $A(m)$ formed of the m classes of residues C_r of integers modulo m, where $C_r = C_\rho$ if and only if $r \equiv \rho \pmod{m}$, and

$$C_r \pm C_\rho = C_{r \pm \rho}, \qquad C_r C_\rho = C_{r\rho}.$$

Then C_0 is the zero element and C_1 the unity. The units are C_a, where a ranges over the integers less than m and prime to m. The non-units are C_r, where r is an integer $< m$ having a factor in common with m. If e and f are relatively prime integers, we have $1 = eu + fv$, where u and v are integers. Hence

$$C_1 = C_e C_u + C_f C_v,$$

so that any common divisor of C_e and C_f divides C_1 and hence (Theorem III) is a unit. Thus C_e and C_f are prime to each other.

If an element of $A(m)$ is a prime it is the associate of an element C_p, where p is a prime factor of m. If C_p is composite we must have

$$C_p = UC_{p^\epsilon} \qquad (\epsilon > 1),$$

where U is a unit. Let p^a be the highest power of p which divides m. If $\epsilon < \alpha$ we multiply the members of the preceding equation by C_{m/p^ϵ} and obtain $C_{m/p^{\epsilon-1}} = C_0$, whence $\epsilon = 1$. If $\epsilon \geqq \alpha$, we multiply by C_{m/p^a} and obtain $C_{m/p^{a-1}} = C_0$, whence $\alpha = 1$. Then

$$s = p\left(p^{\epsilon-1} - \frac{m}{p}\right) \equiv p^\epsilon \qquad (\mathrm{mod}\ m)$$

and C_s is an associate of C_p. Hence C_p is not composite.

Theorem V. *If $p, q, \cdots, r$ are the distinct prime factors of m, the algebra $A\,(m)$ composed of the m classes of residues of integers modulo m contains the prime elements $C_p, C_q, \cdots, C_r$; these and their associates give all the prime elements.*

Any finite algebra $A\,(s)$ contains * a sub-algebra $A\,(m)$ composed of the integral elements C_r. We shall call m the base of $A(s)$. If e and f are relatively prime integers, C_e is prime to C_f within $A\,(s)$.

We note, in addition to $A\,(m)$, the following examples of finite algebras. Miss Sanderson † has considered the classes of residues

$$a\,(y) = a_0 + a_1\,y + \cdots + a_{r-1}\,y^{r-1} \quad (a_i = 0, 1, \cdots, m-1)$$

modulis $m, P\,(y)$, where m is any integer and $P\,(y)$ is a polynomial in y of degree r with integral coefficients, irreducible with respect to each prime factor of m as modulus. She proved that $a\,(y)$ is a unit element if and only if the greatest common divisor of its coefficients a_i is prime to m, and that number of units is

$$m^r\left(1 - \frac{1}{p_1^r}\right)\left(1 - \frac{1}{p_2^r}\right)\cdots\left(1 - \frac{1}{p_k^r}\right),$$

where $p_1, \cdots, p_k$ are the distinct prime factors of m.

Dedekind ‡ has considered the classes of residues of integral numbers of an algebraic field with respect to an ideal α as modulus. These classes form a finite algebra the number of unit elements of which is

$$N\,(\alpha)\left\{1 - \frac{1}{N\,(\rho_1)}\right\}\cdots\left\{1 - \frac{1}{N\,(\rho_r)}\right\},$$

where $\rho_1, \cdots, \rho_r$ are the distinct prime ideal factors of α, and $N\,(k)$ is the norm of k. In particular, if α is a prime ideal of norm p^f, the classes form a finite field of order $s = p^f$.

* L. E. Dickson, *Linear Groups* (Teubner), 1901, p. 9.

† Annals of Mathematics, (2), vol. 13 (1911), p. 36.

‡ Dirichlet-Dedekind, *Zahlentheorie*, 4th ed., pp. 564–580.

4. **Congruence.** Let $M_1, \cdots, M_t$ be elements of a finite algebra $A(s)$. Two elements A and B of the algebra are called congruent (and residues of each other) with respect to a modular system $(M_1, \cdots, M_t)$ if

$$A - B = k_1 M_1 + \cdots + k_t M_t,$$

where $k_1, \cdots, k_t$ are elements of the algebra. We then write

$$A \equiv B \qquad (\text{modd } M_1, \cdots, M_t).$$

All the elements congruent to a given one constitute a class of residues. The classes of residues which give without duplication all the elements form a complete system of classes of residues.

