On a Theorem of Ax

Nicholas M. Katz

American Journal of Mathematics, Vol. 93, No. 2. (Apr., 1971), pp. 485-499.

Stable URL:
http://links.jstor.org/sici?sici=0002-9327%28197104%2993%3A2%3C485%3AOATOA%3E2.0.CO%3B2-W

American Journal of Mathematics is currently published by The Johns Hopkins University Press.

ON A THEOREM OF AX.

By NICHOLAS M. KATZ.

0. Introduction.

0.0. Let k be a finite field of characteristic p, having $q = p^a$ elements. We will be concerned with estimating the number of simultaneous zeroes of a collection of polynomials in several variables over k, when the number of variables is suitably large compared to the degrees of the polynomials.

In order to formulate our result, it is convenient to introduce some notations. For any non-empty finite set S, let $k[S]$ denote the polynomial ring on variables indexed by S, and put $\boldsymbol{A}^S = \mathrm{Spec}(k[S])$. Consider a family of non-constant polynomials f_i in $k[S]$ indexed by a second non-empty finite set T, i.e., a mapping

$$f: T \to \text{the set of non-constant elements of } k[S]$$
$$i \in T \to f_i \in k[S].$$

We put $d_i = \text{degree}\,(f_i)$.

To such a family of polynomials, or, as we shall say, to a triple (S, T, f) as above, we attach

0.1. the closed subscheme $V(S, T, f)$ of $\boldsymbol{A}^S$ defined by the annullation of the f_i, $i \in T$.

0.2. the integer $N(S, T, f)$, defined as the number of points of $V(S, T, f)$ with values in k.

0.3. the integer $\mu(S, T, f)$, defined as the least non-negative integer which is $\geqq$

$$\frac{\mathrm{Card}(S) - \Sigma_{i \in T} d_i}{\sup_{i \in T}(d_i)}.$$

The purpose of this paper is to prove

THEOREM 1.0. $N(S, T, f) \equiv 0 \text{ modulo } q^{\mu(S,T,f)}$.

The idea of obtaining a p-adic congruence for $N(S, T, f)$ is due to

Received March 9, 1970.

Warning [10], who proved that if $\mu(S,T,f) > 0$, i.e., if $\mathrm{Card}(S) > \Sigma_{i\in T} d_i$, then

$$N(S,T,f) \equiv 0 \text{ modulo } p$$

Warning also obtained a striking (and best possible) archimedean lower bound for $N(S,T,f)$: if $N(S,T,f) \geqq 1$, then

$$N(S,T,f) \geqq q^{\mathrm{Card}(S)-\Sigma d_i}.$$

Ax [1] proved 1.0 for hypersurfaces (i.e. $\mathrm{Card}(T) = 1$). As a corollary, he obtained the following congruence in the general case:

Let $\lambda(S,T,f)$ be the least non-negative integer which is $\geqq$

$$\frac{\mathrm{Card}(S) - \Sigma_{i\in T} d_i}{\Sigma_{i\in T} d_i}.$$

Then $N(S,T,f) \equiv 0$ modulo $q^{\lambda(S,T,f)}$.

The possibility of replacing $\lambda(S,T,f)$ by $\mu(S,T,f)$ was suggested by Deligne's calculation [2] of the "Hodge level" of a projective smooth complete intersection. As an application of 1.0, we give below (cf. 2.8) a connection between the Hodge level and the p-adic divisibility properties of the proper values of Frobenius operating on the l-adic etale cohomology of such a variety [cf. also [7], pp. 164-170].

The body of the paper is devoted to the proof of 1.0. The proof is based entirely on Dwork's p-adic theory of the zeta function, via certain completely continuous endomorphisms of (infinite-dimensional) p-adic Banach spaces (cf. [3] and [9]). It depends upon giving suitable bounds on the (operator) norms of these endomorphisms.

The paper concludes by showing that 1.0 is best possible in a suitable sense. The method is to reduce to the case of hypersurfaces, where the result is due to Ax [1].

