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

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

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

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

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

$$f_T = \lambda g \tag{3}$$

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

Received July 11, 1961.

Our original Lemma B: *Every form* f *over* k *of degree* d *and order* n *is equivalent to a form* g *over* $\mathfrak{o}$ *with* $o(g^*) \geq n/d$.

If $\nu(f) \geq 0$, that is, if all the coefficients a are integers, define $\Delta(f)$ to be the greatest common divisor of all n-by-n minors of A if f is non-degenerate, and to be 0 otherwise. Using the same arguments as in [3; see Lemma 2.1 and its Corollary], one easily shows that $\Delta(f)$ is invariant under integral unimodular transformations of the variables.

A form f is called Δ-*reduced* if it is non-degenerate with integral coefficients and $\nu(\Delta(f)) \leq \nu(\Delta(g))$ for all integral forms g equivalent to f. When f is a non-degenerate integral form, $\nu(\Delta(f))$ is a nonnegative integer. It follows that *every non-degenerate form is equivalent to a* Δ-*reduced form.* Note that if f is Δ-reduced and T is integral and unimodular, then $\nu(f) = \nu(f_T) = 0$ and f_T also is Δ-reduced.

Now for a second definition of reduction: Given any assignment of the variables $x_1, \cdots, x_n$ into disjoint batches $B_0, B_1, \cdots$, we can, for a given form g, define a sequence of forms ${}^{(0)}g = g, {}^{(1)}g, {}^{(2)}g, \cdots$ by the relation

$$(4) \qquad {}^{(h)}g = {}^{(h)}g(x_1, \cdots, x_n) = \pi^{-h} g(\pi^{\gamma_{n1}} x_1, \cdots, \pi^{\gamma_{hn}} x_n),$$

where γ_{hr} is 1 if x_r is in $B_0 \cup B_1 \cup \cdots \cup B_{h-1}$ and is 0 otherwise. The ${}^{(h)}g$ depend both on g and on the batching, but all these forms consist of the same power-products of the variables as g, with various powers of π put into or taken out of the coefficients. We shall write β_h for the number of variables in B_h.

A form g of degree d is *weakly reduced* if the variables $x_1, \cdots, x_n$ have been assigned to d disjoint batches $B_0, B_1, \cdots, B_{d-1}$ in such a way that (i) each ${}^{(h)}g$, for $h = 0, 1, \cdots, d-1$, has integral coefficients; (ii) every variable of B_h occurs in ${}^{(h)}g^*$; (iii) no variable of B_h can be eliminated from ${}^{(h)}g^*$ by a non-singular transformation U*, defined over k*, of the type

$$(5) \qquad U^* = U_0^* \otimes U_1^* \otimes \cdots \otimes U_{d-1}^* \quad \text{with } U_i^* = I_i \text{ for } i \neq h,$$

the partitioning of U* being determined by the batching, and I_i being the β_i-by-β_i unit matrix. As usual, $C = A \otimes B$ if $C = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$.

Note that a non-singular linear transformation over k* is always the image of an integral unimodular transformation over k. In particular, U* may be regarded as the image of

$$(6) \qquad U = I_0 \otimes I_1 \otimes \cdots \otimes U_h \otimes I_{h+1} \otimes \cdots \otimes I_{d-1},$$

where U_h is integral and unimodular. It should also be noted that the definition of weak reduction is relative to a particular batching.

When g is weakly reduced, it is convenient to define ${}^{(h)}g$ and B_h for $h \geq d$ by ${}^{(h)}g = {}^{(h-d)}g$ and $B_h = B_{h-d}$; for $h = d$, this definition of ${}^{(d)}g$ is consistent with (4). It is easily seen that if g is weakly reduced, so is ${}^{(h)}g$ $(h \geq 0)$ with

$$B_j({}^{(h)}g) = B_{j+h}(g).$$

If g is weakly reduced, then

$$\sum_{h=0}^{d-1} \beta_h = n, \tag{7}$$

and we assert that

$$o(^{(h)}g^*) \geq \beta_h \quad \text{for } h = 0, 1, \cdots, d-1. \tag{8}$$

To prove (8), suppose it is false for some h; then

$$^{(h)}g^* = q^*(L_1^*, L_2^*, \cdots, L_t^*),$$

where $L_1^*, \cdots, L_t^*$ are independent linear forms over k^*, $t < \beta_h$, and q^* is a form over k^*. Write $L_i^* = M_i^* + N_i^*$, where M_i^* consists of those monomials of L_i^* which contain a variable of B_h; say

$$M_i^* = \sum_j \lambda_{ij}^* \cdot x_j \qquad (i = 1, \cdots, t).$$

Now rank $(\lambda_{ij}^*) \leq t < \beta_h$, so that there exist non-trivial solutions μ_r^* in k of the system

$$\sum_{r=1}^{\beta_h} \mu_r^* \lambda_{jr}^* = 0 \qquad (j = 1, 2, \cdots, t).$$

Suppose that $\mu_1^* \neq 0$; then for the linear transformation U^* with

$$U_h^* = \begin{pmatrix} \mu_1^* & 0 & \cdots & 0 & 0 \\ \mu_2^* & 1 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & 0 & & 1 & 0 \\ \mu_{\beta_h} & 0 & \cdots & 0 & 1 \end{pmatrix},$$

the expression $[\,^{(h)}g(UX)\,]^* \cdot$ does not contain the variable x_1 of B_h; this contradicts (iii).