Consider the case of a single modulus M. If an element A is such that $Ax \equiv 1 \pmod{M}$ holds for an element x of the algebra, A is called a *unit residue* modulo M. If $A_1, \cdots, A_k$ are the incongruent unit residues modulo M, the products $A_i A_1, \cdots, A_i A_k$ are incongruent and hence have in some order the residues $A_1, \cdots, A_k$ modulo M. Thus the unit residues form a commutative group. Any element of the algebra is divisible modulo M by any unit residue.

Order of a finite algebra.

5. The integral marks of the algebra will henceforth be denoted by $0, 1, \cdots, m-1$. Let

$$m = p^\alpha q^\beta \cdots r^\gamma, \tag{1}$$

where $p, \cdots, r$ are distinct primes. Then m/p^α is used to denote $q^\beta \cdots r^\gamma$ and not to denote a division to be performed within the algebra. Let S be any element of the algebra; set

$$S \equiv P \pmod{p^\alpha}, \qquad S \equiv Q \pmod{q^\beta}, \cdots, \qquad S \equiv R \pmod{r^\gamma}.$$

Since the power $\varphi(p^\alpha)$ of m/p^α is $\equiv 1$ modulo p^α and to zero modulo $q^\beta, \cdots$, or r^γ, we have in the algebra

$$\left(\frac{m}{p^\alpha}\right)^{\phi(p^\alpha)} S = \left(\frac{m}{p^\alpha}\right)^{\phi(p^\alpha)} P,$$

since the two are congruent modulo m. Adding this equation to those derived by replacing p by $q, \cdots, r$ in turn, we get

$$S = \left(\frac{m}{p^\alpha}\right)^{\phi(p^\alpha)} P + \left(\frac{m}{q^\beta}\right)^{\phi(q^\beta)} Q + \cdots + \left(\frac{m}{r^\gamma}\right)^{\phi(r^\gamma)} R, \tag{2}$$

the coefficient of S being initially the sum of those of $P, \cdots, R$ and hence $\equiv 1$ with respect to each modulus $p^\alpha, \cdots, r^\gamma$ and hence with respect to m. When $P, \cdots, R$ range over the distinct residues of the elements modulo

$p^\alpha, \cdots, r^\gamma$, respectively, the sum (2) ranges without repetition over the elements of the algebra. For, if (2) equals the same function of $P', \cdots, R'$, then

$$P \equiv P' \pmod{p^\alpha}, \quad \cdots, \qquad R \equiv R' \pmod{r^\gamma}.$$

Theorem VI. *If $N(p^\alpha)$ is the number of residues modulo p^α of the elements of the algebra, the order of the algebra is*

$$N(p^\alpha) \cdot N(q^\beta) \cdots N(r^\gamma). \tag{3}$$

To evaluate $N(p^\alpha)$ we first exhibit a set of multiples of $p^{\alpha-1}$ incongruent modulo p^α such that every element which is a multiple of $p^{\alpha-1}$ is congruent to one of the set modulo p^α. The set contains

$$p^{\alpha-1}(d_1 v_1) \qquad (d_1 = 0, 1, \cdots, p-1; v_1 = 1).$$

If $p^{\alpha-1} v_2$ is an additional element of the set, then

$$p^{\alpha-1}(d_1 v_1 + d_2 v_2) \qquad (d_1, d_2 = 0, 1, \cdots, p-1)$$

are easily seen to be incongruent modulo p^α. Proceeding in this way we see that the set is exhausted by the elements, incongruent modulo p^α,

$$p^{\alpha-1} \sum_{k=1}^{e_{\alpha-1}} d_k v_k \qquad (d_k = 0, 1, \cdots, p-1).$$

