LECTURES IN MATHEMATICS

Department of Mathematics
KYOTO UNIVERSITY

4

p-ADIC ANALYSIS AND ZETA FUNCTIONS

BY

PAUL MONSKY

Published by
KINOKUNIYA BOOK-STORE Co., Ltd.
Tokyo, Japan

LECTURES IN MATHEMATICS

Department of Mathematics

KYOTO UNIVERSITY

4

p-ADIC ANALYSIS

AND

ZETA FUNCTIONS

BY

PAUL MONSKY

Published by

KINOKUNIYA BOOK-STORE CO., Ltd.

Preface

During 1969 I was a guest lecturer in Japan, teaching a course in zeta functions and p-adic analysis at Kyoto University. These notes are essentially the lecture notes for that course.

The first term, I presented several "classical" results on zeta functions in characteristic p : Weil's calculation of the zeta function of a diagonal hypersurface, Grothendieck's proof of the "Riemann hypothesis" for curves via the Riemann-Roch theorem for surfaces, and Dwork's proof of rationality. The second term was increasing p-adic. After sketching Serre's spectral theory for compact operators I gave a version of Dwork's first paper on the zeta function of a non-singular hypersurface, stressing the "Lefschetz fixed point theorem" character of the proof. Finally some indications of the connections between Dwork's differential operator theory and various cohomology theories, classical and otherwise were given, closely following Katz's thesis. So there is little new here ; still I hope to have assembled some pretty results.

I'd like to thank Mr. Sumihiro and Mr. Maruyama for their companionship, and for their writing up of these notes and Professors Nagata and Suzuki among many others for making my year in Japan a delight.

Table of Contents

Chapter 0 - Introduction to Weil's Conjectures

Let k be GF(q) and k_s be GF(q^s). Suppose $F_1 \ldots F_m \in k[X_1, \ldots, X_n]$. Let N_s be the number of solutions in k_s of the equations:

$$F_1(x_1, \ldots, x_n) = F_2(x_1, \ldots, x_n) = \ldots = F_m(x_1, \ldots, x_n) = 0$$

How does N_s depend on s?

Examples

(1) The empty set of equations. $N_s = q^{ns}$.

(2) The single equation $X_1 X_4 - X_2 X_3 = 1$.

Then $N_1 = \dfrac{(q^2 - 1)(q^2 - q)}{q - 1} = q^3 - q$, and $N_s = q^{3s} - q^s$.

The equations $F_i = 0$ define an affine algebraic set in n-space and N_s is the number of k_s-rational points of this set. This suggests the more general question of studying the number of k_s rational points, N_s, of an arbitrary algebraic variety defined over k.

Examples

(1) V = projective n space = P^n. Then $N_1 = \frac{q^{n+1}-1}{q-1} = q^n + q^{n-1} + \ldots + 1$, and

$N_s = q^{ns} + \ldots + 1$.

(2) V = Grassmannian variety of lines in P^3, a 4-dimensional variety. Then

$$N_1 = \frac{(q^3+q^2+q+1)(q^3+q^2+q)}{q(q+1)} = q^4+q^3+2q^2+q+1 \text{ , and}$$

$$N_s = q^{4s}+q^{3s}+2q^{2s}+q^s+1.$$

(3) V is a complete non-singular curve of genus g. Weil proved that

$N_s = q^s - \sum_1^{2g} \alpha_i^s + 1$ where the α_i are algebraic integers of absolute value $\sqrt{q}$.

(We'll give Grothendieck's proof of this in Chapter 2).

The above examples suggest that N_s always has the form $\Sigma\, \alpha_i^s - \Sigma\, \beta_i^s$ for certain algebraic integers α_i and β_i. The classical Lefschetz fixed point theorem suggests why this might be true, at least when V is complete and non-singular.

Fixed point theorem - Let M be a compact smooth manifold and $\varphi: M \longrightarrow M$ be a smooth map. Suppose that φ has isolated fixed points and that at each fixed point P, $\det(I - d\varphi_p) > 0$. Then the number of fixed points of φ is equal to the alternating sum of the traces of the map φ^* on the (rational, say) cohomology groups of M. So if we let α_i be the eigenvalues of φ^* on $H^k(M;Q)$ for k even and β_i be the eigenvalues for k odd, then the number of fixed points of φ is equal to $\Sigma\, \alpha_i - \Sigma\, \beta_i$.

Now we have the following intuitive analogies:

compact manifold <——> complete non-singular variety

smooth map φ: M——> M <——> morphism φ: V ——> V.

When V is defined over GF(q) we have the Frobenius morphism φ: V ——> V given in local coordinates by $(a_1,\dots,a_n) \longrightarrow (a_1{}^q,\dots,a_n{}^q)$. The number of fixed points of φ is clearly N_1, and the differential of φ is 0. Similarly the number of fixed points of φ^s is N_s. So if we could set up a cohomology theory for varieties in arbitrary characteristic, and prove a Lefschetz fixed point theorem, we would have $N_s = \Sigma\, \alpha_i{}^s - \Sigma\, \beta_i{}^s$ where the α_i and β_i are the eigenvalues of φ^* on even and odd-dimensional cohomology. When we re-examine the examples given above we see that they fit very nicely into the proposed plan. Namely, projective n-space over the complexes has Betti numbers 1 in even dimensions up to 2n. Similarly the variety of lines in $P^3(\mathbb{C})$ has Betti numbers $B_0 = 1$, $B_2 = 1$, $B_4 = 2$, $B_6 = 1$ and $B_8 = 1$. So it looks as if the same sort of thing is happening in characteristic p, and as if the eigenvalues of φ^* on the conjectured $H^{2i}(V)$ are q^i for these varieties. Finally a curve of genus g over the complexes is a Riemann surface and has Betti numbers $B_0 = 1$, $B_1 = 2g$ and $B_2 = 1$, agreeing beautifully with example (3).

Considerations such as the above led Weil to certain conjectures which have had an important influence on algebraic geometry:

(a) For any V, $N_s(V) = \Sigma\, \alpha_i^{\,s} - \Sigma\, \beta_i^{\,s}$ with α_i and β_i algebraic integers.

(b) If V is complete and non-singular of dimension n, then $\gamma \longrightarrow q^n/\gamma$ induces a permutation of the α_i and a permutation of the β_i.

(c) If V is complete and non-singular, then each α_i has absolute value an even power of $\sqrt{q}$ and each β_i has absolute value an odd power of $\sqrt{q}$.

(d) More generally, there is a cohomology theory for varieties defined over arbitrary fields. Over the complexes this agrees with classical cohomology, furthermore it behaves well under reduction. For complete non-singular varieties, V, one may prove such results as Poincaré duality and a Lefschetz fixed point theorem. If furthermore V is defined over GF(q) and φ is the Frobenius, the eigenvalues of φ^* on H^i are algebraic integers of absolute value $q^{i/2}$.

(a) is now known to be true. We shall reproduce the first proof of (a), given by Dwork (c.f.[2]) in Chapter 5. (b) has been proved by Grothendieck; special cases of it were treated by Dwork and Lubkin. Once a good cohomology theory is set up, it proves to be a formal consequence of Poincaré duality. (c) is still largely a mystery. It is known for curves, abelian varieties, Grassmannians, the diagonal hypersurfaces $\Sigma\, a_i X_i^{\,n} = 0$, and in a few additional cases.

One difficulty in (d) is the choice of a coefficient field. Easy considerations with super-singular elliptic curves show that there can be no good cohomology theory over Q. For each prime ℓ Grothendieck has constructed an "ℓ-adic" cohomology theory; when V is a variety defined over a field of characteristic $\neq \ell$, this theory has excellent properties. In particular, Grothendieck, Artin and Verdier have proved all the assertions of (d) except for the last; (c) remains impervious to attack so far. This has enabled them to give proofs of (a) and (b). p-adic (or rather Witt vector) cohomology theories for varieties defined over fields of characteristic p have also been studied; these tend to be analogues of classical DeRham cohomology. Of interest here are the work of Dwork, of Lubkin, of Washnitzer and myself, and the theory of "crystals" of Grothendieck.

It is perhaps interesting to note that a Kähler variety analogue of (c) can be proved but that the proof uses integral cohomology, a tool not available in characteristic p.

Chapter 1 - Diagonal Hypersurfaces

Let V be the projective hypersurface in P^n over $k = GF(q)$ defined by the equation $\sum_0^n X_i^d = 0$. Under the assumption $q \equiv 1 \ (d)$ we shall compute $N_s(V)$ and verify the Weil conjectures (a), (b) and (c). The technique is easily modified to handle the hypersurface $\sum_0^n a_i X_i^d = 0$ where $a_i \in k$ and $(d,q) = 1$; for fuller details see [13].

We fix some notation. Let $\mathbb{C}^*$ be the multiplicative group of non-zero complexes. Let $\Theta: k \longrightarrow C^*$ be a fixed non-trivial character of the additive group of k. χ will denote a multiplicative character: $k^* \longrightarrow \mathbb{C}^*$, each such character will be extended to a function $k \longrightarrow \mathbb{C}$ by setting $\chi(0) = 0$. The trivial multiplicative character $a \longrightarrow 1$ $(a \neq 0)$ will be denoted by ϵ.

Definition The Gaussian sum g_χ associated to the character χ is the complex number $\sum_{a\in k} \chi(a)\Theta(a)$.

Lemma 1.1 $\sum_{a\in k} \Theta(a) = 0$. If $\chi \neq \epsilon$, $\sum_{a\in k} \chi(a) = 0$.

Proof: Choose b so that $\Theta(b) \neq 1$. Then, $\sum_{a\in k} \Theta(a) = \sum_{a\in k} \Theta(a+b) = \Theta(b). \sum_{a\in k} \Theta(a)$. The proof for χ is similar.

<u>Lemma 1.2</u> Suppose $\chi \neq \epsilon$. Then, for all $b \in k$, $\sum_{a\in k} \chi(a)\Theta(ab) = \overline{\chi(b)}\cdot g_\chi$.

<u>Proof:</u> If $b = 0$, use Lemma 1.1. Suppose $b \neq 0$. Then

$$\sum_{a\in k} \chi(a)\Theta(ab) = \sum_{a\in k} \chi(ab^{-1})\Theta(a) = \chi(b^{-1})\cdot g_\chi = \overline{\chi(b)}\cdot g_\chi .$$

<u>Lemma 1.3</u> If $\chi \neq \epsilon$, then $|g_\chi| = \sqrt{q}$.

<u>Proof:</u> $|g_\chi|^2 = g_\chi\cdot\bar{g}_\chi = g_\chi\cdot \sum_{b\in k} \overline{\chi(b)}\ \overline{\Theta(b)}$. By Lemma 1.2 we may rewrite this as

$$\sum_{a,b\in k} \chi(a)\Theta(ab)\ \overline{\Theta(b)} = \sum_{a,b} \chi(a)\Theta(b(a-1)) = \sum_{b\in k} \chi(1) + \sum_{a\neq 1} \chi(a) \sum_{b\in k} \Theta(b(a-1)) = q$$

by Lemma 1.1.

<u>Definition</u> Let $\chi_1,\ldots,\chi_s$ $(s \geq 2)$ be multiplicative characters of k and H be the hyperplane $\sum_1^s X_i = 0$ in k^s. The Jacobi sum $j(\chi_1,\ldots,\chi_s)$ is the complex number $\sum_{(a_1,\ldots,a_s)\in H} \chi_1(a_1)\ \ldots\ \chi_s(a_s)$.

<u>Theorem 1.1</u>

(a) If $\prod_1^s \chi_i \neq \epsilon$, then $j(\chi_1,\ldots,\chi_s) = 0$

(b) If $\prod_1^s \chi_i = \epsilon$ and no $\chi_i = \epsilon$, then $j(\chi_1,\ldots,\chi_s) = \frac{q-1}{q} \prod_1^s g_{\chi_i}$

<u>Proof:</u> To prove (a), choose $b \neq 0$ so that $\prod_1^s \chi_i(b) \neq 1$. Since $(a_1,\dots,a_s) \longrightarrow (ba_1,\dots,ba_s)$ maps H 1-1 onto itself, $j = \prod_1^s \chi_i(b)\cdot j$, and $j = 0$.

To prove (b) note that $\bar{j}\cdot g_{\chi_1} \cdots g_{\chi_s} = \sum_{(a_1,\dots,a_s)\in H} \{g_{\chi_1}\overline{\chi_1(a_1)}\} \cdots \{g_{\chi_s}\overline{\chi_s(a_s)}\}$.

By Lemma 1.2 this is just

$$\sum_{(a_1,\dots,a_s)\in H} \quad \sum_{(b_1,\dots,b_s)\in k^s} \chi_1(b_1)\cdots\chi_s(b_s)\cdot\Theta(a_1b_1 + \cdots + a_sb_s).$$

Now consider the contribution made to the above 2s-fold sum for fixed $b_1,\dots,b_s$.

(I) $b_1 = b_2 \cdots = b_s = 0$. The contribution is 0.

(II) $b_1 = b_2 \cdots = b_s = b$, $b \neq 0$. The contribution is $\sum_{(a_1,\dots,a_s)\in H} \Theta(0) = \text{card } H = q^{s-1}$. As there are q-1 possible values for b, these terms give $(q-1)\cdot q^{s-1}$.

(III) The b_i are not all equal. Let c_r be the number of solutions $(a_1,\dots,a_s)$ of the linear equations: $a_1 + \cdots + a_s = 0$, $b_1a_1 + \cdots + b_sa_s = r$. Then

$\sum_{(a_1,\dots,a_s)\in H} \Theta(a_1b_1 + \cdots + a_sb_s) = \sum_{r\in k} c_r\Theta(r)$. Since each $c_r = q^{s-2}$, this sum is 0, and we get no contribution to the 2s-fold sum.

Combining I, II and III we find that $j(\chi_1,\ldots,\chi_s)\cdot\prod_1^s g_{\chi_i} = q^{s-1}(q-1)$, so

$$j(\chi_1,\ldots,\chi_s) = \frac{q-1}{q}\prod_1^s q/\overline{g_{\chi_i}} = \frac{q-1}{q}\cdot\prod_1^s g_{\chi_i}$$ by Lemma 1.3.

We next study the relation between Gaussian sums in k and in an extension $k_\ell = GF(q^\ell)$ of k. Let $\Theta'\colon k_\ell \longrightarrow \mathbb{C}^*$ be the map $\Theta\circ\mathrm{Trace}_{k_\ell/k}$; Θ' is evidently a non-trivial additive character of k_ℓ. If $\chi\neq\epsilon$ is a multiplicative character of k, let χ' be the multiplicative character $\chi\circ\mathrm{Norm}_{k_\ell/k}$ of k_ℓ. Set

$$g_{\chi'} = \sum_{a\in k_\ell} \chi'(a)\Theta'(a).$$

Theorem 1.2 (Davenport-Hasse)

$$g_{\chi'} = (-1)^{\ell-1}\cdot(g_\chi)^\ell .$$

Proof: Suppose $F = X^n - c_1X^{n-1} \ldots + (-1)^n c_n$ is a monic element of $k[X]$. Set $\lambda(F) = \Theta(c_1)\cdot\chi(c_n)$. Then we obviously have (taking $\lambda(1) = 1$):

(1) $\lambda(FG) = \lambda(F)\cdot\lambda(G)$.

(2) Suppose $u\in k_\ell$ and F is the monic irreducible equation satisfied by u over k. Then $\lambda(F)^{\ell/d} = \chi'(u)\Theta'(u)$ where $d = \deg F$.

(3) $g_{\chi'} = \Sigma \deg F \cdot \lambda(F)^{\ell/\deg F}$, where the sum extends over all monic irreducible elements of $k[X]$ of degree dividing ℓ. (Every such F has $\deg F$ roots in k_ℓ and every element of k_ℓ is a root of such an F; now use (2)).

