SOME TOPICS IN THE ARITHMETIC OF POLYNOMIALS

L. CARLITZ

1. **Introduction.** Let $GF(p^n)$ denote a fixed Galois (finite) field, and x an indeterminate. The arithmetic of polynomials in x with coefficients in $GF(p^n)$ is in many ways similar to ordinary arithmetic, and was discussed in some detail by Dedekind.[1] As a matter of fact it appears that in many instances the arithmetic of polynomials is the simpler. Thus, for example, in the case of the analogues of the familiar arithmetic functions, in place of asymptotic formulas there are exact formulas for the polynomial domain. This is perhaps due to the possibility of grouping polynomials according to degree. Again it is familiar that in the problem of representing a rational integer as a sum of an even number of squares there is a considerable difference between the case $2t \leqq 8$ and $2t > 8$; in the former case the number of representations can be expressed in terms of divisor functions, while in the latter case this is in general impossible. For the polynomial case however the number of representations by an even number of squares can always be expressed in terms of divisor functions. Similar remarks apply to the case of an odd number of squares.

In the present paper we rather arbitrarily select three or four topics in the arithmetic of polynomials in a Galois field. In §2 we consider the simplest arithmetic functions. In §3 we discuss the problem of representing a given polynomial as a sum of squares. In §4 we define various special polynomials and functions that are rather intimately connected with the arithmetic of polynomials in $GF(p^n)$; application to power sums are given in §5. Finally in §6 we define analogues of the ordinary Bernoulli numbers; the principal result here is the Staudt-Clausen theorem. We remark that for the most part the extension of theorems from the coefficient field[2] $GF(p)$ to $GF(p^n)$ is quite trivial; however, in at least the last topic mentioned there appears to be some difference between the special and the general case.

It is evident from the above that we are ignoring such questions as construction and distribution of irreducible polynomials, the existence of irreducibles in an arithmetic progression, theorems of reciproc-

An address delivered before the meeting of the Society in Hanover, N. H., on September 12, 1940, by invitation of the Program Committee under the title *Arithmetic of polynomials in a Galois field*; received by the editors January 22, 1942.

[1] Journal für die reine und angewandte Mathematik, vol. 54 (1857), pp. 1–26.

[2] The field $GF(p)$ may be defined as the set of residues (mod p).

ity and higher congruences generally, to mention a few obvious omissions. We give a few references below.[3]

2. **Arithmetic functions.**[4] It will be convenient to denote polynomials in x by capitals $A, B, \cdots, Z$; elements of $GF(p^n)$ and ordinary integers will be denoted by small letters. We write deg M for the degree of M and put $|M| = p^{nm}$, $m = \deg M$; if the coefficient of the highest power of x in M is 1 we call M *primary*. The letter P will be reserved for *irreducible* polynomials. Evidently the number of primary polynomials of fixed degree m is p^{nm}. Hence the ζ-function for our domain becomes

$$\zeta(s) = \sum_M \frac{1}{|M|^s} = \sum_{m=0}^{\infty} \frac{p^{nm}}{p^{nms}} = \frac{1}{1 - p^{n(1-s)}} \tag{2.1}$$

for $\Re(s) > 1$; the first summation in (2.1) is taken over all primary polynomials. Now since the unique factorization theorem applies here we have

$$\begin{aligned}\sum_M \frac{1}{|M|^s} &= \prod_P \left\{1 + \frac{1}{P^s} + \frac{1}{P^{2s}} + \cdots\right\} \\ &= \prod_P \left\{1 - \frac{1}{|P|^{-s}}\right\}^{-1} = \prod_{k=1}^{\infty} \left\{1 - \frac{1}{p^{ks}}\right\}^{-f(k)},\end{aligned}$$

where $f(k)$ denotes the number of (primary) irreducible polynomials of degree k. Comparison with (2.1) leads to the identity

$$1 - p^{n(1-s)} = \prod_{k=1}^{\infty} (1 - p^{-ks})^{f(k)}, \tag{2.2}$$

by means of which it is easy to derive the familiar formula for $f(k)$. We remark that (2.2) can be considerably extended.