It follows at once that

$$p^{\alpha-2} \sum_{k=1}^{e_{\alpha-2}} d_k v_k \qquad (d_k = 0, 1, \cdots, p-1)$$

are incongruent modulo $p^{\alpha-1}$. If $p^{\alpha-2} v_f$, where $f = e_{\alpha-1} + 1$, is not congruent to one of the preceding modulo $p^{\alpha-1}$, then

$$p^{\alpha-2} \sum_{k=1}^{f} d_k v_k \qquad (d_k = 0, 1, \cdots, p-1)$$

are incongruent modulo $p^{\alpha-1}$. In this way we see that all multiples of $p^{\alpha-2}$ incongruent modulo $p^{\alpha-1}$ are given without repetition by

$$p^{\alpha-2} \sum_{k=1}^{e_{\alpha-2}} d_k v_k \qquad (d_k = 0, 1, \cdots, p-1; e_{\alpha-2} \geqq e_{\alpha-1}). \tag{4}$$

To obtain a complete set of incongruent residues modulo p^α of the multiples of $p^{\alpha-2}$ we have merely to add to the elements (4) a complete set of multiples of $p^{\alpha-1}$ incongruent modulo p^α:

$$p^{\alpha-2} \sum_{k=1}^{e_{\alpha-2}} d_k v_k + p^{\alpha-1} \sum_{k=1}^{e_{\alpha-1}} d_k v_k \qquad (d_k = 0, 1, \cdots, p-1).$$

The multiples of $p^{\alpha-\alpha}$ include all elements. Hence after α steps we obtain a complete set of incongruent residues modulo p^α:

$$(5) \qquad \sum_{c=0}^{\alpha-1}\left(p^c \sum_{k=1}^{e_c} d_{ck}\, v_k\right) \qquad (d_{ck} = 0, 1, \cdots, p-1;\, e_{c-1} \geqq e_c).$$

Hence $N(p^\alpha) = p^\pi$, where $\pi = e_0 + e_1 + \cdots + e_{\alpha-1}$. Thus $\pi \overset{=}{>} \alpha$.

Theorem VII. *The order of a finite algebra is a multiple of its base m and contains no prime factor not occurring in m.*

6. Consider an element u of a finite algebra and let n be the least positive integer for which u^n is a linear function of $u^{n-1}, \cdots, u$ with integral coefficients. In case u can be chosen so that the elements

$$(6) \qquad a_0 + a_1 u + \cdots + a_{n-1} u^{n-1} \qquad (a_i = 0, 1, \cdots, m-1)$$

exhaust all elements of the algebra, the latter is called a monomorphic algebra. We give an example of an algebra not of this type.

Consider the classes of residues with respect to the modular system

$$(x^4,\ y^4,\ p)$$

x and y being arbitrary variables and p a prime. There are p^{16} distinct classes of residues represented by

$$\sum_{a,\,b}^{0,\,1,\,2,\,3} c_{a,\,b}\, x^a y^b \qquad (c_{ab} = 0, 1, \cdots, p-1).$$

Suppose that this algebra is monomorphic. Then if u is a properly chosen one of the preceding residues, and if n is the least positive integer for which

$$u^n + c_1 u^{n-1} + \cdots + c_n \equiv 0 \quad (\text{modd } x^4,\ y^4,\ p),$$

$c_1, \cdots, c_n$ being integers, we conclude from the fact that $m = p$ is a prime that no two of the elements (6) are congruent with respect to (x^4, y^4, p). By hypothesis, every residue may be given the form (6). Hence $n = 16$.

The p^4 incongruent residues with respect to (x^2, y^2, p) are congruent to certain elements (6) with respect to (x^4, y^4, p) and hence with respect to (x^2, y^2, p). But if k is the least integer for which

$$\psi(u) = u^k + d_1 u^{k-1} + \cdots + d_k \equiv 0 \quad (\text{modd } x^2,\ y^2,\ p),$$

with $d_1, \cdots, d_k$ integers, there are exactly p^k polynomials in u, with integral coefficients, incongruent with respect to (x^2, y^2, p). Hence $k = 4$. From $\psi(u) = \alpha x^2 + \beta y^2 + \gamma p$, we get

$$u^{12} + \cdots = \{\psi(u)\}^3 \equiv 0 \quad (\text{modd } x^4,\ y^4,\ p).$$

Since this contradicts $n = 16$, the algebra is not monomorphic.