In the formal power series ring $C[[t]]$ we have:

$$(*) \qquad \Sigma\, \lambda(F) t^{\deg F} = \Pi\, (1-\lambda(F)t^{\deg F})^{-1}$$

where the sum extends over all monic F in $k[X]$ and the product over all monic irreducible F; this is a formal consequence of (1) and unique factorization. The sum in (*) is easily evaluated. The constant term is 1 and the coefficient of t is $\sum_c \lambda(X-c) = \sum_c \Theta(c)\chi(c) = g_\chi$. The coefficient of $t^d (d>1)$ is $q^{d-2} \cdot \sum_{c,c'} \Theta(c)\chi(c') = 0$.

So altogether we get $1+g_\chi \cdot t$. Taking formal logarithmic derivatives in (*) and multiplying by t:

$$\frac{g_\chi t}{1+g_\chi t} = \Sigma \frac{\lambda(F)\cdot(\deg F)\cdot t^{\deg F}}{1-\lambda(F)\cdot t^{\deg F}}$$

where the sum extends over all monic irreducible F. Comparing coefficients of t^ℓ on both sides, and using (3) gives the theorem.

We can now compute N_s for a diagonal hypersurface. Let $V \subset P^n$ be defined by the equation $\sum_0^n X_i^d = 0$, and assume $q \equiv 1(d)$. Let M_1 be the number of solutions of $\sum_0^n X_i^d = 0$ in affine $n+1$ space. Clearly $N_1(V) = (M_1 - 1)/q-1$.

Since k^* is cyclic and $q \equiv 1\ (d)$ there is a character χ of k^* onto the d'th roots of unity. Then $a \neq 0$ is a d'th power in k if and only if $\chi(a) = 1$. From this we conclude that if $a \in k$ the number of solutions in k of $z^d = a$ is $1 + \chi(a) + \ldots + \chi(a)^{d-1}$. (Consider the cases $a = 0$, $a \in (k^*)^d$ and $a \notin (k^*)^d$ separately).

Now each solution $(a_0,\ldots,a_n)$ of $\Sigma X_i^d = 0$ gives rise to a solution $(a_0^d,\ldots,a_n^d)$ of $\Sigma X_i = 0$, and the number of $(a_0,\ldots,a_n)$ mapping on a given $(u_0,\ldots,u_n)$ is evidently $(1 + \chi(u_0) + \ldots + \chi^{d-1}(u_0)) \ldots (1 + \chi(u_n) + \ldots + \chi^{d-1}(u_n))$. So M_1 may be explicitly written as:

$$\sum_{u_0 + \ldots + u_n = 0} (1 + \chi(u_0) + \ldots + \chi^{d-1}(u_0)) \ \ldots\ (1 + \chi(u_n) + \ldots + \chi^{d-1}(u_n)).$$

Let us expand the above product into monomials and sum each monomial over the hyperplane $u_0 + \ldots + u_n = 0$. The terms $1 \cdot 1 \cdot \ldots 1$ give a contribution of q^n. Any other term involving a 1 is easily seen to give 0. Recalling the definition of the Jacobi sums we find:

$M_1 = q^n + \sum_{1 \leq c_i \leq d-1} j(\chi^{c_0},\ldots,\chi^{c_n})$. Let S be the set of $n+1$-tuples of integers $(c_0,\ldots,c_n)$ with $1 \leq c_i \leq d-1$ and $\sum_0^n c_i \equiv 0\ (d)$. By Theorem 1.1,

$$M_1 = q^n + \frac{q-1}{q} \sum_{(c_0,\dots,c_n)\in S} g_{\chi^{c_0}} \cdots g_{\chi^{c_n}} . \text{ So}$$

$$N_1 = \frac{M_1 - 1}{q-1} = \frac{q^n - 1}{q-1} + \frac{1}{q} \sum_{(c_0,\dots,c_n)\in S} g_{\chi^{c_0}} \cdots g_{\chi^{c_n}} .$$ If $c = (c_0,\dots,c_n) \in S$,

let $\alpha_c = \frac{1}{q} \prod_0^n (-g_{\chi^{c_i}})$. Then $N_1 = (q^{n-1} + \dots + 1) + (-1)^{n-1} \sum_{c \in S} \alpha_c$. Now replace

k by k_s, q by q^s and χ by $\chi' = \chi \circ \text{Norm } k_s/k$. By Theorem 1.2,

$-g_{(\chi')^c} = (-g_{\chi^c})^s$. It follows that $N_s = (q^{(n-1)s} + \dots + 1) + (-1)^{n-1} \sum_{c \in S} (\alpha_c)^s$.

Furthermore, by Lemma 1.3, each α_c has absolute value equal to $q^{\frac{n-1}{2}}$. Thus

we have verified the Weil conjectures (a) and (c) for V. If

$c = (c_0,\dots,c_n) \in S$, let $c' = (d-c_0,\dots,d-c_n)$. Now $\alpha_c = \frac{(-1)^{n-1}}{q-1} \cdot j(\chi^{c_0},\dots,\chi^{c_n})$.

Consequently, $\alpha_{c'} = \frac{(-1)^{n-1}}{q-1} \cdot j(\bar{\chi}^{c_0},\dots,\bar{\chi}^{c_n}) = \bar{\alpha}_c = \frac{q^{n-1}}{\alpha_c}$. So conjecture

(b) holds too. Finally it may be shown that if V is the complex projective

hypersurface $\sum_{i=0}^{n} X_i^d = 0$, then the j'th Betti number $B_j(V)$ is equal to $B_j(P^{n-1})$

if $j \neq n-1$ and that $B_{n-1}(V) = B_{n-1}(P^{n-1}) + \text{card } S$. This accords perfectly with

conjecture (d), since $N_s(P^{n-1}) = (q^{(n-1)s} + \dots + 1)$ and each α_c has absolute value

equal to $q^{\frac{n-1}{2}}$.

Chapter 2 - Complete Non-singular Curves

Let V be a variety defined over $k = GF(q)$. To study the integers $N_s(V)$ it is convenient to build a certain formal power series $\zeta_V(t)$ out of them; Weil's conjecture (a) turns out to be equivalent to the assertion that $\zeta_V(t)$ is a quotient of 2 polynomials. Using this "zeta-function" and the Riemann-Roch theorem for curves we shall show that $N_s(V)$ has the form $q^s + 1 - \sum_1^{2g} \alpha_i^s$ for V a complete non-singular curve of genus g. Finally, with the aid of some intersection theory on the surface $V \times V$ we show that each α_i has absolute value $\sqrt{q}$, a celebrated result of Weil. The proof we give is due to Grothendieck [5].

Suppose that V is a variety defined over a perfect field k and that $\bar{k}$ is the algebraic closure of k. Identify V with its set of $\bar{k}$-rational points. A 0-cycle D on V is a formal Z-linear combination, $\Sigma\, n_i P_i$, of points of V. D is called "k-rational" if it is invariant under the action of the Galois group $G(\bar{k}/k)$. Let P be a point of V and $\{P_i\}$ be the orbit of P under $G(\bar{k}/k)$. $\Sigma\, P_i$ will be called a prime k-rational 0-cycle. It is easy to see that the k-rational 0-cycles form a free abelian group on the prime k-rational 0-cycles. By the degree of a 0-cycle $\Sigma\, n_i P_i$ we mean the integer $\Sigma\, n_i$; $\Sigma\, n_i P_i$ is "positive" if each $n_i \geq 0$.

Assume now that $k = GF(q)$. Let $k_s = GF(q^s)$ and define integers A_s, M_s and N_s by:

A_s = number of positive k-rational 0-cycles of degree s on V.

M_s = number of prime k-rational 0-cycles of degree s on V.

N_s = number of k_s-rational points of V.

Theorem 2.1

The following 3 formal power series are equal:

(a) $\sum_0^\infty A_s t^s$

(b) $\prod_1^\infty (1-t^s)^{-M_s}$

(c) $\exp\left(\sum_1^\infty \frac{N_s}{s} t^s\right)$.

Proof: Since the k-rational 0-cycles are a free abelian group on the prime ones, (a) = (b). By the Galois theory of finite fields, $N_s = \sum_{d/s} dM_d$. The formal logarithmic derivative of (b) is $t^{-1} \cdot \sum_1^\infty \frac{sM_s t^s}{1-t^s} = t^{-1} \cdot \sum_{s=1}^\infty \sum_{s'=1}^\infty sM_s t^{ss'}$.

But the formal logarithmic derivative of (c) is just $t^{-1} \cdot \sum_{s=1}^\infty N_s t^s$; comparing coefficients we find that (b) = (c).

Definition The above formal power series is the zeta function of V (over k); it is denoted by $\zeta_V(t)$.

Note that $\zeta_V(t)$ has non-negative integer coefficients and constant term 1. Suppose now that there are complex numbers α_i and β_i such that $N_s = \Sigma\, \alpha_i^{\,s} - \Sigma\, \beta_i^{\,s}$. Using definition (c) of $\zeta_V(t)$ we see easily that $\zeta_V(t) = \prod_i(1-\beta_i t)/\prod_i(1-\alpha_i t)$, a quotient of two polynomials over $\mathbb{C}$. Conversely suppose that $\zeta_V(t) = P/Q$ with P and Q in $\mathbb{C}[t]$. We can assume that the constant terms of P and Q are 1. Let $P = \prod(1-\beta_i t)$ and $Q = \prod(1-\alpha_i t)$ with $\alpha_i, \beta_i \in \mathbb{C}$. Taking logarithmic derivatives of the equation $\zeta_V = P/Q$ we find that $\Sigma\, N_s t^s = \Sigma \dfrac{\alpha_i t}{1-\alpha_i t} - \Sigma \dfrac{\beta_i t}{1-\beta_i t}$; equating coefficients of t^s, $N_s = \Sigma\, \alpha_i^{\,s} - \Sigma\, \beta_i^{\,s}$.

We next turn to the study of a non-singular projective curve C/k , of genus g. By the paragraph above we expect that $\zeta_C(t) = \prod_1^{2g} (1-\alpha_i t)/(1-t)(1-qt)$ and that $|\alpha_i| = \sqrt{q}$. To prove this we first recall some results for non-singular projective curves defined over a perfect field k.

Let $\bar{k}$ be the algebraic closure of k and $\bar{k}(C)$ be the function field of C over $\bar{k}$. In place of 0-cycle we use the word "divisor". Every $f \neq 0$ in $\bar{k}(C)$ defines a divisor, (f), of degree 0. If D is a divisor on C, then

$L(D) = \{f \in \bar{k}(C) \mid f = 0 \text{ or } (f) + D > 0\}$ is a finite dimensional vector space over $\bar{k}$. Set $\ell(D) = \dim L(D)$. Divisors D and D' are linearly equivalent if D-D' = (f) for some f.

We shall use the following pieces of the Riemann-Roch theorem for C. If $\deg D > 2g-2$, then $\ell(D) = \deg D - g + 1$. There is a canonical divisor W on C such that $\deg W = 2g-2$ and $\ell(W) = g$. Any divisor D of degree $2g-2$ not linearly equivalent to W has $\ell(D) = g-1$. We also need some "rationality" results. The Galois group $G(\bar{k}/k)$ operates on $\bar{k}(C)$. Call an element of $\bar{k}(C)$ k-rational if it is invariant under $G(\bar{k}/k)$. If f is k-rational then (f) is k-rational. If D is a k-rational divisor, then L(D) admits a basis of k-rational functions. If a k-rational divisor is the divisor of a function, it is the divisor of a k-rational function. Finally the canonical divisor W may be chosen to be k-rational.

We again restrict k to be GF(q).

Theorem 2.2 Let D be a k-rational divisor. The number of positive k-rational divisors linearly equivalent to D is $(q^{\ell(D)} - 1)/(q-1)$.

Proof: Let $\ell = \ell(D)$, and $f_1, \ldots, f_\ell$ be a basis of L(D) consisting of k-rational functions. Every positive k-rational divisor D' linearly equivalent to D has the form $(\sum_1^\ell \alpha_i f_i) + D$ with $\alpha_i \in k$, α_i not all 0. $(\alpha_1, \ldots, \alpha_\ell)$ and $(\beta_1, \ldots, \beta_\ell)$ determine the same divisor D' if and only if $\beta_i = \gamma \alpha_i$ with $\gamma \neq 0$ in k. The theorem follows.

An equivalence class of divisors under linear equivalence is called a divisor class.

Theorem 2.3 Let s be an integer. There are only finitely many divisor classes of degree s containing k-rational divisors.

Proof: Suppose $s \geq 2g$. Then, if $\deg D = s$, $\ell(D) = s - g + 1 \geq g + 1 > 0$. So if D is linearly equivalent to a k-rational divisor it is linearly equivalent to a positive k-rational divisor. As there are only finitely many such of degree s the result follows. To handle arbitrary s choose a k-rational divisor D' of large degree and make use of the map $D \longrightarrow D + D'$.

Definition. The class number, h, of C/k is the number of divisor classes of degree 0 on C containing k-rational divisors.

Let m be the smallest positive integer such that there exists a k-rational divisor of degree m. We shall compute $\zeta_c(t)$, and on the way show that $m = 1$. Observe:

(1) If $m \nmid s$, then $A_s = 0$

(2) If m/s and $s > 2g-2$, then $A_s = h\left(\frac{q^{s-g+1}}{q-1}\right)$, this is an easy consequence of Theorem 2.2.

$$\text{Now } \zeta_c(t) = \sum_{0}^{\infty} A_s t^s = (\text{polynomial in } t^m) + \frac{h}{q-1} \sum_{s=0}^{\infty} (q^{ms-g+1}-1)t^{ms} = (\text{polynomial in } t^m)$$

$$+ \frac{h}{q-1}\left(\frac{q^{1-g}}{1-q^m t^m} - \frac{1}{1-t^m}\right).$$ Thus $\zeta_c(t)$ is a quotient of 2 polynomials in t^m.

Viewing $\zeta_c(t)$ as a function on the complexes we see that it has a simple pole at $t = 1$.

Now let $f(t) = \prod_{s=1}^{\infty} (1-t^s)^{-M_{ms}}$ with the M_j as in Theorem 2.1. Then $\zeta_C(t) = f(t^m)$. By the paragraph above f is a quotient of 2 polynomials. Let $k^* = k_m$ and $\zeta^*(t)$ be the zeta-function of C over k^*. Theorem 2.1 lets us write $\zeta^*(t) = \prod_{s=1}^{\infty} (1-t^s)^{-M_s^*}$. Now if P is any point of C, the prime k-rational divisor determined by P has degree a multiple of m; it follows that $k(P) \supset k^*$. From this we deduce that $[k(P):k] = m \cdot [k^*(P):k^*]$, and that $M_s^* = m \cdot M_{ms}$. So $\zeta^*(t) = f(t)^m$. Since $\zeta^*(t)$ as well as $\zeta(t)$ has a simple pole at $t = 1$, $m = 1$.

Thus $\zeta(t) = (\text{polynomial}) + \frac{h}{q-1} \{ \frac{q^{1-g}}{1-qt} - \frac{1}{1-t} \} = P(t)/(1-t)(1-qt)$ where P is a polynomial with integer coefficients. Since the constant term of ζ is 1, so is that of P. We next show that $P(t) = q^g t^{2g} + \ldots$ Suppose first $g = 0$. Then

$A_s = h\,(\frac{q^{s+1}-1}{q-1})$ for all $s \geq 0$. Taking $s = 0$, we see that

$h = A_0 = 1$. So $\zeta(t) = \sum_0^{\infty} (\frac{q^{s+1}-1}{q-1})t^s = \frac{1}{(1-t)(1-qt)}$ and $P = 1$. Suppose next $g > 0$.

