STRONGLY DEFINITE POLYNOMIALS

D. J. Lewis

A polynomial $F(X) = F(x_1, x_2, \cdots, x_n)$ over a ring R will be said to be a *definite polynomial over* R provided it has the property that its only zero in R is the trivial one; that is, provided for all a_i in R, the equation $F(a_1, a_2, \cdots, a_n) = 0$ holds if and only if $a_i = 0$ for $i = 1, 2, \cdots, n$. Chevalley [2] proved that, for definite polynomials over finite fields, the number of indeterminates cannot exceed the degree of the polynomial. Brauer [1] demonstrated the existence of a function Φ_K such that if $F(X)$ is a definite, homogeneous polynomial of degree d over a $\mathfrak{p}$-adic field K, then $n \leq \Phi_K(d)$. No expression or bound for $\Phi_K(d)$ has been determined, except that when $d \leq 3$, then $\Phi_K(d) = d^2$ (see [3, p 128], [4]).

Let K be a field which is complete under a discrete valuation, and which has a finite residue class field. Let $\mathfrak{o}$ be the ring of integers of K, $\mathfrak{p}$ the prime ideal in $\mathfrak{o}$, π a prime in $\mathfrak{p}$, and q the number of elements in the residue class field $\mathfrak{o}/\mathfrak{p}$.

If $F(X)$ is definite over $\mathfrak{o}$, then the compactness of $\mathfrak{o}$ implies the existence of a rational integer m such that, for a_i in $\mathfrak{o}$, $F(a_1, a_2, \cdots, a_n) \equiv 0 \pmod{\mathfrak{p}^m}$ only if each $a_i \equiv 0 \pmod{\mathfrak{p}}$. This suggests a definition: A polynomial $F(X)$ of degree d over $\mathfrak{o}$ will be said to be *strongly definite over* $\mathfrak{o}$ provided that, for a_i in $\mathfrak{o}$,

$$F(a_1, a_2, \cdots, a_n) \equiv 0 \pmod{\mathfrak{p}^d}$$

if and only if $a_i \equiv 0 \pmod{\mathfrak{p}}$ $(i = 1, 2, \cdots, n)$. While we are unable to determine an explicit formula for Φ_K, we are able to obtain some results for strongly definite polynomials.

THEOREM. *There exist polynomials* $\phi_d(y)$, *of degree* $d - 1$ *over the ring of rational integers, such that if* $F(X)$ *is a strongly definite polynomial over* $\mathfrak{o}$, *of degree* d $(d < q)$, *then* $n \leq d^2 \phi_d(q - 1)$.

Our method of proof is analogous to that used in [2]. Let $\mathfrak{B}_n$ be the set of all n-tuples of $\mathfrak{o}/\mathfrak{p}$, and let $\mathfrak{R}_n$ be the ring of all functions from $\mathfrak{B}_n$ to $\mathfrak{o}/\mathfrak{p}^d$. A polynomial $S(X)$ in n indeterminates over $\mathfrak{o}$ will be said to represent a function in $\mathfrak{R}_n$ if, whenever $a_i \equiv b_i \pmod{\mathfrak{p}}$ $(i = 1, 2, \cdots, n)$, then $S(a_1, a_2, \cdots, a_n) \equiv S(b_1, b_2, \cdots, b_n) \pmod{\mathfrak{p}^d}$. For the remainder of this paper, all polynomials have coefficients in $\mathfrak{o}$, unless the contrary is stated.

Let $H(x) = 1 - x^{q-1}$. Clearly the polynomial $G(x) = H^d(x)$, with $d < q$, represents a function in $\mathfrak{R}_1$; for

$$G(a) \equiv \begin{cases} 1 \pmod{\mathfrak{p}^d} & \text{if } a \equiv 0 \pmod{\mathfrak{p}}, \\ 0 \pmod{\mathfrak{p}^d} & \text{if } a \not\equiv 0 \pmod{\mathfrak{p}}. \end{cases} \tag{1}$$

Consequently $W(X) = \prod_{i=1}^{n} G(x_i)$ represents the basic idempotent function in the ring $\mathfrak{R}_n$, for