We employ the notation (1) for m and make the definition:

For $k < \alpha$, the least integer e_k for which

$$p^k\,(u^{e_k}+c_1\,u^{e_k-1}+\cdots)\equiv 0 \pmod{p^\alpha}\qquad (c\text{'s integers}) \tag{7}$$

is called the degree of u modulo p^α, coefficients p^k. In particular, e_0 is called the degree of u modulo p^α. Multiplying

$$p^{k-1}\,(u^{e_{k-1}}+c_1'\,u^{e_{k-1}-1}+\cdots)\equiv 0 \pmod{p^\alpha}$$

by p and comparing the result with (7), we get $e_k \leqq e_{k-1}$.

Theorem VIII. *If e_k is the degree of u modulo p^α, coefficient p^k, it is also the degree of u modulo p^ϵ, coefficient p^k, where $\alpha > \epsilon > k$.*

Let s the least positive integer for which

$$p^k\,(u^s+d_1\,u^{s-1}+\cdots)\equiv 0 \pmod{p^\epsilon}\qquad (d\text{'s integers}).$$

Since u^{e_0} is congruent modulo p^α to a sum of lower powers of u,

$$p^k\,(u^s+d_1\,u^{s-1}+\cdots)\equiv p^\epsilon\sum_{t=1}^{e_0} f_t u^{e_0-t} \pmod{p^\alpha},$$

where the f_t are integers. If $s < e_k$, multiply each member by the power $e_k - 1 - s$ of u and reduce exponents of u by means of (7). Thus

$$p^k\,\{\,(1-p^{\epsilon-k}c)\,u^{e_k-1}+c'\,u^{e_k-2}+\cdots\,\}\equiv 0 \pmod{p^\alpha}.$$

Multiply this by g, where

$$g\,(1-p^{\epsilon-k}c)\equiv 1 \pmod{p^\alpha}.$$

We obtain a congruence contradicting the definition of e_k in (7).

Order of a monomorphic algebra.

7. Let every element be a polynomial (6) in u. Since u is of degree e_0 modulo p^α, any residue modulo p^α may be written

$$\sum_{\epsilon=0}^{\alpha-1} p^\epsilon \sum_{k=1}^{e_0} d_{\epsilon k}\,u^{e_0-k}\qquad (0\leqq d\leqq p-1). \tag{8}$$

The terms with $\epsilon = 1$ may be reduced by (7) for $k = 1$, to the form

$$p\sum_{k=1}^{e_1} f_{1k}\,u^{e_1-k}+p^2F_2(u)+\cdots+p^{\alpha-1}F_{\alpha-1}(u),$$

where the f's and the coefficients of the F's belong to the set $0, 1, \cdots, p-1$ and each F is of degree $< e_1$. In the new form of (8) occurs

$$p^2\left\{\sum_{k=1}^{e_0} d_{2k}\,u^{e_0-k}+F_2\,(u)\right\},$$

which may be reduced by (7) for $k = 2$ to the form

$$p^2\sum_{k=1}^{e_2} f_{2k} u^{e_2-k} + p^3 G_2(u) + \cdots + p^{\alpha-1} G_{\alpha-1}(u).$$

In this way any residue modulo p^α can be given the form

$$\sum_{c=0}^{\alpha-1} p^c \sum_{k=1}^{e_c} f_{ck} u^{e_c-k} \qquad (0 \leqq f \leqq p-1). \tag{9}$$

Theorem IX. *These elements* (9) *are all incongruent modulo* p^α.

For, if

$$\sum_{c=0}^{\alpha-1} p^c \sum_{k=1}^{e_c} (f_{ck} - g_{ck})\, u^{e_c-k} \equiv 0 \pmod{p^\alpha}, \tag{10}$$

where each f and g is one of the integers $0, 1, \cdots, p-1$, then

$$\sum_{k=1}^{e_0} (f_{0k} - g_{0k})\, u^{e_0-k} \equiv 0 \pmod{p}.$$

By Theorem VIII if $\alpha > 1$ or by (7) if $\alpha = 1$, we get

$$f_{0k} - g_{0k} \equiv 0 \pmod{p} \qquad (k = 1, \cdots, e_0).$$

Hence $f_{0k} = g_{0k}$. The theorem is proved if $\alpha = 1$. If $\alpha > 1$, (10) gives

$$p\sum_{k=1}^{e_1} (f_{1k} - g_{1k})\, u^{e_1-k} \equiv 0 \pmod{p^2}.$$

By Theorem VIII if $\alpha > 2$ or by (7) if $\alpha = 2$,

$$f_{1k} - g_{1k} \equiv 0 \pmod{p}, \qquad f_{1k} = g_{1k}.$$

A repetition of this process proves the theorem for any α.