Let $A_s^* = \frac{h}{q-1}(q^{s-g+1}-1)$. If $s > 2g-2$, $A_s = A_s^*$. The divisor class containing the canonical divisor has $\frac{q^g-1}{q-1}$ positive k-rational divisors in it while the other divisor classes of degree $2g-2$ have the expected $\frac{q^{g-1}-1}{q-1}$. So

$A_s = A_s^* + q^{g-1}$ for $s = 2g-2$.

Now $\sum_0^\infty A_s^* t^s = \frac{h}{q-1} \{ \frac{q^{1-g}}{1-qt} - \frac{1}{1-t} \}$. This may be written as

$\frac{a+bt}{(1-t)(1-qt)}$ for appropriate a and b. So,

$\zeta_C(t) = \sum_0^{2g-2} (A_s - A_s^*)t^s + \sum_0^\infty A_s^* t^s = (q^{g-1}t^{2g-2}+\ldots) + \frac{(a+bt)}{(1-t)(1-qt)}$. It follows

immediately that $P(t) = q^g t^{2g} + \ldots$. Now write $P = \prod_1^{2g} (1-\alpha_i t)$. Since the

coefficients of P are integers, the α_i are algebraic integers. We have proved:

Theorem 2.4

Let C be a non-singular projective curve of genus g over $k = GF(q)$. Then $\zeta_C(t) = \prod_1^{2g} (1-\alpha_i t)/(1-t)(1-qt)$. The α_i are algebraic integers and $\prod_1^{2g} \alpha_i = q^g$.

By using the full Riemann-Roch theorem it's not hard to show that $\alpha \longrightarrow q/\alpha$ is a permutation of the α_i. We shall skip this and go directly to the proof that $|\alpha_i| = \sqrt{q}$. Since $N_s(C) = q^s + 1 - \sum_1^{2g} \alpha_i^s$,

$|\alpha_i| = \sqrt{q} \implies |N_s(C) - q^s - 1| \leq \text{constant} \cdot q^{s/2}$ for all s. Conversely we shall show that if $|N_s(C) - q^s - 1| \leq \text{constant} \cdot q^{s/2}$ for all s, then each α_i has absolute value $\sqrt{q}$.

Lemma 2.1 Let $\lambda_1, \ldots, \lambda_t$ be complex numbers of absolute value 1. Then there exists an integer $m > 0$ such that each λ_i^m is close to 1.

Lemma 2.2 Let $\alpha_1, \ldots, \alpha_t$ be complex numbers. Then there exist infinitely many integers $m > 0$ such that $|\alpha_1|^m \leq |\sum_1^t \alpha_i^m|$.

Proofs: Lemma 2.1 follows from an obvious pigeon-hole principle argument. To prove Lemma 2.2 we may assume $\alpha_1 = 1$, and must show that $|1 + \sum_2^t \alpha_i^m| \geq 1$ for infinitely many $m > 0$. But using Lemma 2.1 we may assume that $\left(\frac{\alpha_i}{|\alpha_i|}\right)^m$ is close to 1 so that the real part of $\alpha_i^m > 0$.

Theorem 2.5

Situation as in Theorem 2.4. The following statements are equivalent:

(a) $|\alpha_i| = \sqrt{q}$ for all i

(b) There is a constant c such that $|N_s - q^s - 1| \leq c \cdot q^{s/2}$ for all s.

Proof: (a) ==> (b) is trivial. Suppose (b) holds. By Lemma 2.2 there are infinitely many $s>0$ such that $|\alpha_1|^s \le |\sum_1^{2g} \alpha_i^s| = |N_s - q^s - 1| \le c\cdot q^{s/2}$. So $|\alpha_1| \le \sqrt{q}$. Similarly, $|\alpha_i| \le \sqrt{q}$. Since $\prod_1^{2g} \alpha_i = q^g$, $|\alpha_i| = \sqrt{q}$.

The simplest proofs that $|N_s - q^s - 1| \le c\cdot q^{s/2}$ involve interpreting N_s as an intersection product of 2 curves on the surface $C \times C$. So we recall some facts on the geometry of non-singular projective surfaces (cf. [9]). By a divisor on the surface S we mean a Z-linear combination of irreducible curves. There is a symmetric bilinear form into Z, the intersection product, defined on the divisors; we write $(D\cdot E)$ for the intersection product of D and E. If D is a divisor let $\mathcal{L}(D)$ be the invertible sheaf attached to D and $h^i(D) = \dim H^i(S, \mathcal{L}(D))$. The Riemann-Roch theorem for S states:

$$h^0(D) - h^1(D) + h^2(D) = \frac{1}{2}(D\cdot D-K) + \text{constant}$$

where K is a certain fixed "canonical divisor" on S. By "Serre duality", $h^2(D) = h^0(K-D)$. If we set $\ell(D) = h^0(D)$ we find that $\ell(D) + \ell(K-D) \ge \frac{1}{2}(D\cdot D-K) + \text{constant}$; this is a classical form of the Riemann-Roch theorem for surfaces, and the one we shall use.

Now fix a projective imbedding $S \subset P^N$. Let H be a hyperplane section of S. If D is a divisor on S set $\deg D = (D\cdot H)$.

Lemma 2.3 Let $\{D_i\}$ be a set of divisors on S. If deg D_i is bounded above, then $\ell(D_i)$ is bounded above.

Proof: If $\ell(D_i) = m$, the positive divisors linearly equivalent to D_i form an m-1 dimensional family. So m-1 is bounded by the dimension of the Chow variety of divisors of a certain degree on S.

Lemma 2.4 (Hodge)

Let D be a divisor on S. If $\deg D = 0$, then $(D\cdot D) \leq 0$.

Proof: By Lemma 2.3, $\{\ell(nD)\}$ and $\{\ell(K-nD)\}$ are bounded above for $n \in Z$. By the Riemann-Roch theorem, $(nD\cdot nD-K)$ is bounded above. So $(D\cdot D) \leq 0$.

Suppose now that $S = C \times C'$ with C and C' non-singular projective curves. If D is a divisor on S, set $d_1(D) = (D\cdot P \times C')$ and $d_2(D) = (D\cdot C \times P')$ where P and P' are points of C and C'. The definition is independent of the choice of P and P'.

Lemma 2.5 (Castelnuovo's inequality)

$$(D.D) \leq 2\, d_1(D) d_2(D)$$

Proof: Let V be the three dimensional vector space over the rationals spanned by the three divisors $P \times C'$, $C \times P'$ and D. Intersection product defines a quadratic form on V whose matrix is given by

$$M = \begin{pmatrix} 0 & 1 & d_1(D) \\ 1 & 0 & d_2(D) \\ d_1(D) & d_2(D) & (D.D) \end{pmatrix}$$

Now det $M = 2\, d_1(D)\, d_2(D) - (D\cdot D)$. Suppose det $M < 0$. Choose an orthogonal basis E_1, E_2, E_3 of V and let $(E_i \cdot E_i) = a_i$. Then $a_1\, a_2\, a_3 < 0$, so we may assume that a_1 and $a_2 > 0$ while $a_3 < 0$. (all a_i can't be < 0 since the quadratic form is indefinite on V). An appropriate Z-linear combination of E_1 and E_2 is a divisor of degree 0 and positive self-intersection number, contradicting Lemma 2.4.

Let C be a non-singular projective curve and $\varphi: C \longrightarrow C$ a morphism. Let Γ_φ and Δ be the graphs of φ and the identity map $C \longrightarrow C$ on the surface $S = C \times C$. We shall apply Castelnuovo's inequality to estimate the "number of fixed points", $(\Gamma_\varphi \cdot \Delta)$ of φ.

Theorem 2.6

Let d be the degree of the morphism $\varphi: C \longrightarrow C$. Then $|(\Gamma_\varphi \cdot \Delta) - 1 - d| \leq (2-(\Delta\cdot\Delta))\cdot \sqrt{d}$.

Proof: Define a symmetric bilinear form $*$ on the divisors of S by $D * E = d_1(D)\, d_2(E) + d_1(E)\, d_2(D) - (D\cdot E)$. By Lemma 2.5, $D * D \geq 0$. The Schwartz inequality then tells us that $|\Gamma_\varphi * \Delta| \leq \sqrt{(\Delta * \Delta)\cdot(\Gamma_\varphi * \Gamma_\varphi)}$.

Now $d_1(\Gamma_\varphi) = 1$, and intersection theory tells us that $d_2(\Gamma_\varphi) = d$. So the theorem will be proved if we can show that $(\Gamma_\varphi * \Gamma_\varphi) = d\cdot(\Delta * \Delta)$ and this reduces to proving that $(\Gamma_\varphi \cdot \Gamma_\varphi) = d\cdot(\Delta\cdot\Delta)$. Let $j\colon C \times C \longrightarrow C \times C$ be the map $(x,y) \longrightarrow (\varphi(x),y)$. j induces a pull-back map j^* on the cycles of $C \times C$, and j^* commutes with intersection product in the Chow ring of $C \times C$. Since $\deg j = d$, j^* induces multiplication by d on 0-cycles mod algebraic equivalence. So $(\Gamma_\varphi \cdot \Gamma_\varphi) = (j^*(\Delta)\cdot j^*(\Delta)) = d\cdot(\Delta\cdot\Delta)$ and we're done.

<u>Remark:</u> It can be shown that $2-(\Delta\cdot\Delta) = 2g$.

<u>Theorem</u> <u>2.7</u> (Weil).

Let C be a projective non-singular curve of genus g defined over $k = GF(q)$. Then $N_s(C) = q^s + 1 - \sum_1^{2g} \alpha_i^s$ where $|\alpha_i| = \sqrt{q}$ for each i.

<u>Proof</u>: Let $\varphi\colon C \longrightarrow C$ be the Frobenius map. Then $\deg \varphi^s = q^s$; by Theorem 2.6 $|(\Gamma_{\varphi^s}\cdot\Delta) - q^s - 1| \leq \{2-(\Delta\cdot\Delta)\} \cdot q^{s/2}$. Now Γ_{φ^s} and Δ intersect precisely at the points (x,x) where x is a k_s-rational point of C; furthermore they meet transversally at each such point with intersection multiplicity 1. Thus $(\Gamma_{\varphi^s}\cdot\Delta) = N_s$, and we may apply Theorem 2.5.

Chapter 3 - Ultra normed fields

We now turn to Dwork's remarkable proof, in [2], of Weil's conjecture (a) for an arbitrary variety defined over $GF(q)$. A basic tool in the proof is analysis in certain ultra-normed fields; we develop some basic machinery in this chapter.

Definition. Let K be a field. A norm on K is a map: $|| \ || : K \longrightarrow \mathbb{R}^+ \cup 0$ such that:

(1) $||x+y|| \leq ||x|| + ||y||$

(2) $||xy|| = ||x|| \cdot ||y||$

(3) $||x|| = 0$ if and only if $x = 0$.

If we define the distance from x to y to be $||x-y||$, then K becomes a metric space and addition, multiplication and inverse are all continuous functions on K. $\mathbb{R}$ = reals and C = complexes are the obvious examples of normed fields, there are some others of quite a different type as we shall soon see.

Definition A norm on K is an ultra-norm (or non-archimidean norm) if $||n \cdot 1|| \leq 1$ for every integer n.

Theorem 3.1

A norm on K is an ultra-norm if and only if the strict triangle inequality, $||x+y|| \leq \max(||x||, ||y||)$ holds for all x and y in K.

Proof Suppose $|| \ ||$ is an ultra-norm and $M = \max(||x||, ||y||)$. Then $||x+y||^n = ||x^n + \ldots + y^n|| \leq (n+1)M^n$. Taking n'th roots and letting $n \longrightarrow \infty$ gives the desired result. The converse is obvious.

Remarks

(1) In characteristic $p \neq 0$, $n \cdot 1$ is a root of unity or 0 for $n \in Z$. So $||n \cdot 1|| = 1$ or 0, and every norm is an ultra-norm.

(2) Ostrowski proved that every archimidean norm on a field K arises from a complex imbedding of K.

Suppose now that K is ultra-normed. Let $\mathcal{O}_K = \{x \in K: ||x|| \leq 1\}$ and $m_K = \{x \in K: ||x|| < 1\}$. $\mathcal{O}_K$ is evidently a valuation ring with maximal ideal m_K and quotient field K. The field $\mathcal{O}_K/m_K$ is called the residue-class field of K, and denoted by $\bar{K}$. We say that K is trivially normed if $\mathcal{O}_K = K$ (i.e. $x \neq 0 \Longrightarrow ||x|| = 1$), and that K is discretely normed if $\mathcal{O}_K$ is a discrete valuation ring.

Suppose K is discretely normed. Let π be a generator of m_K and $\lambda = ||\pi||$. Let ord be the order function arising from the valuation ring $\mathcal{O}_K$. Then for $x \neq 0$ in K, $||x|| = \lambda^{\text{ord } x}$. Conversely if $\mathcal{O}$ is a discrete valuation ring with quotient field K and λ is a real number with $0 < \lambda < 1$, then $x \longrightarrow \lambda^{\text{ord } x}$ is a discrete norm on K.

As an application we determine all non-trivial ultra-norms on the rationals. If p is a prime, the local ring $Z_{(p)}$ is a discrete valuation ring in Q and gives rise to a discrete norm, the p-adic norm. Explicitly, if $(m,p) = (n,p) = 1$, then $||p^s. \frac{m}{n}|| = \lambda^s$. We often normalize this norm by taking $\lambda = \frac{1}{p}$. Now let $||\ \ ||$ be any non-trivial ultra-norm on Q. Then $(\mathcal{O}_Q, m_Q)$ is a valuation ring and $m_Q \cap Z = (p)$ for some prime p. Since $\mathcal{O}_Q \supset Z_{(p)}$, $\mathcal{O}_Q = Z_{(p)}$ and we have the p-adic norm.

Remark It can also be shown that the only archimidean norms on Q are powers of the usual absolute value.

Definition A normed field is complete if it is complete in the metric derived from $||\ \ ||$.

The following is easily proved.

Theorem 3.2.

Let K be a normed field and $\hat{K}$ be the completion of K as metric space. Then $\hat{K}$ has the structure of complete normed field. If K is ultra-normed so is $\hat{K}$, and $\bar{K} = \bar{\hat{K}}$. If K is discretely normed so is $\hat{K}$.

The completion of Q with respect to the p-adic norm will be called Q_p. It is Hensel's "field of p-adic numbers". The analysis that we do in these notes will take place in Q_p (or more generally in finite extensions of Q_p). Analysis is often easier in ultra-normed fields than in archimidean ones. For example:

Theorem 3.3

Let a_i be a sequence in a complete ultra-normed field. Then Σa_i converges if and only if $a_i \longrightarrow 0$.

Proof: If $a_i \longrightarrow 0$, the strict triangle inequality shows that the sequence of partial sums of $\sum_1^\infty a_i$ is Cauchy and so converges. The converse is trivial.

We next study prolongations of ultra-norm. Let K be an ultra-normed field and K' a finite algebraic extension of K. (In the applications, $K = Q_p$).

Theorem 3.4

(1) There is a 1-1 correspondence between the prolongations of $\| \ \|$ to K' and the valuation rings in K' dominating $\mathcal{O}_K$. In particular, at least one prolongation exists.

(2) If K is complete there is a unique prolongation, and K' is complete too.

Proof: For any prolongation, $\{x \in K' : \|x\| \leq 1\}$ is a valuation ring dominating $\mathcal{O}_K$.