2. Applications to complete intersections.

2.0. Let X be any scheme of finite type over k. By the degree of a closed point $\mathfrak{p}$ of X, written $\deg(\mathfrak{p})$, we mean the degree of its residue field $k(\mathfrak{p})/k$. The zeta function of X/k may be defined as an element of $\mathbf{Z}[[t]]$ by the formula

$$Z(t, X/k) = \prod_{\mathfrak{p}} (1 - t^{\deg(\mathfrak{p})})^{-1}.$$

Fixing an algebraic closure $\bar{k}$ of k, we denote by k_s the unique extension of k in $\bar{k}$ of degree s. An elementary calculation then shows that, denoting by $'$ the operation of differentiation with respect to t, one has

$$\frac{Z'(t, X/k)}{Z(t, X/k)} = \sum_{s \geqq 1} \mathrm{Card}(X(k_s))\, t^{s-1}.$$

By [3], the zeta function is a rational function, to which applies Fatou's theorem [5]:

THEOREM 2.1. *If the power series around zero of a rational function lies in* $1 + t\mathbf{Z}[[t]]$, *then every one of its zeroes and poles is the reciprocal of an algebraic integer.*

We recall from [1] the following proposition:

PROPOSITION 2.2. *Let* X *be a scheme of finite type over* k, *and* μ *a positive integer. The following statements are equivalent:*

2.2.1. *The reciprocal of every zero and pole of* $Z(t, X/k)$ *is of the form* q^{μ} (*an algebraic integer*).

2.2.2. *For each integer* $s \geqq 1$, *one has* $\mathrm{Card}(X(k_s)) \equiv 0$ modulo $q^{s\mu}$.

2.2.3. $Z(t, X/k) \in Z[[q^{\mu}t]]$.

Thus 1.0 may be restated:

THEOREM 1.0 *bis*. *The reciprocal of every zero and pole of*

$$Z(t, V(S, T, f)/k)$$

is of the form

$$q^{\mu(S,T,f)} \quad (\textit{an algebraic integer}).$$

2.3. We now recall the connection of the zeta function to the l-adic étale cohomology. We denote by $\bar{X}$ the $\bar{k}$ scheme $X_{xk}\bar{k}$ deduced from X by extension of scalars, and, for each prime number $l \neq p$, we denote by $H^i{}_c(\bar{X}, Q_l)$ the l-adic cohomology groups, with compact supports, of $\bar{X}$. These are finite-dimensional Q_l-vector spaces on which the galois group $\mathrm{Gal}(\bar{k}/k)$ operates. Let $\mathfrak{F}$ denote the inverse of the canonical generator $(x \to x^q)$ of $\mathrm{Gal}(\bar{k}/k)$; one has the fundamental relation [6]

$$2.3.1 \qquad Z(t, X/k) = \prod_{i \geqq 0} [\det(1 - t\mathfrak{F} \mid H^i{}_c(\bar{X}, Q_l))]^{(-1)^{i+1}}.$$

Suppose now that X/k is a projective and smooth complete intersection of dimension n. We denote by

$$\mathrm{Prim}^n(\bar{X}, Q_l)$$

the primitive (in the sense of Hodge-Lefschetz theory, cf. [2]) subspace of $H_c{}^n(\bar{X}, Q_l)$ (the subscript "c" is now superfluous, as $\bar{X}/\bar{k}$ is proper). Using

the known cohomological structure of projective smooth complete intersections, (2.3.1) may be simplified to give

$$2.3.2 \qquad \{Z(t, X/k) \prod_{i=0}^{n} (1 - q^i t)\}^{(-1)^{n+1}} = \det(1 - t\mathfrak{F} \mid \mathrm{Prim}^n(\bar{X}, Q_l)).$$

(This shows, incidentally, that the proper values of $\mathfrak{F}$ acting on $\mathrm{Prim}^n(\bar{X}, Q_l)$ are algebraic integers which are independent of the choice of the prime number $l \neq p$. Needless to say, this independence of choice of l in general is an open problem.)

Combining 2.3.2 with 2.1 and 2.2, we find

PROPOSITION 2.4. *Let $X \hookrightarrow \boldsymbol{P}^N$ be a projective and smooth complete intersection of dimension n, $X_{aff} \hookrightarrow \boldsymbol{A}^{N+1}$ its affine cone, and μ an integer, $0 \leqq \mu \leqq n$. The following statements are equivalent.*

2.4.1. *For every prime $l \neq p$, every proper value of $\mathfrak{F}$ acting on $\mathrm{Prim}^n(\bar{X}, Q_l)$ is of the form*

$$q^\mu \text{ (an algebraic integer)}.$$

$$2.4.2. \qquad Z(t, X/k) \prod_{i=0}^{n} (1 - q^i t) \in Z[[q^\mu t]].$$

2.4.3. *For every integer $s \geqq 1$,*

$$\mathrm{Card}(X(k_s)) \equiv \frac{1}{1 - q^s} \text{ modulo } q^{s\mu}$$

2.4.4. *For every integer $s \geqq 1$,*

$$\mathrm{Card}(X_{aff}(k_s)) \equiv 0 \text{ modulo } q^{s\mu}.$$

Consider now a triple (S, T, f) as in 0.0, which is *homogeneous*, in the sense that each of the polynomials f_i, $i \in T$, is homogeneous. Putting $\boldsymbol{P}(S) = \mathrm{Proj}(k[S])$, we denote by $X(S, T, f)$ the closed subscheme *of* $\boldsymbol{P}(S)$ defined by the annullation of the f_i, $i \in T$. Combining 1.0 and 2.4, we find