Write $e_k^{(p)}$ for e_k. Similarly, let $e_k^{(q)}$ be the degree of u modulo q^β, coefficient q^k, etc. Then by (3) and (9), we obtain

Theorem X. *The order of the algebra is* $p^\pi \cdots r^\rho$, *where*

$$\pi = \sum_{k=0}^{\alpha-1} e_k^{(p)}, \quad \cdots, \qquad \rho = \sum_{k=0}^{\gamma-1} e_k^{(r)}.$$

Units of a monomorphic algebra.

8. The degree e_0 of u modulo p^α is also the degree of u modulo p (Theorem VIII). Let therefore

$$F(u) = u^{e_0} + c_1 u^{e_0-1} + \cdots + c_{e_0} \equiv 0 \pmod{p^\alpha},$$

$$F(u) \equiv g_1^{k_1} g_2^{k_2} \cdots g_s^{k_s} \pmod{p},$$

where $g_1, \cdots, g_s$ are incongruent irreducible polynomials in u modulo p, and g_i is of degree n_i. Thus $\Sigma k_i n_i = e_0$. The p^{e_0} elements

$$\sum_{i=1}^{s} \frac{F(u)}{g_i^{k_i}} \sum_{\epsilon=1}^{n_i k_i} c_{i\epsilon}\, u^{n_i k_i - \epsilon} \qquad (c = 0, 1, \cdots, p-1) \tag{11}$$

are incongruent modulo p. For, if not, we have, for example,

$$\frac{F(u)}{g_1^{k_1}} \sum_{\epsilon=1}^{n_1 k_1} (c_{1\epsilon} - c'_{1\epsilon})\, u^{n_1 k_1 - \epsilon} \equiv 0 \quad (\text{modd } g_1^{k_1},\ p), \tag{12}$$

in which $c_{1\epsilon} - c'_{1\epsilon}$ is not divisible by p for every ϵ. There exists [*] a polynomial $G(u)$ with integral coefficients such that in the algebra

$$G(u) \cdot \frac{F(u)}{g_1^{k_1}} \equiv 1 \quad (\text{modd } g_1^{k_1}, p).$$

Multiply (12) by $G(u)$. Hence

$$\sum_{\epsilon=1}^{n_1 k_1} (c_{1\epsilon} - c'_{1\epsilon})\, u^{n_1 k_1 - \epsilon} \equiv L g_1^{k_1} \quad (\text{mod } p).$$

Multiply this by $F(u) / g_1^{k_1}$. Thus

$$\psi(u) \equiv LF(u) \equiv 0 \quad (\text{mod } p),$$

where $\psi(u)$ is of degree $< e_0$, contrary to the fact that u is of degree e_0 modulo p. Hence *the* p^{e_0} *elements* (11) *give a complete set of residues modulo* p.

The residue of any element modulis $g_1^{k_1}$, p may be written

$$\sum_{i=0}^{k_1 - 1} g_1^i \sum_{\gamma=1}^{n_1} d_{i\gamma}\, u^{n_1 - \gamma} \qquad (0 \leqq d \leqq p-1). \tag{13}$$

No two of these are congruent modulis $g_1^{k_1}$, p. For, if (13) be congruent to the element with the coefficients d', we have

$$\sum_{\gamma=1}^{n_1} (d_{0\gamma} - d'_{0\gamma})\, u^{n_1 - \gamma} \equiv 0 \quad (\text{modd } g_1,\ p).$$

Unless each coefficient is divisible by p (and hence zero), we obtain by multiplication by $F(u) / g_1$ a congruence modulo p of degree $< e_0$. Thus $d_{0\gamma} = d'_{0\gamma}$ for each γ. Then a similar argument with

$$g_1 \sum_{\gamma=1}^{n_1} (d_{1\gamma} - d'_{1\gamma})\, u^{n_1 - \gamma} \equiv 0 \qquad (\text{modd } g_1^2, p)$$

shows that $d_{1\gamma} = d'_{1\gamma}$ for each γ; etc. *The elements* (13) *form a complete set of residues modulis* $g_1^{k_1}$, p.