Conversely suppose $\mathcal{O}$ dominates $\mathcal{O}_K$. We have a map of groups, K^*/units of $\mathcal{O}_K \longrightarrow (K')^*$/units of $\mathcal{O}$. The cokernel of this map is finite. For if $u_1 \ldots u_r \in (K')^*$ are in distinct cosets mod the image, they are linearly independent over K Thus if $x \in (K')^*$, $x^n = \epsilon y$ for some unit ϵ in $\mathcal{O}$ and element y of K. Set

$||x|| = ||y||^{\frac{1}{n}}$; it's easy to see this is well defined and that $||x|| \leq 1$ if and only if $x \in \mathcal{O}$. So $||x|| \leq 1 \Longrightarrow ||x+1|| \leq 1$, and the strict triangle inequality follows proving (1). Suppose K is complete and $[K':K] = m$. Prolong the norm on K to K'. We prove by induction on dimension that every K-linear subspace V of K' is complete. If $\dim V = 1$, this is clear. If $\dim V > 1$, write $V = K\alpha \oplus W$. Since $K\alpha$ and W are complete it's enough to show that the projection map $V \longrightarrow K\alpha$ is continuous. If it's not there's a sequence $x_i \longrightarrow 0$ in V such that $x_i = \lambda_i \alpha + w_i$ with $\lambda_i \in K$ bounded away from 0 and $w_i \in W$. Then $x_i/\lambda_i \longrightarrow 0$ so $w_i/\lambda_i \longrightarrow -\alpha$. As W is complete it is closed in K' and $\alpha \in W$, a contradiction. In particular K' is complete.

Now choose a basis of K' over K. The above proof shows that the projection maps $K' \longrightarrow K$ are continuous so K' is homeomorphic with K^m. So any two norms on K' prolonging the norm on K induce the same topology on K'. Since $||x|| > 1$ if and only if $x^{-n} \longrightarrow 0$ as $n \longrightarrow \infty$, the topology determines $\{x \in K' : ||x|| \leq 1\}$. By (1), the prolongation is unique.

Theorem 3.5

Let K be a complete ultra-normed field and L an algebraic closure of K. The norm on K prolongs uniquely to L (but L need not be complete). $\bar{L}$ is the algebraic closure of $\bar{K}$.

Proof: Existence and uniqueness are obvious from (2) of Theorem 3.4. Also, if K' is finite over K, $\bar{K}'$ is finite over $\bar{K}$ (elements of $\mathcal{O}_{K'}$ representing linearly independent elements of $\bar{K}'$ over $\bar{K}$ are themselves linearly independent over K). Thus $\bar{L}$ is algebraic over $\bar{K}$. Suppose $\bar{f} \in \bar{L}[X]$ is monic. Pull $\bar{f}$ back to f monic in $\mathcal{O}_L[X]$. Since $\mathcal{O}_L$ is integrally closed, f factors into linear factors over $\mathcal{O}_L$,

$\bar{f}$ factors into linear factors over $\bar{L}$ and $\bar{L}$ is algebraically closed.

Theorem 3.6

Let L be the algebraic closure of Q_p; prolong the p-adic norm to L. Suppose $\bar{\alpha} \in \bar{L}$. Then $\bar{\alpha}^{p^r} = \bar{\alpha}$ for some r and there is a unique "Teichmüller representative" $\alpha \in \mathcal{O}_L$ such that $\alpha^{p^r} = \alpha$ and α reduces to $\bar{\alpha}$.

Proof: $\bar{\alpha}$ is algebraic over Z/p; if the degree of $\bar{\alpha}$ is r then $\bar{\alpha}^{p^r} = \bar{\alpha}$. The remaining assertions are true because the polynomial $X^{p^r} - X$ factors into distinct linear factors both over $\mathcal{O}_L$ and $\bar{L}$.

The Teichmüller representatives give a canonical set of representatives for the residue classes of m_L in $\mathcal{O}_L$. They are closed under multiplication, but not under addition.

Chapter 4 - The zeta function is "meromorphic"

Dwork's proof of Weil's conjecture (a) breaks up naturally into two parts. First he expresses $N_s(V)$ in terms of the traces of certain infinite matrices with co-efficients in a finite extension K of Q_p, and deduces that $\zeta_V(t)$ is a quotient of two everywhere convergent power series over K. A p-adic version of a classical theorem of Borel then shows that $\zeta_V(t)$ is a quotient of two polynomials and conjecture (a) follows easily. In this chapter we carry out the first part of this program.

Suppose K is a complete ultra-normed field and $f = \sum_{i \geq 0} a_i X^i \in K[[X]]$. If $u \in K$ and $a_i u^i \longrightarrow 0$ then $\sum_{i \geq 0} a_i u^i$ converges in K; we write $f(u) = \sum_{i \geq 0} a_i u^i$. It's easy to see that the f converging at u form a subring of K[[X]] and that $f \longrightarrow f(u)$ is a homomorphism of this subring to K. Let's assume now that K is a complete extension of Q_p and that the norm in K has been normalized so that $||p|| = p^{-1}$. If λ is real, let $S(\lambda) = \{1 + \sum_1^{\infty} c_i X^i \in K[[X]]$ such that $||c_i|| \leq p^{-\lambda i}$ for all i$\}$. $S(\lambda)$ is closed under multiplication and if $f \in S(\lambda)$ then f converges at all u such that $||u|| < p^{\lambda}$.

Now let π be an element of the algebraic closure, L, of Q_p satisfying $\pi^{p-1} = -p$. We describe certain important power series over the complete ultra-normed field $Q_p(\pi)$.

Definition

If r is an integer ≥ 1, $\Theta_r(X) = \exp \pi(X - X^{p^r})$.

We write Θ for Θ_1. Note that $\Theta_r(X) = \prod_{i=0}^{r-1} \Theta(X^{p^i})$.

Lemma 4.1 $\Theta_r \in S(0)$.

Proof: The exponent to which p occurs in i! is $[\frac{i}{p}] + [\frac{i}{p^2}] + \ldots \leq \frac{i}{p} + \frac{i}{p^2} \ldots = \frac{i}{p-1}$.

It follows that $\left|\left|\frac{\pi^i}{i!}\right|\right| \leq 1$ and that $\exp \pi X \in S(0)$. Similarly $\exp(-\pi X^{p^r}) \in S(0)$.

Our next goal is to show that the $\Theta_r \in S(\lambda)$ for some positive λ. Suppose $s \in Q$ (or even Q_p). By $(1+X)^s$ we mean the formal power series $1 + sX + \frac{s(s-1)}{2} X^2 + \ldots$.

Lemma 4.2 Let $\mu: Z^+ \longrightarrow \{0, \pm 1\}$ be the Möbius function. Then:

(1) $\exp X = \prod_{n \geq 1} (1-X^n)^{-\frac{\mu(n)}{n}}$

(2) $\exp(X + p^{-1}X^p) = \prod (1-X^n)^{\frac{-\mu(n)}{n}} (1-X^{np^2})^{\frac{\mu(n)}{np^2}}$ where the product extends over all positive n prime to p.

Proof: Let $f = \prod_{n\geq 1} (1-X^n)^{\frac{-\mu(n)}{n}}$. Then $Xf'/f = \sum_{n\geq 1} \frac{\mu(n)X^n}{1-X^n}$. Using the familiar fact that $\sum_{d/n} \mu(d) = 0$ for $n > 1$, we find that $f'/f = 1$, proving (1). Now (1) may be rewritten as $\exp X = \prod (1-X^n)^{\frac{-\mu(n)}{n}} (1-X^{np})^{\frac{\mu(n)}{np}}$, the product extending over all positive n prime to p. (2) follows immediately.

Lemma 4.3 Suppose $s \in Q_p$. Then:

(1) $(1+X)^s \in S(0)$ if $||s|| \leq 1$

(2) $(1+X)^s \in S(-r - \frac{1}{p-1})$ if $||s|| = p^r > 1$.

Proof: $(1+X)^s = \sum_0^\infty a_i X^i$ with $a_i = \frac{s(s-1)\dots(s-i+1)}{i!}$. So if $||s|| = p^r > 1$, then $||a_i|| = \frac{p^{ri}}{||i!||} \leq p^{i(r + \frac{1}{p-1})}$. To prove (1) note that $s \in Z \implies a_i \in Z$ and that $s \longrightarrow a_i$ are continuous functions $Q_p \longrightarrow Q_p$.

Theorem 4.1

$$\Theta_r \in S\left(\frac{p-1}{p^{r+1}}\right)$$

Proof: Let $f = \exp(X + p^{-1}X^p)$. By Lemmas 4.2 and 4.3, $f \in S(\delta)$ where

$\delta = \frac{1}{p^2}(-2-\frac{1}{p-1}) = \frac{1-2p}{p^2(p-1)}$. Thus $\Theta(X) = f(\pi X) \in S(\delta + \frac{1}{p-1}) = S(\frac{p-1}{p^2})$.

Now use the fact that $\Theta_r(X) = \prod_{i=0}^{r-1} \Theta(X^{p^i})$.

Corollary Let K be a complete extension of $Q_p(\pi)$ and u an element of K. If $||u|| \leq 1$, then the Θ_r converge at u.

Theorem 4.2

In the situation of the corollary suppose $||u|| \leq 1$. Then $\Theta(u) \equiv 1 + \pi u \ (\pi^2)$ in $\mathcal{O}_K$.

Proof: $\Theta(u) = 1+\pi u + \sum_2^\infty c_i u^i$ with $c_i \in Q_p(\pi)$. It clearly suffices to show that $||c_i|| < ||\pi||$ for $i \geq 2$. This will follow from Theorem 4.1 provided

$i \cdot (\frac{p-1}{p^2}) > \frac{1}{p-1}$, i.e. $i > (\frac{p}{p-1})^2$. So we only need worry about the cases when $2 \leq i \leq (\frac{p}{p-1})^2$. These can only occur when $p = 2$ or 3 and are handled by a direct calculation.

Theorem 4.3

$K = Q_p(\pi)$ contains the p'th roots of unity. There is a unique p'th root of unity λ in K such that $\lambda \equiv 1+\pi(\pi^2)$ in $\mathcal{O}_K$.

Proof: $\Theta(X)^p = (\exp \pi pX)\cdot(\exp - \pi pX^p)$. Both sides converge at X = 1; setting $\lambda = \Theta(1)$ and substituting $X = 1$ we find that $\lambda^p = 1$. By Theorem 4.2, $\lambda \equiv 1+\pi(\pi^2)$. So $\lambda \neq 1$, and the p'th roots of unity are in K. Since $\lambda^i \equiv 1+i\pi\ (\pi^2)$, λ is the unique p'th root of unity $\equiv 1+\pi\ (\pi^2)$.

Now let $k = GF(p^r)$. We shall define an additive character θ_r from k to the multiplicative group of $Q_p(\pi)$ and then show that Θ_r is a lifting of this character.

Definition

(1) $\theta: Z/p \longrightarrow Q_p(\pi)$ is the additive character $\bar{n} \longrightarrow \lambda^n$ (λ as in Theorem 4.3).

(2) $\theta_r: k \longrightarrow Q_p(\pi)$ is the map $\theta \circ Tr$ where Tr is the trace map from k to Z/p.

Since k is separable over Z/p, θ_r is a non-trivial additive character.

Theorem 4.4

Let L be the algebraic closure of Q_p, $\bar{u}$ an element of $\bar{L}$ satisfying $\bar{u}^{p^r} = \bar{u}$, and u the Teichmüller lifting of $\bar{u}$. Then $\Theta_r(u) = \theta_r(\bar{u})$.

Proof: Since $u^{p^r} = u$, the argument of Theorem 4.3 shows that $\Theta_r(u)$ is a p'th root of unity. Furthermore, $\Theta_r(X) = \prod_{i=0}^{r-1} \Theta(X^{p^i})$. Substituting $X = u$ and using Theorem 4.2 we find that $\Theta_r(u) \equiv 1+\pi(u+u^p+\ldots+u^{p^{r-1}})\ (\pi^2)$. Let n be an integer such that $\bar{n} = \mathrm{Tr}\ \bar{u} = (\bar{u}+\bar{u}^p+\ldots)$. Then, $n \equiv (u+u^p+\ldots)\ (\pi)$. So $\Theta_r(u) \equiv 1+n\pi\ (\pi^2)$; it follows that $\Theta_r(u) = \lambda^n = \theta_r(\bar{u})$.

A generalization of Theorem 4.4 in which Θ_r is replaced by a power series in several variables is useful. We use the usual multi-index notation; if $\alpha = (\alpha_0,\ldots,\alpha_n)$ is an n+1 tuple of non-negative integers then X^α means $\prod_0^n X_i^{\alpha_i}$ and $|\alpha|$ means $\sum_0^n \alpha_i$.

Suppose now that L is the algebraic closure of Q_p, that $G \in L[X_0,\ldots,X_n]$ and that every coefficient c of G satisfies $c^q = c$, with $q = p^r$. Let H be the formal power series in n+1 variables $\exp \pi\{G(X) - G(X^q)\}$.

Theorem 4.5

(1) There exists an $\epsilon > 0$ such that $H = \sum c_\alpha X^\alpha$ with $||c_\alpha|| \leq p^{-\epsilon|\alpha|}$.

(2) Suppose $\bar{u} = (\bar{u}_0 \ldots \bar{u}_n)$ is an n+1 tuple in $\bar{L}$ satisfying $\bar{u}^q = \bar{u}$, and $u = (u_0 \ldots u_n)$ is the Teichmüller lifting of $\bar{u}$. Then $H(u) = \theta_r \circ \bar{G}(\bar{u})$.

Proof: Since both exp and Θ_r are multiplicative it suffices to prove (1) and (2) when H is a monomial cX^{β}. Since $c^q = c$, Theorem 4.1 shows that (1) holds with $\epsilon = \frac{p-1}{p^{r+1}|\beta|}$. As for (2), $H(u) = \Theta_r(c\,u^{\beta})$. But cu^{β} is a root of $x^q = x$. By Theorem 4.4, $H(u) = \Theta_r(\bar{c}\,\bar{u}^{\beta}) = \Theta_r \circ \bar{G}(\bar{u})$.

Now let $k = GF(q) = GF(p^r)$ and $f \in k[X_1 \,..\, X_n]$. Let V^* be the variety defined by the equations $f(X_1 .. X_n) = 0$, $X_1 X_2 \,..\, X_n \neq 0$. We shall use p-adic methods to study the zeta function of V^*.

Lemma $$qN_1(V^*) - (q-1)^n = \sum_{(x_0 \ldots x_n) \in (k^*)^{n+1}} \Theta_r(x_0 f(x_1 .. x_n)).$$

Proof: Fix $(x_1 .. x_n) \in (k^*)^n$. If $f(x_1 .. x_n) = 0$, the contribution to the sum is q-1; otherwise it is -1. So the sum is $(q-1)N_1(V^*) - \{(q-1)^n - N_1(V^*)\}$.

Now let L be the algebraic closure of Q_p. Imbed k in $\bar{L}$ and let F be the lifting of f to $\mathcal{O}_L[X_1 .. X_n]$ whose coefficients satisfy $c^q = c$.
Let $G \in \mathcal{O}_L[X_0 .. X_n] = X_0 F$ and $H = \exp \pi\, \{G(X) - G(X^q)\}$. Theorem 4.5 and the lemma show that $qN_1(V^*) - (q-1)^n = \sum H(x_0 .. x_n)$ where $(x_0 .. x_n) \in (L^*)^{n+1}$ and $x_i{}^q = x_i$.
More generally, let $H_s = \exp \pi\, \{G(X) - G(X^{q^s})\} = \prod_{i=0}^{s-1} H(X^{q^i})$. The same argument with q replaced by q^s gives:

Theorem 4.6

$q^s N_s(V^*) - (q^s-1)^n = \Sigma H_s(x_0 \,..\, x_n)$, the sum extending over all

$(x_0 \,..\, x_n) \in (L^*)^{n+1}$ with $x_i^{q^s} = x_i$.