PROPOSITION 2.5. *Let (S, T, f) be a homogeneous triple such that $X(S, T, f)$ is a smooth complete intersection of dimension*

$$n = \mathrm{Card}(S) - \mathrm{Card}(T) - 1.$$

Then, for every prime $l \neq p$, every proper value of $\mathfrak{F}$ acting on

$$\mathrm{Prim}^n(\bar{X}(S, T, f), Q_l)$$

is of the form

$$q^{\mu(S,T,f)} \text{ (an algebraic integer)}.$$

2.5. We now explain the connection with Hodge cohomology. As before, let X/k be a projective and smooth complete intersection of dimension n. For each pair of positive integers (p, q) with $p+q=n$, we define integers

$$h^{p,q}(X) = \dim_k H^q(X, \Omega^p_{X/k}).$$

These integers depend *only* on the dimension of X and on its multidegree [2]. We also define integers

$$h_0^{p,q}(X) = h^{p,q}(X) - \delta_{p,q}, \quad \delta = \text{Kronecker's } \delta;$$

these are the dimensions of the primitive parts of the spaces $H^q(X, \Omega^p_{X/k})$. We now define the "primitive Hodge co-level" of X, $\nu(X)$, to be the least integer a such that $h_0^{a,n-a}(X) \neq 0$; if $h_0^{a,n-a}(X) = 0$ for every a, we put $\nu(X) = \infty$. Deligne [2] has proven:

PROPOSITION 2.7. *Let (S, T, f) be as in 2.5, and suppose that $\sup_{i \in T}(d_i) \geqq 2$ (so that $X(S, T, f)$ is not a linear subspace of $\boldsymbol{P}(S)$). Then*

$$\nu(X(S, T, f)) = \mu(S, T, f).$$

Combining 2.5 and 2.7 gives

THEOREM 2.8. *Let X/k be a projective and smooth complete intersection of dimension n. Then every proper value of $\mathfrak{F}$ acting on $\mathrm{Prim}^n(\bar{X}, Q_l)$ is of the form*

$$q^{\nu(X)} \text{ (an algebraic integer)}.$$

The theorem is vacuous in case X is a linear subspace of projective space, as $\mathrm{Prim}^n(\bar{X}, Q_l)$ is then reduced to zero.)

We conclude this section by formulating a conjecture generalizing 2.8, whose truth in the case of hypersurfaces (of degree prime to p) is due to Dwork [4, p. 286]. Recall that the p-Newton polygon of an element $\sum_{i \geqq 0} a_i t^i \in \boldsymbol{Z}[t]$ is the convex closure in $\boldsymbol{R} \times \boldsymbol{R}$ of the points $(i, \mathrm{ord}_p(a_i))$, $i = 0, 1, \cdots$.

CONJECTURE 2.9. *Let X/k be a projective and smooth complete intersection of dimension n. Then the Newton polygon of*

$$\det(1 - t\mathfrak{F} \mid \mathrm{Prim}^n(\bar{X}, Q_l))$$

is contained in (i.e. in the (x, y)-plane it lies above) the Newton polygon of

$$\prod_{a=0}^{n} (1-q^a t)^{h_0^{a,n-a}}.$$

3. The proof of 1.0.

3.0. We begin by noting that it suffices to prove 1.0 for homgeneous triples. Indeed, given a triple (S,T,f), in which, to fix ideas, $S=(1,\cdots,N)$ and $T=\{1,\cdots,r\}$, we introduce two homogeneous triples:

3.0.1. (S',T,f'), in which

$$S'=\{1,\cdots,N+1\}$$
$$f_i'=X_{N+1}^{d_i}f_i(X_1/X_{N+1},\cdots,X_N/X_{N+1}).$$

3.0.2. (S',T',f''), in which

$$T'=\{1,\cdots,r+1\}$$
$$f_i''=\begin{cases} f_i', & i=1,\cdots,r \\ X_{N+1}, & i=r+1. \end{cases}$$