Now define the Möbius function $\mu(M)$ by means of

$$\mu(1) = 1, \qquad \mu(M) = 0 \quad \text{for} \quad P^2 \mid M,$$
$$\mu(M) = (-1)^r \quad \text{for} \quad M = P_1 \cdots P_r.$$

Then

$$\sum_M \frac{\mu(M)}{|M|^s} = \prod_P \left(1 - \frac{1}{|P|^s}\right) = \frac{1}{\zeta(s)} = 1 - p^{n(1-s)},$$

[3] See for example L. E. Dickson, *Linear Groups*, 1901, pp. 3–54; H. Kornblum, Mathematische Zeitschrift, vol. 5 (1919), p. 107; E. Artin, Mathematische Zeitschrift, vol. 19 (1924), pp. 153–246; O. Ore, Transactions of this Society, vol. 35 (1933), pp. 559–584; L. Carlitz, American Journal of Mathematics, vol. 59 (1937), pp. 618–628.

[4] Compare American Journal of Mathematics, vol. 54 (1932), pp. 39–50.

and therefore

$$\sum_{\deg M=m} \mu(M) = \begin{cases} -p^n & \text{for } m = 1, \\ 0 & \text{for } m > 1. \end{cases}$$

Similarly the number of quadrat-frei (simple) polynomials of degree m is $p^{nm} - p^{n(m-1)}$.

In exactly the same way if $\delta(M)$ denotes the number of (primary) divisors of M and $\phi(M)$ denotes the Euler function (number of residues in a reduced residue system (mod M)) then we have the identities

$$\sum_M \frac{\delta(M)}{|M|^s} = \zeta^2(s) = (1 - p^{n(1-s)})^{-2},$$

$$\sum_M \frac{\phi(M)}{|M|^s} = \frac{\zeta(s-1)}{\zeta(s)} = \frac{1 - p^{n(1-s)}}{1 - p^{n(2-s)}},$$

by means of which it is easy to evaluate

$$\sum_{\deg M=m} \delta(M), \qquad \sum_{\deg M=m} \phi(M).$$

We remark that $\delta(M)$ and $\phi(M)$ may be generalized in the following way

$$\delta_k(M) = \sum_{A|M,\ \deg A=k} 1, \tag{2.3}$$

that is, the number of divisors of given degree k. Similarly $\phi_k(M)$ denotes the number of primary polynomials of degree k, each prime to M. These functions are useful in certain problems (see, for example, (3.8) below).

3. **Sums of squares.**[5] Assume p odd. Let t be an integer greater than 0; $\alpha_1, \cdots, \alpha_t, \beta_1, \cdots, \beta_t$ elements of $GF(p^n)$ such that

$$\gamma_i = \alpha_i + \beta_i \neq 0, \qquad i = 1, \cdots, t. \tag{3.1}$$

Then if $\gamma = \gamma_1 + \cdots + \gamma_t \neq 0$, and M is primary of even degree $2k$, we seek the number of solutions of

$$\gamma M = \alpha_1 X_1^2 + \beta_1 Y_1^2 + \cdots + \alpha_t X_t^2 + \beta_t Y_t^2 \tag{3.2}$$

in primary X_i, Y_i of degree k. We call the problem (A).

Next if $\gamma_1 + \cdots + \gamma_t = 0$, $\alpha \neq 0$, and M is primary of degree less then $2k$, we seek the number of solutions of

[5] Compare Transactions of this Society, vol. 35 (1933), pp. 397–410; Duke Mathematical Journal, vol. 1 (1935), pp. 298–315.

$$(3.3)\qquad \alpha M = \alpha_1 X_1^2 + \beta_1 Y_1^2 + \cdots + \alpha_t X_t^2 + \beta_t X_t^2.$$

We call this problem (B).

The solution of these problems is given in terms of certain "divisor" functions now to be defined. For brevity we limit ourselves to the case of problem (A). Put

$$(3.4)\qquad \rho_t(M) = \left(1 - \frac{1}{p^{nt}}\right) \sum_{A|M}^{a>k} |A|^t + \sum_{A|M}^{a=k} |A|^t,$$

where $a = \deg A$, $|A| = p^{na}$, the first summation is over all primary A dividing M and of degree greater than k, the second is over all primary A dividing M and of degree equal to k;

$$(3.5)\qquad \omega_t(M) = \left(1 + \frac{1}{p^{nt}}\right) \sum_{A|M}^{a>k} (-1)^a |A|^t + \sum_{A|M}^{a=k} (-1)^a |A|^t,$$

the notation having the same meaning as in (3.4). *Then the number of solutions of* (3.2) *is* $\rho_{t-1}(M)$ *or* $\omega_{t-1}(M)$ *according as*

$$(-1)^t \alpha_1 \cdots \alpha_t \beta_1 \cdots \beta_t$$

is or is not a square in $GF(p^n)$.