We next express the sums in the above theorem as the traces of certain infinite matrices. Let $K \subset L$ be the extension of Q_p generated by π and the roots of $x^q = x$. K is complete and contains the coefficients of each H_s. Let W be the vector space of formal sums $\Sigma\, c_\alpha X^\alpha$ with α running over n+1-tuples $(\alpha_0 \,..\, \alpha_n)$, $c_\alpha \in K$ and $c_\alpha \longrightarrow 0$ as $|\alpha| \longrightarrow \infty$. If T: W $\longrightarrow$ W is K-linear and $T(X^\beta) = \sum_\alpha c_{\alpha\beta} X^\alpha$, the matrix of T is the infinite matrix $\{c_{\alpha\beta}\}$. If $c_{\alpha\alpha} \longrightarrow 0$ we define the trace of T (or of the matrix of T) to be $\Sigma\, c_{\alpha\alpha}$. Let ψ: W $\longrightarrow$ W be the map $\Sigma\, c_\alpha X^\alpha \longrightarrow \Sigma\, c_{q\alpha} X^\alpha$.

Lemma Suppose $P \in W$. Let $\psi^s \circ P$: W $\longrightarrow$ W be ψ^s composed with multiplication by P. Let $c_\alpha(P)$ be the coefficient of X^α in P. Then:

$$\text{Trace } (\psi^s \circ P) = \sum_\alpha c_{(q^s-1)\alpha}(P) = \frac{1}{(q^s-1)^{n+1}} \; \Sigma\, P(x_0 \,..\, x_n) ,$$

the sum extending over $(x_0 \,..\, x_n) \in (L^*)^{n+1}$ with $x_i^{q^s} = x_i$.

Proof: The diagonal term $c_{\alpha\alpha}$ in the matrix of $\psi^s \circ P$ is $c_{(q^s-1)\alpha}(P)$.

It suffices to check the second equality for P a monomial ; this is easy.

Theorem 4.7

$$q^s N_s(V^*) - (q^s-1)^n = (q^s-1)^{n+1} \quad Tr(\psi \circ H)^s \quad .$$

Proof By Theorem 4.6 and the lemma it's enough to show that $\psi^s \circ H_s = (\psi \circ H)^s$. Now it's easy to see that for $P \in W$, $\psi \circ (P(X^q)) = P(X) \circ \psi$. Thus

$$(\psi \circ H)^s = \psi \circ H \circ \psi \circ H .. \psi \circ H = \psi^s \circ \{H(X) \cdot H(X^q) ... H(X^{q^{s-1}})\} = \psi^s \circ H_s \quad .$$

Now let $W_0 \subset W = \{\Sigma\, c_\alpha X^\alpha : ||c_\alpha|| \leq 1$ and $c_\alpha \longrightarrow 0\}$. The linear transformations $T: W \longrightarrow W$ such that $T(W_0) \subset W_0$ form an algebra over $\mathcal{O}_K$. If T is in this algebra and $\{c_{\alpha\beta}\}$ is the matrix of T then $c_{\alpha\beta} \in \mathcal{O}_K$ and for fixed β $c_{\alpha\beta} \longrightarrow 0$ as $|\alpha| \longrightarrow \infty$. It's not hard to see that $T \longleftrightarrow \{c_{\alpha\beta}\}$ sets up a 1-1 correspondence between our algebra of linear transformations and the matrices described above. So we can give this set of matrices the structure of $\mathcal{O}_K$ algebra, and we see that addition and multiplication are what we expect. In particular, $(cd)_{\alpha\beta} = \sum_\gamma c_{\alpha\gamma} d_{\gamma\beta}$.

Theorem 4.8

There is a matrix $\{c_{\alpha\beta}\}$ in $\mathcal{O}_K$ with the following properties:

(1) $||c_{\alpha\beta}|| \leq \gamma^{q|\alpha|-|\beta|}$ for some fixed γ, $0 < \gamma < 1$.

(2) $q^s N_s(V^*) - (q^s - 1)^n = (q^s-1)^{n+1} \text{ Tr } M^s$ for all s.

Proof: Let M be the matrix of $\psi \circ H$: $W \longrightarrow W$. If $M = \{c_{\alpha\beta}\}$, then $c_{\alpha\beta} = c_{q\alpha-\beta}(H)$. (1) then follows from Theorem 4.5 with $\gamma = p^{-\epsilon}$. The discussion above shows that the matrix of $(\psi \circ H)^s$ is M^s. Theorem 4.7 then gives (2).

We shall call an element of K[[X]] entire if it converges for all $u \in K$, meromorphic if it is a quotient of 2 entire power series. We shall use Theorem 4.8 to show that $\zeta_{V^*}(t)$ is meromorphic. The key step is:

Theorem 4.9

Let $M = \{c_{\alpha\beta}\}$ be a matrix in $\mathcal{O}_K$. Suppose $||c_{\alpha\beta}|| \leq \gamma^{q|\alpha|-|\beta|}$ for some γ, $0 < \gamma < 1$. Then Tr M^s exists for all s and the "characteristic power series",

$$\varphi_M(t) = \exp(-\sum_1^\infty \frac{\text{Tr } M^s}{s} t^s)$$ is entire.

Remark Let M_0 be a finite matrix. Easy linear algebra shows that

$\exp(-\sum_1^\infty \frac{\text{Tr } M_0{}^s}{s} t^s) = \det(I - tM_0)$. Thus $\varphi_M(t)$ is some sort of generalization of the characteristic polynomial to infinite matrices.

Proof: We need several lemmas.

Lemma 4.4 Tr M^s exists and is equal to $\lim \operatorname{Tr} M_0^s$ where M_0 runs over the finite submatrices of M whose rows and columns have the same indexing set. $\varphi_M(t)$ is the coefficientwise limit of $\det(I - tM_0)$, with M_0 above.

Proof: $M^s_{\lambda^{(0)}\lambda^{(0)}} = \Sigma\, c_{\lambda^{(0)}\lambda^{(1)}} c_{\lambda^{(1)}\lambda^{(2)}} \cdots c_{\lambda^{(s-1)}\lambda^{(0)}}$ where $\lambda^{(j)} (1 \le j \le s-1)$ run over the n+1-tuples of non-negative integers. Now the norm of the term above is $\le \gamma^{(q-1)\sum_{i=0}^{s-1}|\lambda^{(i)}|}$. Since $\sum_{i=0}^{s-1} |\lambda^{(i)}| \longrightarrow \infty$ as the $\lambda^{(i)}$ vary, it follows that Tr M^s exists and is equal to $\sum_{\lambda^{(0)},\dots,\lambda^{(s-1)}} c_{\lambda^{(0)}\lambda^{(1)}} \cdots c_{\lambda^{(s-1)}\lambda^{(0)}}$. Using the similar result for Tr M_0^s we see that Tr $M_0^s \longrightarrow$ Tr M^s. This, together with the remark preceding the lemma, gives the final assertion.

Lemma 4.5 Let M_0 be a $j \times j$ submatrix of M, as in Lemma 4.4. Then, $\|\det M_0\| \le \gamma^{j\lambda_j}$ where $\lambda_j \longrightarrow \infty$ with j.

Proof: $\det M_0$ is a sum of terms of the form $\pm c_{\alpha^{(1)}\beta^{(1)}} \cdots c_{\alpha^{(j)}\beta^{(j)}}$ with the $\alpha^{(i)}$ distinct n+1-tuples, and the $\beta^{(i)}$ a permutation of the $\alpha^{(i)}$. The norm of such a term is $\le \gamma^{(q-1)\sum_1^j \alpha^{(i)}}$. Let $\lambda_j = \frac{q-1}{j} \min \sum_1^j |\alpha^{(i)}|$ where the $\alpha^{(i)}$ run over distinct n+1-tuples. Evidently $\lambda_j \longrightarrow \infty$ with j. Since $\|\det M_0\| \le \gamma^{j\lambda_j}$, we're done.

It's now easy to prove Theorem 4.9. Let M_0 be a finite submatrix of M as in Lemma 4.4. The coefficient of t^j in $\det(I-tM_0)$ is a sum of determinants of $j \times j$ submatrices of M_0 (with rows and columns indexed by the same set) and has norm $\leq \gamma^{j\lambda_j}$ by Lemma 4.5. By Lemma 4.4, if $\varphi = \varphi_M(t)$ then $||c_j(\varphi)|| \leq \gamma^{j\lambda_j}$, so φ is entire.

Theorem 4.10

$\zeta_{V^*}(t)$ is meromorphic over K.

Proof: We may write $(q^s-1)^n = \sum_{i \equiv n(2)} a_i q^{is} - \sum_{i \not\equiv n(2)} b_i q^{is}$,

$(q^s-1)^{n+1} = \sum_{i \not\equiv n(2)} c_i q^{is} - \sum_{i \equiv n(2)} d_i q^{is}$ where a_i, b_i, c_i, d_i (≥ 0) are certain binomial coefficients. By Theorem 4.8, $q^s N_s(V^*) =$

$\Sigma a_i q^{is} - \Sigma b_i q^{is} + \Sigma c_i q^{is} \operatorname{Tr} M^s - \Sigma d_i q^{is} \operatorname{Tr} M^s$. It follows that

$$\zeta_{V^*}(qt) = \exp\left(\Sigma \frac{q^s N_s(V^*)}{s} t^s\right) = \left\{ \frac{\Pi(1-q^i t)^{b_i} \cdot \Pi\, \varphi_M(q^i t)^{d_i}}{\Pi(1-q^i t)^{a_i} \cdot \Pi\, \varphi_M(q^i t)^{b_i}} \right\}.$$

Replace t by $q^{-1}t$ and use Theorem 4.9.

Theorem 4.11

Let V be any variety defined over $k = GF(q)$. Let $K \subset L$ be the extension of Q_p generated by π and the roots of $x^q = x$. Then $\zeta_V(t)$ is meromorphic over K.

Proof: By induction on dim V. If W is a closed subset of V then $N_s(V) = N_s(W) + N_s(V-W)$, so $\zeta_V = \zeta_W \cdot \zeta_{V-W}$. So if the result holds for two of V,W and V-W it holds for the third.

By removing the singular set (which has lower dimension) from V we make V a disjoint union of irreducible varieties and so may assume V irreducible over k. V is birational with a hypersurface over k, and hence birational with a V^* as in Theorem 4.10. Since dense open subsets of V and V^* are isomorphic, Theorem 4.10 and an induction finish the proof.

It's also possible to get Theorem 4.11 from Theorem 4.10 by a combinatorial argument as in Dwork [2].

Chapter 5 - Rationality of the zeta function

We shall need a criterion, due to E. Borel, for a power series to represent a rational function.

Theorem 5.1

Let K be a field and $f = \sum_{0}^{\infty} a_i X^i$ an element of $K[[X]]$. If m,n are integers > 0 let $N_{n,m}$ be the determinant of the matrix $|a_{n+i+j}|$, $0 \leq i,j < m$. Then f is a quotient of two polynomials if and only if there exists an m such that $N_{n,m} = 0$ for all large n.

Proof: Suppose first $f = g/(1-\sum_{1}^{k} d_i X^i)$ with $g \in K[X]$. Then for $n > \deg g$, $a_n = d_1 a_{n-1} + \cdots + d_k a_{n-k}$. So $N_{n,m} = 0$ for $m = k+1$ and n large.

Conversely suppose $N_{n,m} = 0$ for n large ; choose m as small as possible. Take n large with $N_{n+1,m-1} \neq 0$. Let V_i be the column vector $(a_i, \ldots a_{i+m-1})$ and M the symmetric matrix $(V_n | V_{n+1} | \cdots V_{n+m-1})$. Since $\det M = 0$ there is a non trivial relation $\sum_{0}^{m-1} r_i V_{i+n} = 0$. Since $N_{n+1,m-1} \neq 0$, the lower left and upper right $(m-1) \times (m-1)$ submatrices of M are non-singular. It follows that $r_0 \neq 0$ and $r_{m-1} \neq 0$, that V_{n+m-1} is a linear combination of $V_n \ldots V_{n+m-2}$ and that $N_{n+2,m-1} = \pm \frac{r_0}{r_{m-1}} N_{n+1,m-1} \neq 0$. Repeating the argument with n replaced by $n+1$ we find that V_{n+m} is a linear combination of $V_{n+1} \ldots V_{n+m-1}$. I claim in fact that the vector $\sum_{0}^{m-1} r_i V_{i+n+1} = 0$. The first m-1 components of the vector obviously vanish, and the last does also since the bottom row of the matrix $(V_{n+1} | \cdots | V_{n+m})$ is a linear combination of the others.

An induction now shows that $\sum_{0}^{m-1} r_i V_{i+k} = 0$ for all $k \geq n$. Thus $f \cdot (r_{m-1} + \cdots + r_o X^{m-1})$ is a polynomial.

By Theorem 4.11 the zeta-function $\sum_{0}^{\infty} a_i t^i$ of a variety, V, may be written as $\sum_{0}^{\infty} c_i t^i / (1 - \sum_{1}^{\infty} d_i t^i)$ where numerator and denominator are entire over an ultra-normed field K. To show that $\zeta_V(t)$ is rational we study the explicit dependence of the $N_{n,m}$ of Theorem 5.1 on c_i and d_i. The $N_{n,m}$ are clearly polynomials in c_i and d_i, we show in some sense that the c_i and d_i with i small don't make much of a contribution to $N_{n,m}$.

The problem is a formal algebraic one so let c_i $(i \geq 0)$ and d_i $(i \geq 1)$ be indeterminates over Z. Define $a_i \in Z[c_i, d_i]$ by $\sum a_i t^i = \sum c_i t^i / 1 - \sum d_i t^i$ and let $a_i = 0$ for $i < 0$. If $\lambda = (\lambda_1 \cdots \lambda_m)$ and $\mu = (\mu_1 \cdots \mu_m)$ are m-tuples of (possibly negative) integers let $N^{(\lambda_1 \cdots \lambda_m)}_{(\mu_1 \cdots \mu_m)}$ (or more briefly N^λ_μ) be the determinant of the matrix $| a_{\lambda_i + \mu_j} |$; $N^\lambda_\mu \in Z[c_i, d_i]$. Let weight $\Pi c_i^{r_i} \cdot \Pi d_j^{s_j} = \sum i r_i + \sum j s_j$; an element of $Z[c_i, d_i]$ has weight r if every monomial occurring in it has weight r.

<u>Lemma 5.1</u> Notation as above. Then:

(1) Weight $N^\lambda_\mu = \sum \lambda_i + \sum \mu_i$

(2) N^λ_μ has total degree m in the c's

(3) N^λ_μ has degree $\leq \max (\lambda_i + \mu_j)$ in each d

Proof: Clearly $a_i = c_i + d_1 a_{i-1} + \cdots + d_i a_o$, $(i \geq 0)$. By induction a_i has weight i and total degree 1 in the c's . This gives (1) and (2). To prove (3) we may assume that $\lambda_1 < \lambda_2 \cdots < \lambda_m = \lambda'$ and $\mu_1 < \mu_2 \cdots < \mu_m = \mu'$. If $\lambda' + \mu' < 0$, $N^{\lambda}_{\mu} = 0$. So we assume $\lambda' + \mu' \geq 0$ and argue by induction on $\lambda' + \mu'$. Let M be the matrix $|a_{\lambda_i} + \mu_j|$ and M' the same matrix with $a_{\lambda_i + \mu'}$ replaced by $c_{\lambda_i} + \mu'$ (or 0 if $\lambda_i + \mu' < 0$) in the final column. Using the relations $a_k = c_k + d_1 a_{k-1} \cdots + d_k a_0$ to decompose the last column of M we find that

$$N^{(\lambda_1 \cdots \lambda_m)}_{(\mu_1 \cdots \mu_m)} = \sum_{i=1}^{\lambda'+\mu'} d_i N^{(\lambda_1, \lambda_2, \cdots, \lambda')}_{(\mu_1, \mu_2, \cdots, \mu'-i)} + \det M' .$$

Expanding det M' in terms of the last column of M' and using induction gives the lemma.