Thus $V(S',T,f')$ is the affine cone of the projective closure of $V(S,T,f)$, and $V(S',T',f'')$ the part of $V(S',T,f')$ which is "at infinity." It follows that

$$(q-1)N(S,T,f)=N(S',T,f')-N(S',T',f''),$$

while clearly

$$\mu(S',T,f')\geqq\mu(S,T,f)$$
$$\mu(S',T',f'')\geqq\mu(S,T,f).$$

3.1. Henceforth, we consider only homogeneous triples (S,T,f). From such a triple we deduce, for each non-empty subset $A\subset S$ and each non-empty subset $B\subset T$, a homogeneous triple noted $(A,B,f_{A,B})$, whose definition is as follows: denote by $\rho(S,A)$ the homomorphism

$$\rho(S,A): k[S]\to k[A]$$

defined by

$$\rho(S,A)(x_j)=\begin{cases} x_j & \text{if } j\in A \\ 0 & \text{if not.} \end{cases}$$

The mapping $f_{A,B}$ is defined to be the composition

$$\begin{array}{ccccccc} B & \hookrightarrow & T & \xrightarrow{f} & k[S] & \xrightarrow{\rho(S,A)} & k[A] \\ & & & & & & \uparrow \\ & & & & & & f_{A,B} \end{array}$$

We remark that the formation of $f_{A,B}$ is transitive, i.e. that if

$$\phi \neq A' \subseteq A \subseteq S \text{ and } \phi \neq B' \subseteq B \subseteq T,$$

then the triple $(A', B', f_{A',B'})$ is the triple $(A', B', (f_{A,B})_{A',B'})$. We record for later use the elementary inequality

3.10. $$\mu(A, B, f_{A,B}) + \mathrm{Card}(S) - \mathrm{Card}(A) \geqq \mu(S, T, f)$$

3.2. We now "calculate" $N(S, T, f)$. Let us denote by $V^*(S, T, f)$ the open subset of $V(S, T, f)$ where the function $\prod_{i \in S} x_i$ is invertible, and by $N^*(S, T, f)$ the number of points of $V^*(S, T, f)$ with values in k. Clearly we have

3.2.1. $$N(S, T, f) = 1 + \sum_{\phi \neq A \subseteq S} N^*(A, T, f_{A,T}).$$

In order to calculate $N^*(A, T, f_{A,T})$, we introduce a field K of characteristic zero which contains the p'-th roots of unity, and we choose a non-trivial additive character

$$\chi : k^+ \to \mu_p(K).$$

The orthogonality relations

$$\sum_{x \in k} \chi(xy) = \begin{cases} q & y = 0 \\ 0 & y \neq 0 \end{cases}$$

imply the formula (in which a finite set appearing as an exponent "means" its cardinality)

3.2.2. $$q^T N^*(A, T, f_{A,T}) = \sum_{x \in (k^*)^A} \prod_{i \in T} [1 + \sum_{z_i \in k^*} \chi(z_i \rho(S, A)(f_i)(x))].$$

In order to simplify 3.2.2, we introduce, for each homogeneous triple (S, T, f), a quantity $\chi(S, T, f) \in K$, defined by

3.2.3. $$\chi(S, T, f) = \sum_{x \in (k^*)^S,\ z \in (k^*)^T} \chi(\sum_{i \in T} z_i f_i(x)).$$

Expanding the product in 3.2.2 and substituting, via 3.2.3, into 3.2.1, gives the formula

3.2.4. $$N(S, T, f) = 1 + \frac{q^S - 1}{q^T} + \frac{1}{q^T} \sum_{\phi \neq A \subseteq S,\ \phi \neq B \subseteq T} \chi(A, B, f_{A,B}).$$

3.4. We now turn to Dwork [3] to further study $\chi(S, T, f)$. Denote by:

3.4.1. ζ_p a primitive p'-th root of unity in an algebraic closure of Q_p.

3.4.2. K the unramified extension of $Q_p(\zeta_p)$ whose residue field is k.

3.4.2. $\mathfrak{O}_K$ the ring of integers of K.

3.4.4. $\tau \in \mathrm{Gal}(K/Q_p(\zeta_p))$ the Frobenius automorphism of K.

Let $\mathfrak{B}$ be the category whose objects are pairs

3.4.5. $$(L, \alpha)$$

where L is a K-Banach space, and α a completely continuous [9] endomorphism of L as $Q_p(\zeta_p)$-Banach space, which is τ^{-1} linear (i.e. for $b \in K$ and $\eta \in L$, $\alpha(b\eta) = \tau^{-1}(b)\alpha(\eta)$), and whose morphisms are K-linear continuous maps compatible with the given endomorphisms. Notice that the a'-th iterate α^a of α is a completely continuous endomorphism of L as a K-space, (recall that $a = \mathrm{degree}(k/\mathbf{F}_p) = \mathrm{degree}(K/Q_p(\zeta_p))$), whose *trace* verifies

3.4.6. $$|\operatorname{trace}(\alpha^a)| \leqq \|\alpha\|^a,$$

where $\| \ \|$ denote the operator norm of $Q_p(\zeta_p)$-linear endomorphisms of L.