Received March 29, 1956.

$$W(a_1, a_2, \cdots, a_n) \equiv \begin{cases} 1 \pmod{\mathfrak{p}^d} & \text{if each } a \equiv 0 \pmod{\mathfrak{p}}, \\ 0 \pmod{\mathfrak{p}^d} & \text{if some } a \not\equiv 0 \pmod{\mathfrak{p}}. \end{cases} \tag{2}$$

Let R be a complete residue system of $\mathfrak{o}$, modulo $\mathfrak{p}^d$. Let ρ be the canonical map of $\mathfrak{o}/\mathfrak{p}^d$ onto R. If t is any function in $\mathfrak{R}_n$, then

$$T(X) = \sum_{(a_1, a_2 \cdots, a_n) \in \mathfrak{B}_n} \rho[t(a_i, a_2, \cdots, a_n)]\, W(x_1 - a_1, x_2 - a_2, \cdots, x_n - a_n) \tag{3}$$

is a polynomial over $\mathfrak{o}$ which represents the function t. Thus every function in $\mathfrak{R}_n$ may be considered to arise from a polynomial.

A polynomial over $\mathfrak{o}$ which represents a function in $\mathfrak{R}_n$ will be said to be *reduced* if there does not exist a polynomial over $\mathfrak{o}$ of lower degree which represents the same function of $\mathfrak{R}_n$. It was shown in [5] that a polynomial S(X) over $\mathfrak{o}$ may be expressed uniquely in the form

$$S(X) = \sum_{s \geq 0} \sum_{\sigma(s)} \sum_{j \geq 0} \pi^j P_{j,s,\sigma(s)}(X) \Lambda_s^{\sigma(s)}(X),$$

where $\sigma(s)$ ranges over certain partitions of s into n nonnegative integers, where the $P_{j,s,\sigma(s)}(X)$ are polynomials over $\mathfrak{o}$ such that the degree of each x_i in each $P_{j,s,\sigma(s)}$ is less than q and the nonzero coefficients of the $P_{j,s,\sigma(s)}$ are not in $\mathfrak{p}$, and where the $\Lambda_s^{\sigma(s)}$ are polynomials over $\mathfrak{o}$ such that the functions represented by them map $\mathfrak{o}^{(n)}$ into $\mathfrak{p}^s$. ($\mathfrak{o}^{(n)}$ denotes the Cartesian product of $\mathfrak{o}$ by itself n times.)

If S represents a function in $\mathfrak{R}_n$, then the polynomial

$$S^*(X) = \sum_{j+s<d} \sum_{\sigma(s)} \pi^j P_{j,s,(s)}(X) \Lambda_s^{\sigma(s)}(X) \tag{4}$$

represents the same function of $\mathfrak{R}_n$. If the polynomials S* and

$$U(X) = \sum_{j+s<d} \sum_{\sigma(s)} \pi^j Q_{j,s,\sigma(s)}(X) \Lambda_s^{\sigma(s)}(X)$$

represent the same function of $\mathfrak{R}_n$, then

$$S^* - U = \sum_{j+s<d} \sum_{\sigma(s)} [P_{j,s,\sigma(s)} - Q_{j,s,\sigma(s)}]\, \pi^j \Lambda_s^{\sigma(s)}$$

is in $\mathfrak{B}_d$, where $\mathfrak{B}_d$ denotes the set of polynomials over $\mathfrak{o}$ which, as functions, map $\mathfrak{o}^{(n)}$ into $\mathfrak{p}^d$. Theorem III of [5] implies that each of the polynomials

$$P_{j,s,\sigma(s)} - Q_{j,s,\sigma(s)}$$

is the zero polynomial; hence U = S*. It follows that the reduced polynomials are of the form (4), and that each polynomial which represents a function of $\mathfrak{R}_n$ is associated with a unique reduced form.