Let R be an element (13) in which not every $d_{0\gamma} = 0$. Then R and $g_1^{k_1}$ have no common divisor modulo p involving u. Hence [†] there exist two

[*] Dickson, *Linear Groups*, p. 8.

[†] Dickson, *Linear Groups*, p. 8.

polynomials K and L in u with integral coefficients such that

$$KR - Lg_1^{k_1} \equiv 1 \pmod{p}.$$

By the definition in § 4, R is a unit residue modulis $g_1^{k_1}, p$.

If an element g_1R of the form (13) with each $d_{0\gamma} = 0$ were a unit residue, $g_1 RK \equiv 1$ (modd $g_1^{k_1}, p$), we would have $F(u)/g_1 \equiv 0 \pmod{p}$.

An element (13) *is a unit residue modulis* $g_1^{k_1}, p$ *if and only if not every* $d_{0\gamma}$ *is zero. The number of these unit residues is*

$$p^{n_1k_1}\left(1 - \frac{1}{p^{n_1}}\right).$$

It now follows from (11) that

$$U = \sum_{i=1}^{s} \frac{F(u)}{g_i^{k_i}} R_i \tag{14}$$

ranges over the incongruent residues modulo p prime to $g_1, \cdots, g_s$ when R_i ranges over the unit residues modulis $g_i^{k_i}, p$. We can determine two functions H and M of u such that

$$HU - MF(u) \equiv 1 \pmod{p},$$

whence $HU \equiv 1 \pmod{p}$. Thus U is a unit residue modulo p.

Theorem XI. *The number of unit residues modulo p is*

$$p^{e_0}\prod_{i=1}^{s}\left(1 - \frac{1}{p^{n_i}}\right).$$

To apply this result to the enumeration of the units, we require the

Lemma. *If two polynomials* $f_0(z)$ *and* $f_1(z)$ *with integral coefficients have no common factor involving z with respect to any of the prime factors of m as modulus, there exist two polynomials* $\psi_0(z)$ *and* $\psi_1(z)$ *with integral coefficients such that*

$$f_0\psi_0 - f_1\psi_1 \equiv 1 \quad (\mathit{mod}\ m). \tag{15}$$

We first prove the lemma when m is a power p^a of a prime. There exist polynomials $x(z)$, $y(z)$ and $w(z)$ such that

$$xf_0 - yf_1 = 1 - pw.$$

Multiply this by $1 + pw + p^2w^2 + \cdots + (pw)^{a-1}$. We obtain (15).

Next, let

$$m = \Pi p_i^{a_i}, \qquad f_0x_i - f_1y_i \equiv 1 \pmod{p_i^{a_i}} \quad (i = 1, \cdots, s).$$

Then (15) holds for

$$\psi_0 = \sum_{i=1}^{s}\left(\frac{m}{p_i^{a_i}}\right)^{\phi(p_i^{a_i})} x_i, \qquad \psi_1 = \sum_{i=1}^{s}\left(\frac{m}{p_i^{a_i}}\right)^{\phi(p_i^{a_i})} y_i.$$

Theorem XII. *The unit residues modulo p^a are*

$$(16)\qquad U + \sum_{c=1}^{a-1} p^c \sum_{k=1}^{e_c} f_{ck} u^{e_c-k},$$

where U ranges over the unit residues modulo p and $f = 0, 1, \cdots, p-1$.