PROPOSITION. *If* f *is* Δ*-reduced, there exists an integral unimodular transformation* V *such that* f_V *is weakly reduced relative to a particular batching of the variables.*

Proof. The variables of any Δ-reduced form f may be batched to satisfy (i) and (ii) in a straightforward manner, as follows. Take B_0 as all variables occurring in f^*; then, for $1 \leq h \leq d-1$, take B_h as all variables occurring in $^{(h)}f^*$ which have not already been assigned to an earlier batch. (Note that the definition of $^{(h)}f$ in (4) depends only on $B_0, \cdots, B_{h-1}$.) It is easily seen that, for each $h \leq d$, $^{(h)}f$ has integral coefficients. For a monomial in f could only occur in $^{(h)}f$ with a non-integral coefficient if all its variables were in $B_0, \cdots, B_{h-2}$; such a monomial is multiplied by π^{d-h} in $^{(h)}f$, and therefore it occurs with an integral coefficient. Hence the above process of batching is meaningful, and (i) is satisfied. (At this stage we have used only the fact that f has integral coefficients.) Observe that if f is Δ-reduced, then

for each variable x_j there exists a monomial M of f such that the power of x_j in M exceeds $\nu(M)$; for otherwise the form

$$g(X) = f(x_1, \cdots, x_{j-1}, \pi^{-1}x_j, x_{j+1}, \cdots, x_n)$$

would be an integral form with $\nu(\triangle(g)) < \nu(\triangle(f))$. Hence each variable occurs in some B_h; for if x_j does not occur, then the corresponding monomial of ${}^{(d)}f$ does not have integral coefficients—a contradiction.

Now choose an integral unimodular transformation V such that, relative to the process of batching just described, the integers $\beta_0(f_V), \beta_1(f_V), \cdots, \beta_{d-2}(f_V)$ are successively as small as possible. Set $g = f_V$. If a variable of $B_h(g)$ could be eliminated from ${}^{(h)}g^*$ by a non-singular transformation U* of type (5), then $B_0, \cdots, B_{h-1}$ would be the same for g_U as for g, so that

$$\beta_j(g_U) = \beta_j(g) \qquad \text{for } j = 0, 1, \cdots, h-1,$$

while

$$\beta_h(g_U) < \beta_h(g),$$

where U is as in (6). This contradicts the choice of V. Hence (iii) is satisfied for g.

COROLLARY. *Every non-degenerate form is equivalent to a weakly reduced form.*

In view of (7) and (8), our original Lemma B is now an immediate consequence of the Corollary, since there exists some h such that $\beta({}^{(h)}f) \geq n/d$, whence $o({}^{(h)}g^*) \geq n/d$. Once Lemma B or its equivalent has been proved, one can easily obtain a bit more. A weakly reduced form f is called *strongly reduced* if

$$\sum_{h=0}^{d-1} h\beta_h(f) \leq \sum_{h=0}^{d-1} h\beta_h(g) \tag{9}$$

whenever g is weakly reduced and equivalent to f.

If f is weakly reduced, then so are the ${}^{(h)}f$, with $B_s({}^{(h)}f) = B_{s+h}(f)$. Hence by (9), if f is strongly reduced, then

$$\sum_{h=0}^{d-1} h\beta_h(f) \leq \sum_{h=0}^{d-1} h\beta_h({}^{(s)}f) \leq \sum_{h=0}^{d-1} h\beta_{h+s}(f) \qquad (s = 0, 1, \cdots, d-1).$$

Using (7), we obtain the following sharpened version of the original lemma:

LEMMA B'. *Every form of degree* d *and order* n *is equivalent to a weakly reduced form* f *for which*

$$d\sum_{h=0}^{H-1} \beta_h(f) \geq Hn \qquad \textit{for } H = 1, 2, \cdots, d.$$

REFERENCES

1. B. J. Birch and D. J. Lewis, *p-adic forms*, J. Indian Math. Soc. 23 (1959), 11-32.
2. B. J. Birch, D. J. Lewis and T. G. Murphy, *Simultaneous quadratic forms* (to appear).
3. H. Davenport, *Cubic forms in thirty-two variables*, Philos. Trans. Roy. Soc. London. Ser. A 251 (1959), 193-232.

Churchill College, Cambridge
and
The University of Michigan