Suppose that the polynomial S^* given in (4) represents a function of $\mathfrak{R}_n$. Suppose that $M(X)$ is a polynomial over $\mathfrak{o}$ such that $\pi^{-e} M(X)$ represents that same function of $\mathfrak{R}_n$. Then the polynomial $M(X) - \pi^e S^*(X) = L(X)$ is in $\mathfrak{B}_{d+e}$; that is,

$$L(X) = \sum_{j+s \geq d+e} \sum_{\sigma(s)} \pi^j P_{j,s,\sigma(s)}(X) \Lambda_s^{\sigma(s)}(X).$$

It follows that the degree of $M(X)$ can not be smaller than the degree of $S^*(X)$.

Since $G(x)$ is a monic polynomial of degree $(q - 1)d$, it follows that when $d < q$, then $G(x)$ can be expressed as in (4) and therefore $G(x)$ is reduced. This can also be seen by the following argument. If $U(x)$ and $G(x)$ represent the same function in $\mathfrak{R}_1$, then $U - G = C$ is in $\mathfrak{B}_d$; it follows from Theorem II of [5] that if $d < q$, then either the degree of C is at least dq, or all of the coefficients of C are in $\mathfrak{p}$. In either case, the degree of U cannot be less than the degree of G.

However, it is not likely that $W(X)$ is reduced. Suppose that W^* is the reduced polynomial which represents the same function of $\mathfrak{R}_n$ as does W; then (3) remains valid if W is replaced by W^*. Consequently, the degree of W^* can not be smaller than that of any other reduced polynomial. When $d < q$, the polynomial $\pi^{d-1}\Pi_{i=1}^n x_i^{q-1}$ is reduced. Hence the degree of W^* cannot be smaller than $(q - 1)n$.

Define $\psi_0(x) = 1$; and inductively for $m \geq 1$, define

$$\psi_m(x) = 1 + x \sum_{j=0}^{m-1} (m - j)\psi_j(x).$$

Let $a_j = d\psi_j(q - 1)$, and set

$$E(x) = \prod_{j=0}^{d-1} H^{a_j}(\pi^{j+1-d} x). \tag{5}$$

Let $d = k + r + 1$. As a function from $\mathfrak{o}$ to $\mathfrak{o}$, E maps $\mathfrak{p}^k$ $(0 \leq k < d)$ into $\mathfrak{p}^z$, where

$$z = a_r + (q - 1)\sum_{j=0}^{r-1} (j - r)a_j = d\left[\psi_r(q - 1) - (q - 1)\sum_{j=0}^{r-1} (r - j)\psi_j(q - 1)\right] = d.$$

Clearly, E maps $\mathfrak{p}^d$ into $1 + \mathfrak{p}^d$. Thus we have

$$E(a) \equiv \begin{cases} 1 \pmod{\mathfrak{p}^d} & \text{if } a \equiv 0 \pmod{\mathfrak{p}^d}, \\ 0 \pmod{\mathfrak{p}^d} & \text{if } a \not\equiv 0 \pmod{\mathfrak{p}^d}, \end{cases} \tag{6}$$

and the degree of E is $(q - 1)d \sum_{j=0}^{d-1} \psi_j(q - 1)$.

If $F(X)$ is strongly definite over $\mathfrak{o}$, the polynomials $W(X)$ and $E[F(X)]$ represent the same function of $\mathfrak{R}_n$. Thus the degree of $E[F(X)]$ must be as large as the degree of W^*. We have

$$d^2(q-1)\sum_{j=0}^{d-1}\psi_j(q-1) \geq n(q-1).$$

Let $\phi_d(y) = \sum_{j=0}^{d-1}\psi_j(y)$; then $d^2\phi_d(q-1) \geq n$, and the theorem is proved.

REMARKS

1. We give two examples of strongly definite polynomials over $\mathfrak{o}$.

(a) If k is the field of degree d over $\mathfrak{o}/\mathfrak{p}$, the norm function N from k to $\mathfrak{o}/\mathfrak{p}$ may be considered to be a homogeneous, definite polynomial over $\mathfrak{o}/\mathfrak{p}$ of degree d in d indeterminates. Let σ be the homomorphic map of $\mathfrak{o}[X]$ onto $\mathfrak{o}/\mathfrak{p}[X]$ which agrees with the natural map of $\mathfrak{o}$ onto $\mathfrak{o}/\mathfrak{p}$ and which leaves the x_i invariant. If $G(X)$ is in $\mathfrak{o}[X]$ and if the image of G under σ is N, then G satisfies the following condition:

(7) $\qquad G(a_1, a_2, \cdots, a_d) \equiv 0 \pmod{\mathfrak{p}}$ if and only if each $a_i \equiv 0 \pmod{\mathfrak{p}}$.