The proof of this theorem is by induction. The case $t=1$ is easily proved. For the rest it suffices to prove the following three formulas

$$(3.6)\qquad \begin{aligned} \sum \rho_s(A)\rho_t(B) &= \rho_{s+t+1}(M), \\ \sum \rho_s(A)\omega_t(B) &= \omega_{s+t+1}(M), \\ \sum \omega_s(A)\omega_t(B) &= \rho_{s+t+1}(M), \end{aligned}$$

where the summation is over all primary A, B of degree $2k$ such that

$$(3.7)\qquad (\alpha + \beta)M = \alpha A + \beta B,$$

and α, β are elements of $GF(p^n)$, $\alpha\beta(\alpha+\beta) \neq 0$. We sketch briefly a proof of the first of (3.6); by introducing certain additional notation we may prove all three formulas simultaneously.

It is convenient to make use of the divisor function $\delta_i(M)$ defined in (2.3). For this function we have the theorem[6]

$$(3.8)\qquad \sum \delta_i(A)\delta_j(B) = (1 - p^{-n}) \sum_{a=i+1}^{2k} \delta_a(M) + \delta_i(M),$$

where $k \leqq j \leqq i \leqq 2k$, and the summation on the left is over all A,

[6] Proceedings of the London Mathematical Society, (2), vol. 38 (1934), pp. 116–124, in particular, p. 122.

B satisfying (3.7). Then by (3.4)

$$\sum \rho_s(A)\rho_t(B) = \epsilon_s\epsilon_t \sum_{i,j=k+1}^{2k} p^{n(is+jt)}g(i, j) + p^{nk(s+t)}g(k, k)$$

$$+ \epsilon_s p^{nkt} \sum_{i=k+1}^{2k} p^{nis}g(i, k) + \epsilon_t p^{nks} \sum_{j=k+1}^{2k} p^{njt}g(k, j),$$

where $g(i, j)$ denotes the left member of (3.8) and $\epsilon_t = 1 - p^{-nt}$. Now using (3.8) the proof of the formula in question follows without much difficulty.

We have assumed p odd. For $p=2$ the right member of (3.2) or (3.3) is a perfect square and therefore the problem is of no interest. However, in this case we may consider the number of solutions of

$$\gamma M = \sum_{i=1}^{t} (\alpha_i X_i^2 + \beta_i X_i Y_i + \gamma_i Y_i^2),$$

where now $\prod \beta_i \neq 0$. It may be shown that results similar to the above still hold. The final form of the result depends on whether the quadratic form $\alpha_i X^2 + \beta_i XY + \gamma_i Y^2$ is irreducible in $GF(2^n)$. As a special case of some interest we take

$$(3.9) \qquad \gamma M = \beta_1 X_1 Y_1 + \cdots + \beta_t X_t Y_t,$$

where

$$\gamma = \beta_1 + \cdots + \beta_t \neq 0, \qquad \beta_i \neq 0.$$

Evidently the number of solutions of this problem in primary X_i, Y_i of degree k is

$$(3.10) \qquad \sum \delta_k(M_1) \cdots \delta_k(M_t),$$

the summation extending over primary M_i of degree $2k$ such that $\gamma M = \beta_1 M_1 + \cdots + \beta_t M_t$. But by (3.4) and the definition of $\delta_i(M)$ it is clear that $\delta_k(M) = \rho_0(M)$, so that (3.9) becomes

$$\sum \rho_0(M_1) \cdots \rho_0(M_t) = \rho_{t-1}(M),$$

as follows from (3.6). Hence the number of solutions of (3.9) is $\rho_{t-1}(M)$. This result holds for all p.

The situation for an odd number of squares is quite different. Corresponding to (3.2) we consider

$$(3.11) \qquad \epsilon M = \alpha_1 X_1^2 + \cdots + \alpha_{2t+1} X_{2t+1}^2,$$

where $\epsilon = \alpha_1 + \cdots + \alpha_{2t+1} \neq 0$, while to (3.3) corresponds

$$(3.12) \qquad \alpha M = \alpha_1 X_1^2 + \cdots + \alpha_{2t+1} X_{2t+1}^2,$$

where $\alpha_1 + \cdots + \alpha_{2t+1} = 0$, $\alpha \neq 0$ arbitrary.