Lemma 5.2 Let K be an ultra-normed field. Suppose $c_i (i \geq 0)$, $d_i (i > 0) \varepsilon K$. Define $a_i \varepsilon K$ by $\Sigma a_i t^i = \Sigma c_i t^i / 1 - \Sigma d_i t^i$, and $N_{n,m} \varepsilon K$ as in Theorem 5.1.

Suppose $||c_j|| \leq \lambda^j$ and $||d_j|| \leq \lambda^j$ for j large, where $\lambda > 0$. Then there is a constant c such that $|| N_{n,m} || \leq c^{n+3m} . \lambda^{m(m-1) + nm}$.

Proof: Choose $A \geq 1$ and j_o so that $||c_j||$ and $||d_j||$ are $\leq A \lambda^j$ for all j and $\leq \lambda^j$ for $j > j_o$. Let $\Pi c_i^{r_i} \cdot \Pi d_j^{s_j}$ be a monomial occuring in $N_{n,m}$. In the notation of Lemma 5.1, $N_{n,m} = N^{(0,1 \cdots m-1)}_{(n,n+1, \cdots n+m-1)}$. So:

(1) $\Sigma\, i r_i + \Sigma\, j s_j = nm + m(m-1)$

(2) $\Sigma r_i \leq m$

(3) $s_j \leq n + 2m$

Thus $|| \Pi c_i^{r_i} \cdot \Pi d_j^{s_j} || \leq A^m \cdot A^{j_o(n+2m)} \cdot \lambda^{nm + m(m-1)}$

Now take $c = A^{j_o}$ and use the strict triangle inequality.

Lemma 5.3. Let $|| \quad ||$ be the normalized p-adic norm on Q, $| \quad |$ the usual absolute value. If n is an integer and $|| n || \cdot | n | < 1$, then $n = 0$.

Proof: Write $n = \pm p^s m$ with $(m,p) = 1$. Then $|| n || \cdot | n | = m$.

Theorem 5.2 (Dwork)

Let $f \in Z[[X]]$. Suppose that f has positive radius of convergence in $\mathbb{C}$ and is meromorphic over some extension K of Q_p. Then f is a quotient of two polynomials with rational co-efficients.

(A similar result was proved by Borel, assuming that f was a quotient of two entire power series over $\mathbb{C}$, rather than over K. For generalizations see Dwork [2]).

Proof: Write $f = \sum_0^\infty a_i X^i$, $a_i \in Z$. Since f has positive radius of convergence in $\mathbb{C}$, $| a_i | < aR^i$ for some constants a and R. Choose λ so $\lambda R < 1$. Normalize the norm in K so that $||p|| = p^{-1}$ and write $f = \Sigma c_i X^i / 1 - \Sigma d_i X^i$ with numerator and denominator entire. Then $||c_j||$ and $||d_j||$ are $< \lambda^j$ for j large.

Now define $N_{n,m}$ as in Theorem 5.1. The $N_{n,m}$ are integers; we shall estimate $||N_{n,m}||$ and $|N_{n,m}|$. By Lemma 5.2 $||N_{n,m}|| \leq c^{n+3m} \lambda^{m(m-1) + nm}$ for some constant c. Since $|a_i| \leq aR^i$, obvious estimates show that $|N_{n,m}| \leq m! \cdot a^m \cdot R^{m(m-1) + nm}$. Choose an m so large that $(\lambda R)^m \leq \frac{1}{2c}$. Then, $||N_{n,m}|| \cdot |N_{n,m}| \leq$ constant $\cdot$

$c^n \cdot (\lambda R)^{nm} \leq \text{constant} \cdot (\frac{1}{2})^n$. By Lemma 5.3, $N_{n,m} = 0$ for n large, and Theorem 5.1 finishes the proof.

Theorem 5.3

Let V be a variety over $k = GF(q)$. Then $\zeta_V(t)$ is a rational function over Q . More precisely $\zeta_V(t) = g/h$ where g and $h \in Z[t]$ and have constant term 1 ; thus Weil's conjecture (a) holds for V .

Proof: Note first that $\zeta_V(t)$ has positive radius of convergence over $\mathbb{C}$. (When $V = k^n$, $\zeta_V(t) = \frac{1}{1-q^n t}$, when $V \subset k^n$ the co-efficients of $\zeta_V(t)$ are bounded in absolute value by the co-efficients of $\frac{1}{1-q^n t}$, and the general case reduces easily to the affine case on covering V with finitely many affines.) We saw in the last chapter that $\zeta_V(t)$ is meromorphic over an extension of Q_p . By Theorem 5.2, $\zeta_V(t) = g/h$ with g and h in $Q[t]$. We may assume that $(g,h) = 1$ in $Q[t]$ and that g and h have constant term 1. It will suffice to show that $h \in Z[t]$. Suppose on the contrary that some prime r divides the denominator of a co-efficient of h . Write $h = \Pi\,(1-\alpha_i t)$ with α_i in the algebraic closure of Q_r . Evidently $\|\alpha_i\| > 1$ for some i . Then $h \cdot \zeta_V(t) = g$ and both sides coverge at $t = \alpha_i^{-1}$, since $\zeta_V \in Z[[t]]$. Substituting $t = \alpha_i^{-1}$ we find that $g(\alpha_i^{-1}) = h(\alpha_i^{-1}) = 0$, contradicting the fact that $(g,h) = 1$. Writing $g = \Pi\,(1-\beta_i t)$ and $h = \Pi\,(1-\alpha_i t)$, we get Weil's conjecture (a) easily.

Not too much is known about the α_i and the β_i in general. As we've remarked, Weil conjectured that for V complete $|\alpha_i|^2$ is an even and $|\beta_i|^2$ an odd power of q ; perhaps $|\alpha_i|^2$ and $|\beta_i|^2$ are powers of q even when V isn't complete. There's one further interesting result. Putting Theorem 5.3 together with a result of Lang and Weil one finds that if V is absolutely irreducible of dimension n then $N_s(V) = q^{ns} + \Sigma \alpha_i^s - \Sigma \beta_i^s$ with $|\alpha_i|$ and $|\beta_i| \leq q^{n-\frac{1}{2}}$. (The proof depends on Weil's results for curves.) Presumably $|\alpha_i| \leq q^{n-1}$, but this remains unknown.

The proof that we've given of Theorem 5.2 differs a little from Dwork's, which makes use of some factorization theorems for entire power series. As these results are of interest in themselves we devote the rest of this chapter to them. Let K be a complete ultra-normed field, $\mathcal{O} = \{ u \in K \mid \|u\| \leq 1 \}$ and $\mathcal{O}\{X\}$ the ring of power series $\sum_0^\infty c_i X^i$ where $c_i \in \mathcal{O}$ and $c_i \longrightarrow 0$.

If $f = \Sigma c_i X^i \in \mathcal{O}\{X\}$, set $\|f\| = \max \|c_i\|$. It's easy to see that $\|f+g\| \leq \max(\|f\|, \|g\|)$, $\|fg\| = \|f\| \cdot \|g\|$, and that $\mathcal{O}\{X\}$ is complete in the metric, $d(f,g) = \|f-g\|$, defined by $\|\ \ \|$. If $f = \Sigma c_i X^i \in \mathcal{O}\{X\}$, let $\bar{f}$ be the element $\Sigma \bar{c}_i X^i$ of $\bar{K}$. Note that f is a unit in $\mathcal{O}\{X\}$ if and only if $\bar{f}$ is a non-zero constant. For suppose $\bar{f}$ is a constant $\neq 0$. We may suppose $\bar{f} = 1$. Then $f = 1-g$ with $\|g\| < 1$, and $1 + g + g^2 + \cdots$ converges to an inverse of f. Conversely if f is a unit in $\mathcal{O}\{X\}$, $\bar{f}$ is a unit in $\bar{K}[X]$, and so constant.

We now prove a "Weierstrass preparation theorem" in $\mathcal{O}\{X\}$.

<u>Theorem 5.4</u>

Suppose $f \in \mathcal{O}\{X\}$, $\bar{f} \neq 0$, $\deg \bar{f} = n$. Then $f = ug$ where u is a unit in $\mathcal{O}\{X\}$ and $g \in \mathcal{O}[X]$ is monic of degree n. The decomposition is unique. If f is in $\mathcal{O}[X]$, so is u; if f is entire so is u.

Proof: Choose $f_o \varepsilon \mathcal{O}[X]$ of degree n so that $\bar{f} = \bar{f}_o$. Then $\| f-f_o \| < 1$; choose α in $\mathcal{O}$ so that $\|\alpha\| = \| f-f_o \|$. Since every element of $\mathcal{O}\{X\}$ is congruent to a polynomial mod α, the ring $\mathcal{O}\{X\}/(\alpha,f) = \mathcal{O}\{X\}/(\alpha,f_o)$ is generated as $\mathcal{O}$-module by X^i, $0 \le i < n$. In particular, $X^n = \sum_1^n a_i X^{n-i} + v_1 \alpha + w_1 f$ with $a_i \varepsilon \mathcal{O}$ and v_1, w_1 in $\mathcal{O}\{X\}$. Continuing we may write:

$$v_1 = \sum_1^n b_i X^{n-i} + v_2 \alpha + w_2 f$$

$$v_2 = \sum_1^n c_i X^{n-i} + v_3 \alpha + w_3 f$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot$$

where b_i, c_i, ... are in $\mathcal{O}$ and v_i, w_i are in $\mathcal{O}\{X\}$. Now let $r_i = a_i + \alpha b_i + \alpha^2 c_i + \cdots$ and $w = w_1 + \alpha w_2 + \alpha^2 w_3 + \cdots$. Then, $X^n = \sum_1^n r_i X^{n-i} + wf$. So wf is an element $g = X^n - \sum_1^n r_i X^{n-i}$ of $\mathcal{O}[X]$, monic of degree n. Since $\overline{wf} = \bar{g}$, $\bar{w}$ is a non-zero constant and w is a unit. Set $u = w^{-1}$.

Next write $f = \sum_o^\infty \alpha_i X^i$, $u = \sum_o^\infty \beta_i X^i$. Since $f = ug$, we find that:

$$\beta_i = \alpha_{i+n} + r_1 \beta_{i+1} + \cdots + r_n \beta_{i+n}$$

$$\beta_{i+1} = \alpha_{i+n+1} + r_1 \beta_{i+2} + \cdots + r_n \beta_{i+n+1}$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot$$

Since $||\beta_j|| \longrightarrow 0$ as $j \longrightarrow \infty$, the above equations show that

$||\beta_i|| \leq \max ||\alpha_{n+i+k}||$ $(k \geq 0)$. So if f is in $\mathcal{O}[X]$, so is u; if f is entire so is u. Suppose finally we had two decompositions

$f = ug = u^*g^*$. Then $g = \eta g^*$ with η a unit in $\mathcal{O}\{X\}$. Since $g \in \mathcal{O}[X]$, the argument above shows that $\eta \in \mathcal{O}[X]$ As g and g^* are monic of degree n, $g = g^*$ and the decomposition is unique.

Corollary Suppose $f \in \mathcal{O}[X]$ and $0 < \deg \bar{f} < \deg f$. Then f is reducible in $\mathcal{O}[X]$.

The corollary may be used to give another proof of the unique prolongation of norm to a finite extension L of K. For suppose that $u \in L$ and $N_{L/K}(u) \in \mathcal{O}$. The irreducible equation h of u over K then has the form $X^n + \sum_1^n a_i X^{n-i}$ with $a_n \in \mathcal{O}$. Now every a_i must be in $\mathcal{O}$, otherwise a constant multiple of h would give a counterexample to the corollary. So u is integral over $\mathcal{O}$. Thus $N_{L/K}(u) \in \mathcal{O}$ if and only if u is integral over $\mathcal{O}$, and the integral closure of $\mathcal{O}$ in L is a valuation ring. The rest is easy.

Theorem 5.5

Suppose $f \in K[[X]]$ is entire and r is a positive real number. Then $f = g f_1$ where $g \in K[X]$, $f_1 = 1 + \sum_1^\infty c_i X^i$ is entire, and $||c_i|| < r^i$ for all i.

Proof: If $r \geq 1$, apply Theorem 5.4 to a suitable constant multiple of f. In general, choose u in K so that $0 < \| u \| \leq r$ and replace f by $f(u^{-1}X)$.

Remark: This is the tool used by Dwork in his proof of Theorem 5.2 which takes the place of our Lemma 5.1. For details see [2].

Now let E be the ring of entire power series over K and $E_0 = \{f \in E \mid c_0(f) = 1\}$. We shall use Theorem 5.5 to study the multiplicative structure of E_0.

Lemma Let p be an irreducible element of $K[X]$ and u a root of p in the algebraic closure of K. Suppose $f \in E$. Then p divides f in E if and only if $f(u) = 0$.

Proof: Suppose $f(u) = 0$. Let $r = \| u \|^{-1}$ and write $f = g f_1$ as in Theorem 5.5. Since $\| c_i u^i \| < 1$, $f_1(u) \neq 0$ so $g(u) = 0$. Thus p divides g in $K[X]$ and f in E. The converse is obvious.

The lemma shows that p generates a prime ideal in E. Furthermore, $\cap\, p^n E = (0)$. For suppose that $f \neq 0$ is in E. Write $f = g f_1$ as in the proof of the lemma. Then p doesn't divide f_1 and only divides g to finite order. Now, if $f \neq 0$ is in E let $\operatorname{ord}_p(f)$ be the largest integer s such that p^s divides f. Evidently $\operatorname{ord}_p(fg) = \operatorname{ord}_p(f) + \operatorname{ord}_p(g)$.

We now turn our attention to E_0, the set of elements of E of constant term 1. If $f \in E_0$ set $\lambda(f) = \max_{i>0} \| c_i(f) \|^{\frac{1}{i}}$. (Note that $\| c_i(f) \|^{\frac{1}{i}} \longrightarrow 0$ since f is entire.)

Lemma $\lambda(fg) = \max(\lambda(f), \lambda(g))$. In particular, if f divides g in E_0, then $\lambda(f) \leq \lambda(g)$.

Proof: Let $r = \max(\lambda(f), \lambda(g))$. Then $||c_i(f)|| \leq r^i$, $||c_i(g)|| \leq r^i$ for all i. It follows that $||c_i(fg)|| \leq r^i$ and that $\lambda(fg) \leq r$. To prove the converse there are two cases to consider. Suppose first that $r = \lambda(f) > \lambda(g)$. Choose $i > 0$ so that $||c_i(f)|| = r^i$; then $c_i(fg) = r^i$ too and $\lambda(fg) \geq r$. Finally, if $\lambda(f) = \lambda(g) = r$ choose i and j as large as possible so that $||c_i(f)|| = r^i$, $||c_j(g)|| = r^j$. Then $||c_{i+j}(fg)|| = r^{i+j}$ and $\lambda(fg) \geq r$.

Theorem 5.6

Let $\{f_i\}$ be a sequence in E_0 such that $\lambda(f_i) \longrightarrow 0$. Then $\prod_1^\infty f_i$ converges co-efficientwise to some $f \in E_0$. Furthermore $\mathrm{ord}_p(f) = \sum_1^\infty \mathrm{ord}_p(f_i)$ for every irreducible p in $K[X]$.

Proof: Since $\lambda(f_i) \longrightarrow 0$, all but finitely many f_i are in $\mathcal{O}\{X\}$, and $f_i \longrightarrow 1$ in the norm metric on $\mathcal{O}\{X\}$. Using the completeness of $\mathcal{O}\{X\}$ we find that $\prod f_i$ converges co-efficientwise to some f and that a non-zero constant multiple of f is in $\mathcal{O}\{X\}$, i.e. that $c_j(f) \longrightarrow 0$. Suppose $u \in K$. Since $\lambda(f_i(uX)) = ||u|| \cdot \lambda(f_i)$ we may apply the above argument to the sequence $f_i(uX)$ and conclude that $||u||^j \cdot c_j(f) \longrightarrow 0$. As this is true for all u, f is in E_0.