For, by (9) and (14), this set gives a complete set of residues modulo p^a which are prime to $F(u)$. If V is one of them,

$$V\psi_0 - F(u)\psi_1 \equiv 1, \qquad V\psi_0 \equiv 1 \pmod{p^a}.$$

The remaining residues modulo p^a are divisible modulo p by a factor of $F(u)$. If such a residue N is a unit residue, modulo p^a,

$$NZ \equiv 1 \pmod{p^a}, \qquad N \equiv N' g_i \pmod{p}.$$

Hence

$$N' g_i Z \equiv 1, \qquad F(u) / g_i \equiv 0 \pmod{p}.$$

Theorem XIII. *The unit elements of the algebra are*

$$(17)\qquad U_{p^a}\left(\frac{m}{p^a}\right)^{\phi(p^a)} + U_{q^\beta}\left(\frac{m}{q^\beta}\right)^{\phi(q^\beta)} + \cdots + U_{r^\gamma}\left(\frac{m}{r^\gamma}\right)^{\phi(r^\gamma)},$$

where U_{p^a} ranges over the unit residues modulo p^a, etc.

When an element U given by (17) is considered as a function of u, it is prime to $F(u)$ modulo p, to $F_q(u)$ modulo q, etc., where

$$F_q(u) \equiv 0 \pmod{q^\beta}$$

is the congruence of smallest degree satisfied by u modulo q^β. Now

$$M = \left(\frac{m}{p^a}\right)F(u) + \left(\frac{m}{q^\beta}\right)F_q(u) + \cdots + \left(\frac{m}{r^\gamma}\right)F_r(u)$$

is prime to U with respect to any prime factor of m as modulus. By the lemma, we may set

$$U\psi_0 - M\psi_1 \equiv 1 \pmod{m}.$$

Thus $U\psi_0 = 1$ in the algebra, and U is a unit.

For an element N not of type (17), there is a prime factor μ of m and a factor G of $F_\mu(u)$ modulo μ such that

$$N \equiv GN' \pmod{\mu}.$$

Then N is not a unit. For if so we would have

$$GN'K \equiv 1, \qquad F_\mu(u)/G \equiv 0 \pmod{\mu}.$$

By Theorems XI and XIII, the number of unit residues modulo p^a is

$$(18)\qquad V(p^a) = p^E \prod_{i=1}^{s}\left(1 - \frac{1}{p^{n_i}}\right), \qquad E = e_0 + e_1 + \cdots + e_{a-1}.$$

Hence by (17) the number of units in the algebra is

$$V(p^\alpha)\cdot V(q^\beta)\cdots V(r^\gamma).$$

9. Write relation (7) in the form

$$p^k F_k(u) \equiv 0 \pmod{p^\alpha} \qquad (k = 0, 1, \cdots, \alpha - 1). \tag{19}$$

Let R be the polynomial in u of degree $< e_i$ for which

$$F_{i-1} = F_i \psi_i + R.$$

Then $p^i R \equiv 0 \pmod{p^\alpha}$. Hence, by the definition of e_i, each coefficient in $R(u)$ is divisible by p. Thus

$$F_{i-1} = F_i \psi_i + pR_i \qquad (i = 1, \cdots, \alpha - 1). \tag{20}$$

It follows at once that

$$F_0 \equiv F_{\alpha-1}\psi_1\psi_2\cdots\psi_{\alpha-1} \pmod{p}.$$

Now $e_{i-1} \geqq e_i$. Unless $e_{i-1} = e_i$, and therefore $F_{i-1} = F_i$, ψ_i is not independent of u. *Hence F_0 has at least as many factors modulo p as there are distinct integers in the set $e_0, e_1, \ldots, e_{\alpha-1}$.*

Hensel* has given a reduction of the modular system

$$(p^\alpha, f_1(x), f_2(x), \cdots, f_u(x)),$$

in which p is the least integer dividing the system, to a canonical form

$$[p^\alpha, p^{\alpha-1}f_1'(x), p^{\alpha-2}f_2'(x), \cdots, f_\alpha'(x)],$$

in which the f_i' are connected by certain relations and the coefficient of the highest power of x in each f_i' is prime to p. The classes of residues with respect to this modular system define a monomorphic finite algebra. The f_i' have the same properties as the functions F_i in the abstract algebra with the base $m = p^\alpha$. Under the latter restriction, F_0, $pF_1, \ldots, p^{\alpha-1}F_{\alpha-1}$ are zero in the algebra.

* Kronecker's *Vorlesungen über Zahlentheorie*, vol. 1, pp. 202–211.