Put $\theta = (-1)^t \epsilon \alpha_1 \cdots \alpha_{2t+1}$ or $(-1)^t \alpha \alpha_1 \cdots \alpha_{2t+1}$ according as (3.11) or (3.12) is being considered. For simplicity we limit ourselves to the case M quadrat-frei. Then the number of solutions of (3.11) or (3.12) is given by

$$(3.13) \qquad \begin{aligned} p^{nk(t-1)}\{\sigma_k + p^{nt}\sigma_{k-1} + (p^{2nt} - p^n)\sigma_{k-2} + \cdots \\ + (p^{nkt} - p^{n(kt-2t+1)})\sigma_0\} \end{aligned}$$

where

$$\sigma_j = \sigma_j(\theta M) = \sum_{\deg A = j} (\theta M/A),$$

summed over primary A of degree j, and $(\theta M/A)$ is the quadratic residue symbol. The proof of (3.13) depends on the previous results for (3.2) and (3.3).

We remark finally that the results of this section can be obtained by an entirely different method which applies to either an odd or even number of squares. This was suggested by Hardy's paper *On the representation of a number as the sum of any number of squares and in particular of five.*[7] However, we shall not take the space to discuss this method.

4. Special polynomials and functions.[8] Put

$$(4.1) \qquad \begin{aligned} F_k &= [k][k-1]^{p^n} \cdots [1]^{p^{n(k-1)}}, & F_0 &= 1, \\ L_k &= [k][k-1] \cdots [1], & L_0 &= 1, \end{aligned}$$

where

$$[k] = x^{p^{nk}} - x.$$

Then as is well known, $[k]$ is the product of irreducible polynomials of degree a divisor of k. As for F_k and L_k, it may be shown that F_k is the product of the (primary) polynomials of degree k, while L_k is the least common multiple of these polynomials.

Next consider

$$(4.2) \qquad \psi_m(t) = \prod_{\deg A < m} (t + A), \qquad \psi_0(t) = t,$$

where t is a second indeterminate and the product is over all $A = A(x)$ of degree less than m. It is not difficult to show that (4.2) implies

[7] Transactions of this Society, vol. 21 (1920), pp. 255–284.

[8] Compare Duke Mathematical Journal, vol. 1 (1935), pp. 137–168.

$$(4.3) \qquad \psi_m(t) = \sum_{i=0}^{m} (-1)^{m-i} \begin{bmatrix} m \\ i \end{bmatrix} t^{p^{ni}},$$

where the coefficients are determined by

$$\begin{bmatrix} m \\ i \end{bmatrix} = \frac{F_m}{F_i L_{m-i}^{p^{ni}}}, \qquad \begin{bmatrix} m \\ 0 \end{bmatrix} = \frac{F_m}{L_m}, \qquad \begin{bmatrix} m \\ m \end{bmatrix} = 1,$$

and are integral, that is, polynomials in x. Of the properties of $\psi_m(t)$ that follow from (4.3) we mention

$$(4.4) \qquad \psi_m(xt) = x\psi_m(t) + [m]\psi_{m-1}^{p^n}(t),$$

$$(4.5) \qquad \psi_m(t) = \psi_{m-1}^{p^n}(t) - F_{m-1}^{p^n-1}\psi_{m-1}(t).$$

Also as a consequence of (4.2) we have

$$(4.6) \qquad \psi_m(M) = F_m$$

for M primary of degree m. Note that

$$\psi_m(t+u) = \psi_m(t) + \psi_m(u), \quad \psi_m(ct) = c\psi_m(t) \text{ for } c \text{ in } GF(p^n);$$

we therefore call $\psi_m(t)$ a "linear" polynomial.