Dwork [3] attaches to each homogeneous triple (S, T, f) an object $(L(S, T, f), \alpha(S, T, f))$ of $\mathfrak{B}$, in such a way that

3.4.7. $$\chi(S, T, f) = (q-1)^{S+T} \operatorname{trace}(\alpha(S, T, f)^a).$$

3.5. In order to complete the proof of 1.0, we will attach to each homogeneous triple (S, T, f) a second object $(D(S, T, f), \gamma(S, T, f))$ of $\mathfrak{B}$, such that

3.5.1. $$\|\gamma(S, T, f)\| \leqq |p^{T+\mu(S,T,f)}|$$

3.5.2. there is a finite filtration of $(L(S, T, f), \alpha(S, T, f))$ whose associated graded object is

$$(K, \tau^{-1}) \oplus \sum_{\phi \neq A \subseteq S,\ \phi \neq B \subseteq T} (D(A, B, f_{A,B}), \gamma(A, B, f_{A,B}))$$

Admitting for a moment 3.5.1 and 3.5.2, let us conclude the proof of 1.0. By 3.5.2, we have, for every pair of non-empty subsets A and B of S and T respectively,

3.5.3. $$\operatorname{trace}(\alpha(A, B, f_{A,B})^a) = 1 + \sum_{\phi \neq A' \subseteq A,\ \phi \neq B' \subseteq B} \operatorname{trace}(\gamma(A', B', f_{A',B'})^a).$$

Substituting 3.5.3 into 3.4.7, and using 3.2.4 gives, after an elementary calculation, the formula

3.5.4. $$N(S, T, f) = q^S + \sum_{\phi \neq A \subseteq S,\ \phi \neq B \subseteq T} (q-1)^{A+B} q^{S-A-B} \operatorname{trace}(\gamma(A, B, f_{A,B})^a)$$

We conclude the proof of 1.0 by noting the inequality

3.5.5. $$|q^{S-A-B}\operatorname{trace}(\gamma(A,B,f_{A,B})^a)| \leqq |q^{\mu(S,T,f)}|$$

which follows immediately from 3.4.6, 3.5.1, and 3.1.0.

3.6. We must now implement the program of 3.5, which will require going back to the definition of $(L(S,T,f),\alpha(S,T,f))$. To fix ideas, we suppose $S=\{1,\cdots,N\}$, $T=\{1,\cdots,r\}$.

3.6.0. Let π be a prime element of $\mathfrak{O}_K$ (so that $\operatorname{ord}_p(\pi)=1/p-1$) which is a zero of the power series in t

$$\sum_{n\geqq 0} p^{-n}t^{p^n}$$

(there are $p-1$ possible choices of such a π—we fix one).

3.6.1. Rather than directly define $L(S,T,f)$, we first define the $\mathfrak{O}_K$-module $\boldsymbol{L}(S,T,f)$ consisting of the elements η of $L(S,T,f)$ having $\|\eta\|\leqq 1$.

$\boldsymbol{L}(S,T,f)$ is that *subring* of $\mathfrak{O}_K[[\pi Z_1,\cdots,\pi Z_r,X_1,\cdots,X_N]]$ consisting of those series

3.6.2. $$\sum A_{U,V}\pi^{|U|}Z^UX^V$$

for each term of which

3.6.3. $$\begin{cases} A_{U,V}\in\mathfrak{O}_K \\ \sum_{i\in S} v_i = \sum_{i\in T} u_i d_i \\ |U| = \sum_{i\in T} u_i \end{cases}$$

$L(S,T,f)$ is obtained by putting

3.6.4. $$L(S,T,f)=\boldsymbol{L}(S,T,f)\otimes_{\mathfrak{O}_K} K$$

and endowing it with the unique structure of K-Banach space for which $\boldsymbol{L}(S,T,f)$ consists precisely of the elements η of $L(S,T,f)$ having $\|\eta\|\leqq 1$. We note that multiplication of power series makes $L(S,T,f)$ into a Banach algebra.