Let $G_1, G_2, \cdots, G_d$ be polynomials over $\mathfrak{o}$ satisfying (7); then the polynomial

$$F(X) = G_1(x_{11}, x_{12}, \cdots, x_{1d}) + \pi G_2(x_{21}, x_{22}, \cdots, x_{2d}) + \cdots + \pi^{d-1}G_d(x_{d1}, x_{d2}, \cdots, x_{dd})$$

is a strongly definite polynomial over $\mathfrak{o}$.

(b) If $\mathfrak{o}$ is the ring of 3-adic integers and

$$G(X) = 2y_1^4 + y_2^4 + y_3^4 + y_1^2y_2^2 + y_1^2y_3^2 + y_2^2y_3^2 + 6y_1y_2y_5 + 3(y_4^2 + y_4y_5 + 2y_5^2)^2,$$

then the polynomial $F(X) = G(x_1, x_2, \cdots, x_5) + 9G(x_6, x_7, \cdots, x_{10})$ is strongly definite over $\mathfrak{o}$.

2. If $d \geq q$, there exist polynomials which satisfy (6); however, their degree is much larger in comparison with the case above. It is for this reason that we restricted our attention to the case $d < q$.

3. The polynomials satisfying (6) are exactly those polynomials which are necessary for showing that every continuous function from $\mathfrak{o}$ to $\mathfrak{o}$ can be approximated by a polynomial over K.

4. If $A(X)$ is a polynomial over K, the content $c(A)$ of $A(X)$ is the largest power of π dividing every coefficient of $A(X)$. Determine rational integers b_i such that

$$c(E) + d = \sum_{i=1}^{m} b_i(q^i - 1)/(q-1) \qquad (b_m \neq 0,\ 0 \leq b_i \leq q).$$

Results in [5] show that there exists a polynomial over K which satisfies (6) and has degree $\Sigma_{i=1}^m b_i q^i$. Also, $\Pi_{i=1}^n x_i^{q-1}\Lambda_{d-1}(x_1)$ is a reduced polynomial of degree $(q-1)n + (d-1)q$, and we have a larger bound on the degree of W^* than the one used in the proof. Thus to some extent the bound on n could be decreased. However, even this last bound appears to be excessively large, and we have not tried for the best possible result in this direction.

5. Let $\mathfrak{S}$ be the set of all functions from $\mathfrak{o}/\mathfrak{p}^d$ to $\mathfrak{o}/\mathfrak{p}^d$; then E(x) represents the basic idempotent in $\mathfrak{S}$. If f is in $\mathfrak{S}$, then

$$F(x) = \sum_{a \in \mathfrak{o}/\mathfrak{p}^d} \rho[f(a)]E(x - a)$$

is a polynomial over $\mathfrak{o}$ representing the function f. Many of the results obtained in [6] follow as a consequence of this last fact, as do the structure theorems for $\mathfrak{S}$.

REFERENCES

1. R. Brauer, *A note on systems of homogeneous algebraic equations*, Bull. Amer. Math. Soc. 51. (1945), 749-755.
2. C. Chevalley, *Démonstration d'une hypothèse de M. Artin*, Abh. Math. Sem. Univ. Hamburg 11 (1936), 73-75.
3. H. Hasse, *Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper*, J. Reine Angew. Math. 153 (1924), 113-130.
4. D. J. Lewis, *Cubic homogeneous polynomials over $\mathfrak{p}$-adic number fields*, Ann. of Math. (2) 56 (1952), 473-478.
5. ———, *Ideals and polynomial functions*, Amer. J. Math. 78 (1956), 71-77.
6. L. Rédei and T. Szele, *Algebraisch-zahlentheoretische Betrachtungen über Ringe. I.*, Acta Math. 79 (1947), 291-320.

University of Notre Dame