The formula (4.4) suggests the operator Δ defined by

$$\Delta g(t) = g(xt) - xg(t);$$

Δ^k is defined recursively by

$$\Delta^{k+1}g(t) = \Delta^k g(xt) - x^{p^{nk}}\Delta^k g(t).$$

From these formulas it follows in particular that

$$(4.7) \qquad \Delta^k\psi_m(t) = [m]\cdots[m-k+1]^{p^{n(k-1)}}\psi_{m-k}^{p^{nk}}(t), \qquad m \geqq k.$$

Now let $g(t) = \sum \alpha_i t^{p^{ni}}$ be any linear polynomial in t. Clearly it may be expressed in the form $\sum \beta_i \psi_i(t)$. The coefficients are readily determined by means of (4.7). Replacing t by tu we get the expansion

$$(4.8) \qquad g(tu) = \sum_i (1/F_i)\psi_i(u)\Delta^i g(t).$$

Thus for $g(t) = \psi_m(t)$, (4.8) becomes

$$(4.9) \qquad \psi_m(tu) = \sum_{i=0}^{m} \begin{Bmatrix} m \\ i \end{Bmatrix} \psi_i(u)\psi_{m-i}^{p^{ni}}(t),$$

while for $g(t) = t^{p^{nm}}$ we get

$$t^{p^{nm}} = \sum_{i=0}^{m} \left\{ \begin{matrix} m \\ i \end{matrix} \right\} \psi_i(t). \tag{4.10}$$

The coefficients in (4.9) and (4.10) are given by

$$\left\{ \begin{matrix} m \\ i \end{matrix} \right\} = \frac{F_m}{F_i F_{m-i}^{p^{ni}}}, \qquad \left\{ \begin{matrix} m \\ 0 \end{matrix} \right\} = \left\{ \begin{matrix} m \\ m \end{matrix} \right\} = 1,$$

and are integral.

The polynomial $\psi_m(t)$ suggests the construction of a function vanishing for all $A = A(x)$. We find that the function

$$\psi(t) = \sum_{i=0}^{\infty} (-1)^i t^{p^{ni}}/F_i \tag{4.11}$$

has the product expansion

$$\psi(t) = t \prod_{M} \left\{ 1 - \frac{t^{p^n-1}}{(M\xi)^{p^n-1}} \right\}, \tag{4.12}$$

the product extending over *all* primary M. Hence $\psi(A\xi) = 0$ for all A. As for ξ it may be defined by

$$\xi = \lim_{k=\infty} \frac{[1]^{p^{nk}/(p^n-1)}}{L_k} \cdot \tag{4.13}$$

It has recently been proved[9] that ξ is transcendental relative to the field $GF(p^n, x)$, that is, the field of rational functions in x with coefficients in $GF(p^n)$.

Applying the operator Δ to $\psi(t)$ we find

$$\psi(xt) = x\psi(t) - \psi^{p^n}(t); \tag{4.14}$$

repeated use of this formula leads to the multiplication formula

$$\psi(Mt) = \sum_{i=0}^{m} (-1)^i \frac{\psi_i(M)}{F_i} \psi^{p^n}(t), \tag{4.15}$$

where M is primary of degree m. This in turn suggests the introduction of the linear polynomial $\omega_M(u)$ defined by

$$\omega_M(\psi(t)) = \psi(Mt);$$

next put

$$W_M(u) = \prod_{AB=M} \{\omega_A(u)\}^{\mu(B)},$$

with $\mu(B)$ as in §2. Then $W_M(u)$ may be thought of as an analogue of the cyclotomic polynomial; in particular it is irreducible.[10]

[9] L. I. Wade, Duke Mathematical Journal, vol. 8 (1941), pp. 701–720.

[10] See Transactions of this Society, vol. 43 (1938), pp. 167–182.

Returning to (4.11) we find that the inverse of $\psi(t)$ is also of simple form, namely

$$\lambda(t) = \sum_{i=0}^{\infty} (1/L_i)t^{p^{ni}}. \tag{4.16}$$

As for the convergence of (4.11) and (4.16) if we take

$$t = c_k x^k + \cdots + c_0 + \frac{c_{-1}}{x} + \cdots , \tag{4.17}$$

where the c_j are all in $GF(p^n)$, then $\psi(t)$ converges for all t while $\lambda(t)$ converges only for $k \leqq 1$.