3.6.5. For each integer $\nu\geqq 0$, we define $\boldsymbol{L}^{(\nu)}(S,T,f)$ to be the free $\mathfrak{O}_K$-module having as basis all monomials

$$\pi^\nu Z^UX^V$$

verifying

$$\begin{cases} \sum_{i\in S} v_i = \sum_{i\in T} u_i d_i \\ \nu = \sum_{i\in T} u_i. \end{cases}$$

We note for later use the decomposition (of $\mathfrak{O}_K$-modules)

3.6.6. $$\boldsymbol{L}(S,T,f) = \prod_{\nu \geqq 0} \boldsymbol{L}^{(\nu)}(S,T,f).$$

We now turn to defining $\alpha(S,T,f)$, beginning with some preliminary definitions.

3.6.7. Let $F_1, \cdots, F_r \in \mathfrak{O}_K[X_1, \cdots, X_N]$ be the unique homogeneous polynomials of degrees $d_1, \cdots, d_r$, whose non-zero coefficients are all $q-1$-st roots of unity, and which reduce modulo (π) to $f_1, \cdots, f_r \in k[X_1, \cdots, X_N]$. We write each F_i as a sum of monomials

$$F_i = \sum A_V^{(i)} X^V.$$

We denote by $E(t)$ the Artin-Hasse exponential series

3.6.8. $$E(t) = \exp\Big(\sum_{n \geqq 0} p^{-n} t^{p^n}\Big)$$

which, as is well known, lies in $\boldsymbol{Z}_p[[t]]$. (The element π of 3.6.0 was chosen so that $E(\pi)$ is a primitive p-th root of unity.) We define

$$H(S,T,f) \in \boldsymbol{L}(S,T,f)$$

by setting

3.6.9. $$H(S,T,f) = \prod_{i=1}^{r} \prod_{V} E(\pi A_V^{(i)} Z_i X^V).$$

We next define a completely continuous endomorphism, ψ, of $L(S,T,f)$ by

3.6.10. $$\psi\Big(\sum A_{U,V} \pi^{|U|} Z^U X^V\Big) = \sum A_{pU,pV} \pi^{p|U|} Z^U X^V.$$

Notice that

3.6.11. $$\psi(\boldsymbol{L}(S,T,f) \subset \prod_{\nu \geqq 0} p^\nu \boldsymbol{L}^{(\nu)}(S,T,f).$$

Finally we introduce a τ^{-1}-linear automorphism, noted τ^{-1}, of $L(S,T,f)$, by setting

3.6.12. $$\tau^{-1}\Big(\sum A_{U,V} \pi^{|U|} Z^U X^V\Big) = \sum \tau^{-1}(A_{U,V} \pi^{|U|}) Z^U X^V.$$

We can now define $\alpha(S,T,f)$:

3.6.13. $$\alpha(S,T,f) = \tau^{-1} \circ \psi \circ H(S,T,f)$$

i.e. for $\eta \in L(S,T,f)$,

$$\alpha(S,T,f)(\eta) = \tau^{-1}(\psi(\eta \cdot H(S,T,f))).$$

Note that, as $H(S,T,f) \in \boldsymbol{L}(S,T,f)$, 3.6.11 gives

3.6.14. $$\alpha(S,T,f)\,(\boldsymbol{L}(S,T,f)) \subset \prod_{\nu\geqq 0} p^{\nu}\boldsymbol{L}^{(\nu)}(S,T,f).$$

3.7. We can now define $(D(S,T,f),\gamma(S,T,f))$.

3.7.0. Just as in 3.6.1, we first define the $\mathfrak{O}_K$-module $\boldsymbol{D}(S,T,f)$; it is the ideal of the ring $\boldsymbol{L}(S,T,f)$ consisting of those series

$$\sum A_{U,V}|U|Z^UX^V$$

in which

3.7.1. $A_{U,V}=0$ unless $u_i\geqq 1$, $i=1,\cdots,r$ *and* $v_i\geqq 1$, $i=1,\cdots,N$.

Then we put $D(S,T,f)=\boldsymbol{D}(S,T,f)\otimes_{\mathfrak{O}_K}K$, norming it so that $\boldsymbol{D}(S,T,f)$ consists precisely of the elements η of $D(S,T,f)$ having $\|\eta\|\leqq 1$.

3.7.2. Viewed as a subspace of $L(S,T,f)$, $D(S,T,f)$ is stable under $\alpha(S,T,f)$; we define $\gamma(S,T,f)$ to be the restriction of $\alpha(S,T,f)$ to $D(S,T,f)$.