Now choose r so that $0 < r < \lambda(p)$. (We may assume that $c_o(p) = 1$). Let $g = \prod_{\lambda(f_i) > r} f_i$ and $h = \prod_{\lambda(f_i) \leq r} f_i$; the infinite product for h converges by the paragraph above. Using the lemma we see that $\lambda(h) \leq r$ so p does not divide h. Thus $\mathrm{ord}_p(f) = \mathrm{ord}_p(g) = \sum_{\lambda(f_i) > r} \mathrm{ord}_p(f_i) = \sum_1^\infty \mathrm{ord}_p(f_i)$.

Theorem 5.7

Suppose $p_i (i \geq 1)$ are distinct and irreducible elements of $K[X]$ with constant term 1 and that n_i $(i \geq 1)$ are positive integers. Suppose further that $\lambda(p_i) \longrightarrow 0$. Then $\prod_{i \geq 1} p_i^{n_i}$ converges co-efficientwise to an element f of E_0. Conversely, every $f \in E_0$ admits such a "Weierstrass factorization", and the p_i and n_i are uniquely determined.

Proof: The first statement and the uniqueness assertion are immediate from Theorem 5.6. To show that f admits a Weierstrass factorization choose $r \geq \lambda(f)$ and write $f = g\, f_1$ with $g \in K[X]$ and $\lambda(f_1) \leq \frac{r}{2}$, this is possible by Theorem 5.5. Write $g = \prod_1^{s_1} p_i^{n_i}$ with p_i irreducible. Since p_i divides f, $\lambda(p_i) \leq r$. By absorbing the p_i with $\lambda(p_i) \leq \frac{r}{2}$ into f_1 we may assume that $\frac{r}{2} < \lambda(p_i) \leq r$. Similarly we may write $f_1 = (\prod_{s_1+1}^{s_1+s_2} p_i^{n_i}) \cdot f_2$ where

$\lambda(f_2) \leq \frac{r}{4}$ and $\frac{r}{4} < \lambda(p_i) \leq r/2$. Continuing in this way we get a Weierstrass factorization of f .

In particular if K is complete and algebraically closed then every f in E_0 has a product representation $\prod_{i \geq 1} (1-a_i X)^{n_i}$ with $a_i \longrightarrow 0$.

Chapter 6 - p-adic Banach Spaces

In the proof that the zeta-function of a variety is p-adic meromorphic a certain linear transformation, $\psi \circ H$, on an infinite dimensional vector space arose. We shall develop Serre's theory of completely continuous operators on p-adic Banach spaces and use it to study these transformations. A fuller treatment is given in Serre [12].

Let K be a complete ultra-normed field and V a vector space over K. A norm on V is a function $|| \ ||$ from V to the non-negative reals satisfying:

(1) $||u+v|| \leq \max(||u||, ||v||)$

(2) $||au|| = ||a|| \cdot ||u||$, $a \in K$

(3) $||u|| = 0$ if and only if $u = 0$.

If we set $d(u,v) = ||u-v||$ we get a metric on V; V is said to be a Banach space over K if it is complete in this metric. An important example is the following. Let I be any set and $C(I)$ the vector space of functions $f: I \longrightarrow K$ such that $f(i) \longrightarrow 0$. (I.e. for any $r > 0$ there are only finitely many i with $||f(i)|| \geq r$). Set $||f|| = \max ||f(i)||$; with this norm $C(I)$ becomes a Banach space. For $j \in I$ let $e_j \in C(I)$ be the j-th coordinate vector, $e_j(i) = \delta_{i,j}$. The e_j are said to form an orthonormal basis of $C(I)$. A collection $\{v_i\}$ of elements in a Banach space V is an "orthonormal basis" of V if there is a Banach space isomorphism $V \approx C(I)$ mapping v_i on e_i. If a Banach space admits one orthonormal basis it admits many. In fact we have the following useful result.

Theorem 6.1

Suppose V admits an orthonormal basis and W is a finite dimensional subspace of V. Then there exists an orthonormal basis of V containing a basis of W over K.

Proof: To simplify notation suppose V has a countable orthonormal basis $\{e_i\}$. We argue by induction on $\dim W$. Choose $w = \sum_1^\infty a_i e_i \neq 0$ in W. Multiplying by a constant and permuting the e_j we may assume $a_1 = 1$, $||a_i|| \leq 1$. Now the map $\sum_1^\infty r_i e_i \longrightarrow r_1 e_1 + \sum_2^\infty (r_i + a_i r_1)\, e_i$ is norm-preserving and bijective, fixes $e_i (i \geq 1)$ and maps e_1 on w. So we may assume e_1 is in W. Now let V' be the closed subspace of V having $e_i (i \geq 1)$ as an orthonormal basis, $W' = V' \cap W$, and continue by induction.

Theorem 6.1 shows that W admits an orthonormal basis and is closed in V. (More generally, a finite dimensional subspace W of any Banach space V is closed; a proof along the lines of Theorem 3.4 is easily given).

We next study spaces of linear transformations. If $T: V \longrightarrow W$ is a linear map of Banach spaces let $||T|| = \sup \frac{||T(u)||}{||u||}$, $u \neq 0$ in V. Then T is continuous if and only if $||T|| < \infty$. Let $L(V,W)$ be the space of continuous linear maps $V \longrightarrow W$. Then $T \longrightarrow ||T||$ is a norm on this space; one checks easily that $L(V,W)$ is complete in the norm metric and thus a Banach space. The space $L(V,V)$ is even a "Banach algebra", i.e. $||T \circ U|| \leq ||T|| \cdot ||U||$.

Suppose now that V admits a countable orthonormal basis $\{e_i\}$. Let $C^*(Z)$ be the space of sequences $a = \{a_i\}$ in K of bounded norm; set $||a|| = \sup ||a_i||$. Then $L(V,K)$ is isomorphic with $C^*(Z)$ as Banach space, the isomorphism mapping T on the sequence $\{T(e_i)\}$. One can give a similar explicit description of $L(V,V)$. Let $\mathfrak{M}$ be the space of matrices $M = |a_{ij}|$, $(1 \leq i,j < \infty)$, in K such that $||a_{ij}||$ is bounded and the column vectors of M are in $C(Z)$. Set $||M|| = \sup ||a_{ij}||$. If $T \in L(V,V)$ define a matrix $M = |a_{ij}|$ by $T(e_j) = \sum_{i=1}^{\infty} a_{ij} e_i$. Then $T \longleftrightarrow M$ gives a Banach space isomorphism of $L(V,V)$ with $\mathfrak{M}$, and composition of maps correspondsto matrix multiplication. Note that if $M \in \mathfrak{M}$ then the row vectors of M are in $C^*(Z)$ (but not necessarily in $C(Z)$).

From now on let V be a fixed Banach space admitting a countable orthonormal basis. We shall study a certain class of elements of $L(V,V)$, the "completely continuous" operators. (In fact, we don't need to assume that the basis of V is countable and only do so to avoid the awkward notation arising from matrices with uncountably many rows and columns. Also many of the results we'll get are true for arbitrary Banach spaces.)

<u>Definition</u>. $C_{fin}(V,V)$ is the 2-sided ideal in $L(V,V)$ consisting of operators with finite dimensional image. $C(V,V)$ is the closure of $C_{fin}(V,V)$ in the norm topology of $L(V,V)$. The elements of $C(V,V)$ are called "completely continuous operators".

It's easy to see that $C(V,V)$ is a 2-sided ideal in $L(V,V)$. Note also that every element, T, of $C_{fin}(V,V)$ is the sum of finitely many, each of which has 1-dimensional image. For we have an orthonormal basis $\{e_i\}$ of V with $e_1,\dots,e_s$ spanning the image of T. If we let $p_i : V \longrightarrow K e_i$ be the i'th projection map then $T = \sum_1^s p_i \circ T$.

Theorem 6.2

Let $\{e_i\}$ be an orthonormal basis of V, T an element of $L(V,V)$ and M the matrix of T on the basis $\{e_i\}$. Then $T \in C(V,V)$ if and only the row vectors of $M \longrightarrow 0$ in the norm topology of $C^*(Z)$.

Proof: Let $\mathfrak{M}_0 \subset \mathfrak{M}$ be those matrices whose row vectors $\longrightarrow 0$. We show first that $T \in C(V,V) \Longrightarrow M \in \mathfrak{M}_0$. As $\mathfrak{M}_0$ is a closed subspace of $\mathfrak{M}$ we may assume that $T \in C_{fin}(V,V)$, and even that T has 1-dimensional image. Let $u = \sum_1^\infty r_i e_i$ be an element of image T of norm 1. Then $T(e_i) = a_i u$ with $||a_i|| \leq ||T||$, and the i'th row vector $(a_1 r_i, a_2 r_i, \ldots)$ of M has norm $\leq ||T|| \cdot ||r_i||$. Conversely suppose $M \in \mathfrak{M}_0$. Let M_i be the matrix obtained from M by replacing all row vectors after the i'th by zero and T_i the element of $L(V,V)$ with matrix M_i. Since $M_i \longrightarrow M$ in $\mathfrak{M}$, $T_i \longrightarrow T$ in $L(V,V)$. As image $T_i \subset \sum_{j=1}^{i} K e_j$, $T \in C(V,V)$.

Our next goal is to describe a certain entire power series $D_\Theta(t)$, the Fredholm determinant, attached to a completely continuous operator Θ. Suppose first that $\Theta \in C_{fin}(V,V)$. Let W be a finite dimensional subspace of V containing image Θ and $\Theta_0 = \Theta | W$. Set $c_i(\Theta) = c_i(\Theta_0) = (-1)^i \operatorname{Tr} \Lambda^i(\Theta_0)$. Let $D_\Theta(t)$ be the polynomial $1 + \sum_{i>0} c_i(\Theta) t^i = \det(1 - t\Theta_0)$. An easy matrix calculation shows that $D_\Theta(t)$ is independent of the choice of W.

Theorem 6.3

Suppose Θ and $\Theta' \in C_{fin}(V,V)$ and have norm ≤ 1. Then $||c_k(\Theta) - c_k(\Theta')|| \leq ||\Theta - \Theta'||$ for all k.

Proof: Let W be a finite dimensional subspace of V containing image Θ and image Θ'. Let $\{e_i\}$ be an orthonormal basis of V such that $e_1,\ldots,e_s$ span W. Let $M = |a_{ij}|$ and $M' = |a_{ij}'|$ be the matrices of $\Theta|W$ and $\Theta'|W$ on the basis $e_1,\ldots,e_s$ of W. By hypothesis, $||a_{ij}|| \leq 1$, $||a_{ij}'|| \leq 1$, and $||a_{ij} - a_{ij}'|| \leq ||\Theta - \Theta'||$. Since $c_k(\Theta) = c_k(\Theta|W)$ is a polynomial in the a_{ij} with integer coefficients the result follows.

Combining Theorem 6.3 with the fact that $c_k(a\Theta) = a^k c_k(\Theta)$ we find:

Corollary The functions $c_k: C_{fin}(V,V) \longrightarrow K$ are uniformly continuous on bounded subsets of $C_{fin}(V,V)$ and thus extend uniquely to continuous functions $c_k: C(V,V) \longrightarrow K$.

Definition If $\Theta \in C(V,V)$, $D_\Theta(t)$ is the power series $1 + \sum_1^\infty c_k(\Theta)t^k$.

We shall show that D_Θ is entire. Choose an orthonormal basis $\{e_i\}$ of V and let M be the matrix of Θ on this basis. Arrange the norms of the row vectors of M in order of decreasing size, allowing repetitions. We get in this way a sequence of non-negative real numbers r_i such that $r_1 \geq r_2 \geq r_3 \ldots$ and $r_i \longrightarrow 0$.

Theorem 6.4.

With the notation as above, $||c_k(\Theta)|| \leq r_1 r_2 \ldots r_k$. Thus $D_\Theta(t)$ is entire.

Proof: Let M_i^* be the upper left $i \times i$ submatrix of M and T_i be the maps defined in the proof of Theorem 6.2. Then $T_i \in C_{fin}(V,V)$ and $c_k(T_i)$ is the coefficient of t^k in $\det(1-tM_i^*)$. This coefficient is a sum of products, each of which involves terms from k distinct rows of M. Thus $||c_k(T_i)|| \leq r_1 r_2 \ldots r_k$. As $T_i \longrightarrow \Theta$, $c_k(T_i) \longrightarrow c_k(\Theta)$ and we're done.

In the study of completely continuous operators on V it's useful to consider the K-algebra of formal power series $f = \sum_0^\infty A_i t^i$ with co-efficients in $L(V,V)$. The entire f, i.e. those for which $r^i \cdot ||A_i|| \longrightarrow 0$ for all real r, form a subalgebra of this algebra. If f is entire and $u \in K$ then $\sum_0^\infty u^i A_i$ converges in $L(V,V)$ to an operator which we call $f(u)$; clearly $f \longrightarrow f(u)$ is a homomorphism. By identifying the element a of K with the element $a \cdot I$ of $L(V,V)$ we may view every power series over K as a power series over $L(V,V)$; we do this from now on without further comment.

Definition Suppose $\Theta \in C(V,V)$. $R_\Theta(t)$ is the formal power series $D_\Theta(t) \cdot (1 + \Theta t + \Theta^2 t^2 \ldots)$

R_Θ is called the Fredholm resolvent of Θ. Its co-efficients are polynomials in Θ.

Theorem 6.5

R_Θ is entire.

Proof: Let $\{e_i\}$ be an orthonormal basis of V, M the matrix of Θ on this basis and $r_1 \geq r_2 \geq \dots$ the sequence of norms of row vectors of M arranged in order of decreasing size. Let $R_\Theta(t) = 1 + \sum_1^\infty u_i(\Theta)\cdot t^i$. Since $r_i \longrightarrow 0$ it suffices to prove:

Lemma $$||u_i(\Theta)|| \leq r_1 r_2 \dots r_i$$

Now choose a sequence $\Theta_i \longrightarrow \Theta$ as in the proof of Theorem 6.3 such that image $\Theta_s \subset \sum_1^s K e_j$. Since $u_i(\Theta)$ is a continuous function of Θ it suffices to prove the lemma for each Θ_s. Thus we may assume image $\Theta \subset \sum_1^s K e_j$. Let Θ_o and $u_i(\Theta_o)$ be the restrictions of Θ and $u_i(\Theta)$ to $V_o = \sum_1^s K e_j$. We must show that $||u_i(\Theta_o|| \leq r_1 \dots r_i$. Restricting the equation $(1-\Theta t)\cdot R_\Theta = D_\Theta$ to V_o we find that $(1-\Theta_o t)(1 + \sum u_i(\Theta_o)t^i) = \det (1-\Theta_o t)$. It follows that $u_i(\Theta_o)$ is the co-efficient of t^i in the adjoint transformation $(1-\Theta_o t)^A$ to $(1-\Theta_o t)$. Now the co-efficients of the matrix of $(1-\Theta_o t)^A$ are $(s-1) \times (s-1)$ sub-determinants of the matrix of $(1-\Theta_o t)$, and we may continue as in the proof of Theorem 6.4.

Theorem 6.6

Suppose $\Theta \in C(V,V)$. If $1-\Theta$ is injective, then it is invertible in $L(V,V)$.