It follows from (4.11) and (4.12) that

$$\psi(t + M\xi) = \psi(t) + \psi(M\xi) = \psi(t), \tag{4.18}$$

for arbitrary M; in other words $\psi(t)$ has the period ξ. This property can be generalized and "linear" functions with any number of periods can be constructed. For example, if we write (4.17) in the form

$$\psi(t + M_0\xi + M_1\theta\xi + \cdots + M_{n-1}\theta^{n-1}\xi) = \psi(t),$$

where θ defines $GF(p^n)$ and the M_i have coefficients in $GF(p)$, then we may regard $\psi(t)$ as an n-ply periodic function with respect to the smaller field. For the general case we put

$$f(t) = \sum_{i=0}^{\infty} (-1)^i A_i t^{p^{ni}}/F_i; \tag{4.19}$$

in place of (4.14) we now have

$$f(xt) = xf(t) + \sum_{j=1}^{k} (-1)^j \gamma_j f^{p^{ni}}(t), \tag{4.20}$$

which is characteristic. Using (4.20) we get a recursion for A_i,

$$A_i = \sum_{j=1}^{k} \frac{F_{i-1}^{p^n}}{F_{i-j}^{p^{nj}}} \gamma_j A_{i-j}^{p^{nj}}.$$

It is easily verified that (4.19) converges for all t defined by (4.17). The multiplication formula (4.15) now becomes

$$f(Mt) = \sum_{i=0}^{mk} (-1)^i \frac{f_i(M)}{F_i} f^{p^{ni}}(t),$$

thus defining a set of linear polynomials $f_i(u)$.

5. **Power sums.**[11] Going back to (4.2) it is not difficult to show that it implies

$$(5.1)\qquad \sum_{\deg M=m} \frac{1}{t+M} = (-1)^m \frac{F_m}{L_m} \frac{1}{\psi_m(t)+F_m}.$$

In this identity put $t=0$ and we get

$$(5.2)\qquad \sum_{\deg M=m} (1/M) = (-1)^m/L_m,$$

so that by the remark at the beginning of §4, the sum of the reciprocals of the polynomials of degree m is, except for sign, the reciprocal of the L. C. M. If we expand (5.1) in descending powers of t it is easily seen that

$$(5.3)\qquad \sum_{\deg M=m} M^{p^{nm}-1} = (-1)^m F_m/L_m$$

while

$$(5.4)\qquad \sum_{\deg M=m} M^k = 0 \qquad \text{for} \quad k < p^{nm}-1.$$

(5.2) and (5.3) are special cases of[12]

$$(5.5)\qquad \sum_{\deg M=m} M^{p^{nk}-1} = (-1)^m \frac{F_k}{L_m F_{k-m}^{p^{nm}}}, \qquad k \geqq m,$$

and

$$(5.6)\qquad \sum_{\deg M=m} M^{1-p^{nk}} = \frac{L_{k+m-1}}{L_{k-1} L_m^{p^{nk}}}.$$

We outline a new proof of these formulas.

Consider the sum

$$(5.7)\qquad \sum_{\deg M=m} M(t)/M(x).$$

Since (5.7) is a polynomial in t of degree m, it may be determined by assigning $m+1$ values to t. We take

$$t = x^{p^{ni}}, \qquad i = 0, 1, \cdots, m.$$

Using the Lagrange interpolation formula together with (5.3) and (5.4) leads to the identity

$$(5.8)\quad \sum_M M(t)/M(x) = ((-1)^m/L_m)(t-x)(t-x^{p^n}) \cdots (t-x^{p^{n(m-1)}}).$$

[11] Compare Duke Mathematical Journal, vol. 5 (1939), pp. 941–947.

[12] More general formulas are proved by H. L. Lee in a Duke University thesis.

In (5.8) take $t=x^{p^{nk}}$ and we get (5.5); on the other hand interchange x and t, put $t=x^{p^{nk}}$, and the result is (5.6).

We next construct a polynomial[13] $G_m(t)$ which is useful in evaluating more general power sums. Put

$$m = a_0 + a_1p^n + a_2p^{2n} + \cdots, \qquad 0 \leqq a_i < p^n;$$

then define

$$G_m(t) = \psi_0^{a_0}(t)\psi_1^{a_1}(t)\psi_2^{a_2}(t)\cdots, \qquad G_0(t) = 1, \tag{5.9}$$

so that $G_m(t)$ is of degree m in t, and the coefficients are integral in x. We also define

$$g_m = F_1^{a_1}F_2^{a_2}\cdots, \qquad g_0 = 1. \tag{5.10}$$

We shall not now go into the connection between $G_m(t)$ and power sums but instead quote an application of a different sort. A polynomial $f(t)$ may be called integral-valued if $f(A)$ is integral for all integral A. Then we have the theorem:—*the polynomial*

$$\sum_{i=0}^{k} A_iG_i(t)/g_i$$

is integral-valued if and only if the coefficients A_i are integral, that is, polynomials in x.