For each integer $\nu\geqq 0$, we put

3.7.3. $$\boldsymbol{D}^{(\nu)}(S,T,f)=\boldsymbol{D}(S,T,f)\cap\boldsymbol{L}^{(\nu)}(S,T,f);$$

we have the decomposition (of $\mathfrak{O}_K$-modules)

3.7.4. $$\boldsymbol{D}(S,T,f)=\prod_{\nu\geqq 0}\boldsymbol{D}^{(\nu)}(S,T,f).$$

From 3.6.14 we find

3.7.5. $$\gamma(S,T,f)\,(\boldsymbol{D}(S,T,f)) \subset \prod_{\nu\geqq 0} p^{\nu}\boldsymbol{D}^{(\nu)}(S,T,f).$$

3.8. We can now prove

3.5.1. $$\|\gamma(S,T,f)\|\leqq |\,p^{T+\mu(S,T,f)}\,|.$$

Indeed, by 3.7.5, it suffices to prove

LEMMA 3.8.0. *If* $\nu<\mathrm{Card}(T)+\mu(S,T,f)$, *then*

$$\boldsymbol{D}^{(\nu)}(S,T,f)=0.$$

Proof. We must show that if $Z^UX^V\in D(S,T,f)$, *then*

$$\sum_{i\in T}u_i\geqq \mathrm{Card}(T)+\mu(S,T,f).$$

As $Z^UX^V\in D(S,T,f)$, we have

$$\begin{cases} u_i\geqq 1, & i\in T\\ v_i\geqq 1, & i\in S\\ \sum\limits_{i\in S}v_i=\sum\limits_{i\in T}u_id_i. \end{cases}$$

Thus we find

$$\begin{aligned}\mathrm{Card}(S) &\leqq \sum_{i\in S} v_i = \sum_{i\in T} u_i d_i \\ &= \sum_{i\in T} d_i + \sum_{i\in T} (u_i - 1) d_i \\ &\leqq \sum_{i\in T} d_i + \sup_{i\in T}(d_i) \sum_{i\in T} (u_i - 1) \\ &\leqq \sum_{i\in T} d_i + \sup_{i\in T}(d_i)\,[\sum_{i\in T} u_i - \mathrm{Card}(T)]\end{aligned}$$

whence

$$\sum_{i\in T} u_i \geqq \mathrm{Card}(T) + \frac{\mathrm{Card}(S) - \sum_{i\in T} d_i}{\sup_{i\in T}(d_i)} \quad . \qquad \text{Q. E. D.}$$

3.9. To establish 3.5.2 and finish the proof of 1.0, we first note the direct sum decomposition of $L(S,T,f)$:

3.9.0. $$L(S,T,f) \cong K + \sum_{\phi\neq A\subset S, \phi\neq B\subset T} D(A,B,f_{A,B})$$

according to which of the exponents of a monomial $Z^U X^V$ is strictly positive.

We next choose a total ordering $<$ on the set of all pairs (A,B) where A (resp. B) is a non-empty subset of S (resp. T) which satisfies the following property:

3.9.1. if $A \subseteq A'$ and $B \subseteq B'$, then $(A,B) \leqq (A',B')$

(such orderings do exist!). The desired filtration F of $L(S,T,f)$ is given by the subspaces (using the isomorphism 3.9.0)

3.9.2. $$F^{A,B}(L(S,T,f)) = \sum_{(A',B')\geqq(A,B)} D(A',B',f_{A',B'}).$$

One checks immediately that each of these subspaces is stable under $\alpha(S,T,f)$ The desired filtration of $(L(S,T,f), \alpha(S,T,f))$ is by the subobjects

$$(F^{A,B}(L(S,T,f)), \alpha(S,T,f) \mid F^{A,B}(L(S,T,f))).$$

The desired decomposition 3.5.2 of the associated graded object now follows directly from the definitions. This completes the proof of 1.0.

4. We will now prove that 1.0 is "best possible" in the following sense:

PROPOSITION 4.0. *Given non-empty finite sets S and T, and a mapping*

$$d: T \to \mathbf{Z}_{>0},$$

there exists a homogeneous triple (S,T,f) such that

4.0.1. $$\text{degree}(f_i) = d_i \quad \textit{for } i \in T$$

4.0.2. $$N(S,T,f) = q^{\mu(S,T,f)} \quad (\textit{an integer prime to } p).$$

Proof. We first consider the case $\mu(S,T,f) = 0$, i.e.

