SUMS OF n-TH POWERS IN FIELDS OF PRIME CHARACTERISTIC

By Leonard Tornheim

A consequence of Waring's theorem on the representation of integers as sums of n-th powers is that every positive rational number is expressible as a finite number of n-th powers, the number required being less than a constant depending upon n. In the present paper we obtain similar theorems for fields of prime characteristic. The results tell which quantities are expressible as sums of n-th powers and how many n-th powers are needed.

Let F be a field of characteristic p, G the multiplicative group of non-zero elements, H the subgroup of all n-th powers, L the set of all elements expressible as sums of n-th powers, and K the set of all non-zero elements of L. We first prove

Lemma 1. *The set L is a field.*

Evidently L is closed under addition and multiplication. If $x = \sum_{i=1}^{r} x_i^n \neq 0$, then $-x = x + \cdots + x = (p - 1)x$ and $1/x = [(1/x)^n]x^{n-1}$. Thus L is a subfield of F and K is a subgroup of G containing H.

An example of a field for which $K \neq G$ is the finite field of four elements and $n = 3$. Here K has only the element 1.

Theorem 1. *Let F be a finite field. Every quantity in F which is expressible as a sum of n-th powers is a sum of n n-th powers.*

Let K_r be the set of all non-zero elements that are sums of r n-th powers; e.g., $H = K_1$. There exists a first subscript t for which $K_t = K$, $K_{t-1} < K$. Let $x = \sum_{i=1}^{t} x_i^n$ be in K_t, but not in K_{t-1}. Then $x' = \sum_{i=1}^{t-1} x_i^n$ is in K_{t-1} but not in K_{t-2}; otherwise $x = x' + x_t^n$ would be in K_{t-1}. Hence $K_{t-2} < K_{t-1}$. The argument is repeated for each $x^{(s)} = \sum_{i=1}^{t-s} x_i^n$ $(s = 2, \cdots, t - 1)$ to prove that $K_1 < K_2 < \cdots < K_t$.

If an element $y = \sum_{i=1}^{r} y_i^n$ is in K_r, the coset determined by y is in K_r, since every element of the coset has the form $z^n y = \sum_{i=1}^{r} (zy_i)^n$. It follows that each K_r, containing an element not in K_{r-1}, contains a coset not in K_{r-1}. Hence $t \leqq d$, where d is the index of H in K. Since $K = K_t$, every element expressible as a sum of n-th powers is a sum of $t \leqq d$ n-th powers.

It remains to prove that $d \leqq n$. Denote the index of H in G by m; then $d \leqq m$, since $K \leqq G$. The index m is equal to the number of distinct quantities

Received December 13, 1937.