ON $\mathfrak{p}$-ADIC FORMS

B. J. Birch and D. J. Lewis

In a recent paper [1], concerned with homogeneous equations in a $\mathfrak{p}$-adic field, we had difficulty in proving a crucial result (Lemma B, quoted below) on the normalization of homogeneous forms with $\mathfrak{p}$-adic coefficients. In this note, using on the way an invariant introduced by Davenport [3], we prove a sharper result more simply. We shall have to describe several methods of reduction of such forms.

Let $f = f(X) = f(x_1, \cdots, x_n)$ be a form of degree d over a field k, say

(1) $$f(x_1, \cdots, x_n) = \sum_1^n a_{j_1,\cdots,j_d} x_{j_1} \cdots x_{j_d},$$

where the a's are symmetric in $j_1, \cdots, j_d$. (It is perfectly easy to carry out our arguments with a linear system of forms rather than with a single form f, if in the definition of equivalent linear systems, the λ of (3) is taken to be a non-singular matrix. However, when one studies problems concerning the solubility of simultaneous equations over a $\mathfrak{p}$-adic field in more detail (see [2]), it becomes clear that this would be downright misleading.) Write A for the n-by-n^{d-1} matrix $(a_{j_1,\cdots,j_{d-1},J})$ whose rows correspond to $J = 1, \cdots, n$ and whose columns correspond to the $(d-1)$-tuples $(j_1, \cdots, j_{d-1})$. If $X \to TX$ is a linear transformation, we write $f_T(X)$. As in our earlier paper, we write $\gamma(f)$ for the number of variables that occur in monomials of f with non-zero coefficient, and define the order $o(f)$ of f by

(2) $$o(f) = \min_T \gamma(f_T),$$

where the minimum is taken over all non-singular linear transformations T defined over k. A form is called *degenerate* if its order is less than n. As Davenport observed: *A form* f *is degenerate if and only if all* n-by-n *minors of* A *vanish.*

Suppose now that k is a $\mathfrak{p}$-adic field with ring of integers $\mathfrak{o}$, local prime π, prime ideal $\mathfrak{p} = \pi\mathfrak{o}$, and residue class field $k^* = \mathfrak{o}/\mathfrak{p}$. (In all our applications, k^* is finite; however such an assumption is not necessary here.) If a is in $\mathfrak{o}$, denote its canonical image in k^* by a^*. This homomorphism can be extended to a homomorphism of $\mathfrak{o}[X]$ onto $k^*[X]$; thus if f is a polynomial with integer coefficients, then f^* denotes the residue class of f modulo $\mathfrak{p}$. Let $\nu(f)$ denote the greatest power of $\mathfrak{p}$ dividing every coefficient of f.

Two forms f and g are called *equivalent* if there exists a non-singular linear transformation T and a non-zero element λ in k such that

(3) $$f_T = \lambda g$$

(T being defined over k). For example, every form f is equivalent to one with $\nu(g) = 0$.

Received July 11, 1961.