4.0.3. $$\text{Card}(S) \leqq \sum_{i \in T} d_i.$$

We will construct an f as above so that

4.0.4. $$N(S,T,f) = 1.$$

To do this, choose a covering of S by non-empty subsets $\{S_i\}_{i \in T}$, chosen so as to have

$$\text{Card}(S_i) \leqq d_i.$$

For each $i \in T$, we let

$$\xi_j^{(i)}, \quad j \in S_i$$

be $\text{Card}(S_i)$ linearly independent (over k) elements of k_{d_i}, the extension of k of degree d_i. We now use the norm from k_{d_i} to define f_i:

$$f_i = N_{k_{d_i}/k}\Big(\sum_{j \in S_i} \xi_j^{(i)} X_j\Big).$$

Clearly if x is a point of $\boldsymbol{A}^S$ with values in k,

$$f_i(x) = 0 \Leftrightarrow x_j = 0 \text{ for every } j \in S_i$$

and, as the S_i cover S, 4.0.4 follows.

We now consider the case $\mu(S,T,f) > 0$, i.e.

4.0.5. $$\text{Card}(S) \geqq \sum_{i \in T} d_i.$$

To fix ideas, suppose $T = \{1, \cdots, r\}$, and $d_1 \leqq d_2 \leqq \cdots \leqq d_r$. Let

4.0.6. $$\begin{cases} T' = \{1, \cdots, r-1\} \\ T'' = \{r\} \end{cases}$$

and let $S = S' \cup S''$ be a partition of S into two disjoint subsets, chosen so that

4.0.7. $$\begin{cases} \text{Card}(S') = \sum_{i \in T'} d_i \\ \text{Card}(S'') = \text{Card}(S) - \sum_{i \in T'} d_i. \end{cases}$$

We apply the previous technique to the situation $S', T', d_1, \cdots, d_{r-1}$, to obtain homogeneous polynomials $f_1', \cdots, f_{r-1}' \in k[S']$, degree $(f_i') = d_i$, and such that

4.0.8. $$N(S', T', f') = 1.$$

We next consider the situation S'', T'', d_r. Ax [1] exihibits a homogeneous polynomial $f'' \in k[S'']$ of degree d_r such that

4.0.9 $$N(S'', T'', f'') = q^{\mu(S'', T'', f'')} \text{ (an integer prime to } p).$$

Denoting by

$$\beta_{S',S}: k[S'] \to k[S]$$
$$\beta_{S'',S}: k[S''] \to k[S]$$

the canonical inclusions, the desired f is

4.0.10. $$f_i' = \begin{cases} \beta_{S',S}(f_i'), & i = 1, \cdots, r-1 \\ \beta_{S'',S}(f''), & i = r. \end{cases}$$

Indeed

4.0.11 $$V(S, T, f) = V(S', T', f') \underset{k}{x} V(S'', T'', f''),$$

so that

4.0.12 $$\begin{aligned} N(S, T, f) &= N(S', T', f') \cdot N(S'', T'', f'') \\ &= N(S'', T'', f'') \text{ by } 4.0.9. \end{aligned}$$

The conclusion now follows from 4.0.9, since by construction we have

4.0.13. $$\mu(S'', T'', f'') = \mu(S, T, f).$$ Q.E.D.

REFERENCES.

[1] J. Ax, "Zeroes of polynomials over finite fields," *American Journal of Mathematics*, vol. 86 (1964), pp. 255-261.

[2] P. Deligne, "Cohomclogie des Intersections Completes," Exposé XI, SGA7, 1969, multigraph available from *I. H. E. S.*, 91 Bures-sur-Yvette, France.

[3] B. Dwork, "On the rationality of the zeta function of an algebraic variety," *American Journal of Mathematics*, vol. 82 (1960), pp. 631-648.

[4] ———, "On the zeta function of a hypersurface: II," *Annals of Mathematics*, vol. 80, no. 2 (1964), pp. 227-229.

[5] ———, "Some remarks concerning the zeta function of an algebraic variety over a finite feld," in *Proceedings of the Woods Hole Summer Conference on Algebraic Geometry* (1964) (multigraph).

[6] A. Grothendieck, "Formule de Lefschetz et Rationalité des Fonctions *L*," *Seminaire Bourbaki*, 1964-65, no. 279, and reprinted in *Dix Exposés sur la Cohomologie des schémas*, North-Holland, Amsterdam (1968), pp. 31-45.

[7] ———, "Le Groupe de Brauer III: Exemples et Compléments," in *Dix Exposés sur la Cohomologie des schémas*.

[8] N. Katz, "Une Formule de Congruence pour la Fonction Zeta," Exposé XXII, SGA7, 1969, available from *I.H.E.S.*, 91 Bures-sur-Yvette, France.

[9] J.-P. Serre, "Endomorphismes Completement Continus des Espaces de Banach p-adiques, *Pub. Math. I.H.E.S.*, vol. 12 (1962).

[10] E. Warning, "Bermerkung zur Vorstehenden Arbeit von Herr Chevalley," *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, vol. 11 (1936), pp. 76-83.