6. **Bernoulli numbers.**[14] As analogues of the Bernoulli numbers we define a set of rational functions B_m by means of

$$\frac{t}{\psi(t)} = \sum_{m=0}^{\infty} \frac{B_m}{g_m} t^m, \tag{6.1}$$

where $\psi(t)$ is defined by (4.11) and g_m is given by (5.10). Note that B_m is defined only for m a multiple of p^n-1. Then in the first place we have the formula

$$\sum_A \frac{1}{A^m} = \frac{B_m}{g_m}\xi^m, \qquad p^n - 1 \mid m, \tag{6.2}$$

the summation extending over all primary polynomials, and ξ as in (4.13). Thus (6.2) is the analogue of a familiar formula; in particular it shows that $B_m \neq 0$. Unfortunately no formula connecting B_m with

[13] See Duke Mathematical Journal, vol. 6 (1940), pp. 486–504.

[14] Compare Duke Mathematical Journal, vol. 3 (1937), pp. 503–517; vol. 7 (1940), pp. 62–67.

finite power sums is available and therefore the usual methods for deriving arithmetic properties of the ordinary Bernoulli numbers paparently cannot be applied. Instead we make use of certain ideas due to Hurwitz.[15]

We call a series of the form

$$H(t) = \sum_{m=0}^{\infty} A_m t^m / g_m, \tag{6.3}$$

where the A_m are integral, a Hurwitz series, briefly an H-series. It follows that the sum and product of two H-series are again H-series; if $A_0 = 1$ then the reciprocal is an H-series. If $A_0 = 0$ we call (6.3) an H_1-series. For this case we have the result that H_1^k/g_k is an H-series. This result applied to

$$\psi^{p^{nk}-1}(t) = \sum_m A_m^{(k)} t^m / g_m \tag{6.4}$$

shows that $A_m^{(k)}$ is a multiple of F_k/L_k.

Now returning to the definition of B_m we have

$$\frac{t}{\psi(t)} = \frac{\lambda(\psi(t))}{\psi(t)} = \sum_{k=0}^{\infty} \frac{1}{L_k} \psi^{p^{nk}-1}$$

by (4.15) and therefore using (6.4) we get the formula

$$B_m = \sum_k \frac{1}{L_k} A_m^{(k)}. \tag{6.5}$$

From this result it follows that the denominator of B_m contains only simple factors. To improve this we require the following lemma: *Let P be irreducible of degree k. Then*

$$\psi^{p^{nk}-1}(t) \equiv \left\{ \sum_{i=0}^{\infty} (-1)^i \frac{t^{p^{nki}}}{F_{ki}} \right\}^{p^{nk}-1} \pmod{P}. \tag{6.6}$$

It is now easy to evaluate $A_m^{(k)}$ (mod P). Substituting in (6.5) we get the following result.

THEOREM ($p^n \neq 2$). *Let*

$$m = \sum_i a_i p^i, \qquad 0 \leqq a_i < p.$$

Then if

[15] Mathematische Annalen, vol. 51 (1899), pp. 196–226 (= Mathematische Werke II, Basel, 1933, pp. 342–373).

$$(6.7)\qquad \sum_i a_i = nk(p-1), \qquad p^{nk}-1 \mid m,$$

is inconsistent, B_m is integral; while if (6.7) *is consistent, k is uniquely determined and*

$$(6.8)\qquad B_m = G_m - e \sum_{\deg P = k} \frac{1}{P},$$

where G_m is integral, the summation is over irreducible polynomials P of degree k, and

$$e = \frac{(-1)^{nk+dk}}{\prod_i (a_i!)}, \qquad d = \sum_{i,j} i a_{ink+j}.$$

The case $p^n = 2$ is covered by a supplementary theorem which we shall omit.

We remark that if the function $f(t)$ has an inverse of the form $\sum (D_i/L_i) t^{p^{ni}}$, where the D_i are integral, then for the coefficients of $t/f(t)$ there is a decomposition into partial fractions similar to (6.8). This result evidently generalizes the above theorem on B_m.

Duke University