Proof: The automorphism of $L(V,V)[t]$ mapping t on $t + 1$ is easily seen to extend to the algebra of entire power series over $L(V,V)$. Let

$\sum_0^\infty A_i t^i$ and $\sum_0^\infty a_i t^i$ be the images of R_Θ and D_Θ under this map. Since $R_\Theta \neq 0$, some $A_i \neq 0$. Let A_s be the first non-vanishing A. Now $(1-\Theta t)\cdot R_\Theta = D_\Theta$; it follows that $((1-\Theta) - \Theta t)\cdot\sum_0^\infty A^i t^i = \sum_0^\infty (a_i I)t^i$. Comparing co-efficients we find that $(1-\Theta)\cdot A_s = a_s I$. As $1-\Theta$ is injective, it's not a left zero-divisor in $L(V,V)$. Thus $a_s \neq 0$ and $(1-\Theta)\cdot(a_s^{-1}A_s) = I$. Since the A_j are limits of polynomials in Θ they commute with Θ; it follows that $(1-\Theta)$ is invertible.

Our next goal is to show that $1-\Theta$ *is invertible if and only if* $D_\Theta(1) \neq 0$. We need several lemmas.

<u>Lemma 6.1</u> Suppose $a \in K$. Then $\Theta \longrightarrow D_\Theta(a)$ is a continuous function $C(V,V) \longrightarrow K$.

<u>Proof</u>: We may suppose $a \neq 0$. Choose an orthonormal basis $\{e_i\}$ of V. If $\Theta \in C(V,V)$ let M be the matrix of Θ and $r_1 \geq r_2 \geq \dots$ the sequence of norms of row vectors of M arranged in order of decreasing size. Let Θ' be a second element of $C(V,V)$, and define M' and r_i' in a similar way. We must show that as $M' \longrightarrow M$, $\sum_1^\infty a^i c_i(\Theta') \longrightarrow \sum_1^\infty a^i c_i(\Theta)$. Given an $\varepsilon > 0$ choose j so large that $\prod_1^j \max(r_i, \frac{1}{2a}) \leq \frac{\varepsilon}{a^j}$, and $r_j \leq \frac{1}{a}$. Suppose $||\Theta' - \Theta|| \leq \frac{1}{2a}$. Then, $r_i' \leq \max(r_i, \frac{1}{2a})$, so $\prod_1^k r_i' \leq \frac{\varepsilon}{a^k}$ for all $k \geq j$. By Theorem 6.4, $||a^k c_k(\Theta')|| \leq \varepsilon$ for all $k \geq j$, and the same estimate holds for $||a^k c_k(\Theta)||$. By taking Θ' sufficiently close to Θ we can make $||a^k c_k(\Theta') - a^k c_k(\Theta)|| \leq \varepsilon$ for all $k < j$; the lemma follows.

Lemma 6.2

(1) If $\theta, \theta' \in C(V,V)$ then $D_\theta(a) \cdot D_{\theta'}(a) = D_{\theta+\theta'-a\theta\theta'}(a)$

(2) Suppose $g \in K[X]$ has constant term 0; let $1-g = \Pi(1-\alpha_i X)$, α_i algebraic over K. Then for $\theta \in C(V,V)$, $D_{g(\theta)}(1) = \Pi\, D_\theta(\alpha_i)$

Proof: By Lemma 6.1, it suffices to prove (1) when θ and θ' have finite dimensional image. Let W be a finite dimensional space containing image θ and image θ', and φ and φ' be the restrictions of θ and θ' to W. Then $\det(1-a\varphi) \cdot \det(1-a\varphi') = \det(1-a\varphi-a\varphi' + a^2\varphi\varphi')$ and (1) follows easily. The proof of (2) is similar.

Theorem 6.7

Suppose $\theta \in C(V,V)$ and $a \in K$. Then $1-a\theta$ is invertible in $L(V,V)$ if and only if $D_\theta(a) \neq 0$.

Proof: Suppose first that $D_\theta(a) \neq 0$. Substituting $t = a$ in the relation $(1-\theta t) \cdot R_\theta(t) = D_\theta(t)$ we find that $1-a\theta$ is invertible. Conversely suppose $1-a\theta$ is invertible; let $1-a\theta'$ be the inverse. Then $\theta + \theta' - a\theta\theta' = 0$. Since $C(V,V)$ is a 2-sided ideal in $L(V,V)$, $\theta' \in C(V,V)$. By Lemma 6.2, $D_\theta(a) \cdot D_{\theta'}(a) = D_0(a) = 1$, and $D_\theta(a) \neq 0$.

Theorem 6.8

Suppose $\theta \in C(V,V)$ and $f \in K[t]$ with constant term $\neq 0$. The following conditions are equivalent:

(1) $f(\theta)$ is injective

(2) $f(\theta)$ is invertible in $L(V,V)$

(3) $D_\Theta(u^{-1}) \neq 0$ for each root u of f in the algebraic closure of K.

Proof: We may assume that the constant term of f is 1; let $f = 1-g$. Then $g(\Theta) \in C(V,V)$ and (1) and (2) are equivalent by Theorem 6.6. By Theorem 6.7, $f(\Theta)$ is invertible if and only if $D_{g(\Theta)}(1) \neq 0$; now apply the second part of Lemma 6.2.

The following notation will be convenient. If $f = t^n + a_1 t^{n-1} + \ldots + a_n$ is a monic element of $K[t]$ with $a_n \neq 0$ set $f^* = t^n f(t^{-1}) = 1 + a_1 t + \ldots + a_n t^n$. f^* is irreducible if and only if f is, and the roots of f^* are the reciprocals of the roots of f. From Theorem 6.8 we immediately get:

Corollary Suppose $\Theta \in C(V,V)$ and $f \neq t$ is a monic irreducible element of $K[t]$. Then $f(\Theta)$ injective $\Longleftrightarrow$ $f(\Theta)$ bijective $\Longleftrightarrow$ $\mathrm{ord}_{f^*} D_\Theta = 0$.

From now on we shall make use of the notation and results of the final part of Chapter 5, dealing with entire power series.

Lemma Suppose $\Theta \in C(V,V)$ and $f \neq t$ is a monic irreducible element of $K[t]$. Then:

(1) $N = \bigcup_{s=1}^{\infty} \ker f(\Theta)^s$ is finite dimensional

(2) $\dim N = (\deg f) \cdot \mathrm{ord}_{f^*} D_\Theta$

(3) $f(\Theta)$ induces a bijective map $V/N \longrightarrow V/N$

Proof: To prove (1) it suffices to give an upper bound for the dimension of a finite dimensional subspace N_0 of N. But every such N_0 is contained in a finite dimensional Θ-invariant subspace (since a finitely generated torsion module over $K[t]$ is finite over K). Thus we may assume $\Theta(N_0) \subset N_0$. Let $\{e_i\}$ be an orthonormal basis of V whose first j elements span N_0. The matrix M of Θ on $\{e_i\}$ has the form $\begin{vmatrix} M' & ? \\ 0 & M'' \end{vmatrix}$ where M' is the matrix of $\Theta|N_0$. Now M'' is evidently the matrix of some completely continuous operator $\bar{\Theta}$. The proof of Theorem 6.4 shows how to compute D_Θ and $D_{\bar{\Theta}}$ using finite submatrices of M and M''. In particular, we see easily that $D_\Theta = \det\,(1-t(\Theta|N_0)).D_{\bar{\Theta}}$.

Since $f(\Theta)^s$ annihilates N_0 for some s, the characteristic polynomial of $\Theta|N_0$ has the form f^{ℓ}. Then $\det(t-(\Theta|N_0)) = f^{\ell}$ and $\det\,(1-t(\Theta|N_0)) = (f^*)^{\ell}$. So $D_\Theta = (f^*)^{\ell} D_{\bar{\Theta}}$, $\ell \leq \mathrm{ord}_{f*}\, D_\Theta$ and $\dim N_0 = \ell\cdot\deg f$ is bounded above. To prove (2) and (3), repeat the above construction with N_0 replaced by N, now known to be finite dimensional. It's easy to see that V/N has the structure of Banach space with countable orthonormal basis and that Θ induces a completely continuous operator $\bar{\Theta}$ on V/N with matrix M''. $f(\Theta)$ is evidently injective on V/N. By Theorem 6.8 it's bijective proving (3). By the corollary $\mathrm{ord}_{f*} D_{\bar{\Theta}} = 0$; thus $\mathrm{ord}_{f*}(D_\Theta) = \ell$ and $\dim N = \ell\cdot\deg f = (\deg f)\cdot\mathrm{ord}_{f*} D_\Theta$.

<u>Theorem 6.9</u> (Serre)

Suppose $\Theta \in C(V,V)$ and $f \neq t$ is a monic irreducible element of $K[t]$. Then:

(1) $V = N_f \oplus W_f$ where N_f and W_f are Θ-invariant subspaces, N_f is finite dimensional, $f(\Theta)$ is nilpotent on N_f and bijective on W_f.

(2) For any $r > 0$ there are only finitely many f such that $N_f \neq 0$ and $\lambda(f^*) \geq r$

(3) $\dim N_f = (\deg f) \cdot \mathrm{ord}_{f^*} D_\Theta$.

<u>Remark</u>. Note that any decomposition $V = N \oplus W$ as in (1) is unique. For evidently, if such a decomposition exists, $N = \bigcup \ker f(\Theta)^s$ and $W = \bigcap \text{image } f(\Theta)^s$.

<u>Proof</u>: Let $T = f(\Theta)$. By the lemma, $N = \bigcup \ker T^s$ is finite dimensional and $T: V/N \longrightarrow V/N$ is bijective. Choose ℓ so that $T^\ell N = 0$. Since $T^\ell: V/N \longrightarrow V/N$ is bijective, $V = N + T^\ell V$ and one sees easily that the sum is direct. As T is bijective on V/N it is bijective on $T^\ell V$ proving (1). Since D_Θ is entire it admits a Weierstrass factorization, and there are only finitely many f with $\mathrm{ord}_{f^*} D_\Theta > 0$ and $\lambda(f^*) \geq r$. (2) follows immediately, and the lemma gives (3).

Our next goal is to show that the sum of the diagonal elements of the matrix of Θ is equal to the "sum of the eigenvalues" of Θ. For this purpose it's convenient to abstract Theorem 6.9 into a definition.

<u>Definition</u> Let U be a vector space (not necessarily a Banach space) over K and $\Theta: U \longrightarrow U$ a linear map. Θ is "nuclear" if it satisfies (1) and (2) of Theorem 6.9. If Θ is nuclear, then $\mathrm{Tr}_{nuc}(\Theta) = \Sigma\, \mathrm{Tr}\, (\Theta | N_f)$, the sum ranging over all monic irreducible $f \neq t$.

Note that the above sum converges. For if $f = t^n + a_1 t^{n-1} + \ldots + a_n$, then

$-\mathrm{Tr}(\theta|N_f) = (\frac{\dim N_f}{\deg f})\cdot a_1$. Thus $||\mathrm{Tr}(\theta|N_f)|| \leq ||a_1|| \leq \lambda(f^*)$, and $\mathrm{Tr}(\theta|N_f) \longrightarrow 0$. Observe also that if U is finite dimensional then any $\theta: U \longrightarrow U$ is nuclear with $\mathrm{Tr}_{nuc}(\theta) = \mathrm{Tr}(\theta)$. (In fact, the structure theorem for finitely generated torsion modules over $K[t]$ shows that $U = \bigoplus N_f$ where f ranges over the monic irreducible polynomials including t; the rest is easy).

Theorem 6.10

Let V be a Banach space admitting a countable orthonormal basis $\{e_i\}$ and θ an element of $C(V,V)$ with matrix $M = \{a_{ij}\}$ on $\{e_i\}$. Then θ is nuclear and $\mathrm{Tr}_{nuc}(\theta) = -c_1(\theta) = \sum_i a_{ii}$.

Proof: By Theorem 6.9, θ is nuclear and $D_\theta(t)$ has the Weierstrass factorization $\prod(f^*)^{\frac{\dim N_f}{\deg f}}$. Thus the co-efficient $c_1(\theta)$ of t in D_θ is just $\sum(\frac{\dim N_f}{\deg f})\cdot c_1(f^*)$, the sum extending over the monic irreducible $f \neq t$ in $K[t]$. By the paragraph above this is $-\mathrm{Tr}_{nuc}(\theta)$. Finally one proves that $-c_1(\theta) = \sum_i a_{ii}$ by approximating θ by a sequence in $C_{fin}(V,V)$.

Theorem 6.11

Let U be a complex $U_n \longrightarrow U_{n-1} \cdots \longrightarrow U_0$ of vector spaces over K and $\theta: U \longrightarrow U$ a chain map such that each θ_i is nuclear. Then each $(\theta_i)_*$ is nuclear and $\sum_0^n(-1)^j\,\mathrm{Tr}_{nuc}(\theta_j) = \sum_0^n(-1)^j\,\mathrm{Tr}_{nuc}(\theta_j)_*$.

Proof: For each monic irreducible $f \neq t$ in $K[t]$, U is the direct sum of the subcomplexes $N_f(U)$ and $W_f(U)$. Then $H_{\cdot}(U) = H_{\cdot}(N_f(U)) \oplus H_{\cdot}(W_f(U))$; the rest is easy.

Chapter 7 - Dwork's "Lefschetz Fixed Point Theorem"

Let U be a hypersurface $f(X_1,\cdots,X_n) = 0$ of degree d in projective n-1 space over $k = GF(q)$. What can be said about $N_s(U)$? In Chapter 2 we computed $N_s(U)$ for certain diagonal hypersurfaces. In the next two chapters we shall develop a similar result for arbitrary non-singular U :

$$N_s(U) = \frac{q^{(n-1)s}-1}{q^s - 1} + (-1)^n \sum_1^{\ell} \gamma_i^{\ s}$$

where the γ_i are algebraic integers $\neq 0$ and $\ell = d^{-1}\{(d-1)^n + (-1)^n (d-1)\}$. The proof will be similar to that given by Dwork in [3].

As in the case of diagonal hypersurfaces, the above result is in agreement with Weil's conjecture (d), and the γ_i are presumably the eigenvalues of the Frobenius on some sort of $H^{n-2}(U)$. Thus $\gamma \longrightarrow \frac{q^{n-2}}{\gamma}$ should be a permutation of the γ_i. This result has also been proved by Dwork, in [4]. Proofs have been given by Grothendieck and Lubkin too, but they're all very difficult. One expects furthermore that $|\gamma_i| = q^{\frac{n-2}{2}}$, but except for such special cases as diagonal hypersurfaces this remains unproven.

We adopt the notation of Chapter 4. K is the extension of Q_p generated by π and the roots of $X^q = X$, where $\pi^{p-1} = -p$. K is discretely normed with residue class field $k = GF(q)$, and π generates the maximal ideal of $\mathcal{O}_K$. Normalize the norm in K so that $||p|| = p^{-1}$. Let f be an element of $k[X_1,\cdots,X_n]$, homogeneous of degree d and U be the projective hypersurface defined by f. We put no restrictions on U in this chapter. Let F be the Teichmüller lifting of F to $\mathcal{O}_K[X_1,\cdots,X_n]$, $G = X_0F$, $H = \exp\ \pi\{G(X)-G(X^q)\}$ and $H_s = \exp\ \pi\{G(X)-G(X^{q^s})\}$.

Suppose now that γ is a positive real number. Let $L(\gamma)$ denote the Banach space contained in $K[[X_0,\cdots,X_n]]$ and having as orthonormal basis the elements $\pi^{[\gamma\lambda_0]} X^\lambda$ with $d\lambda_0 = \sum_1^n \lambda_i$. (In other words $L(\gamma)$ consists of infinite K-linear combinations of these elements with co-efficients $\longrightarrow 0$). We write L for $L(1)$.

Lemma 7.1 $H \in L(\gamma)$ for $\gamma < \frac{(p-1)^2}{pq}$

Proof: Whenever a_λ is a non-zero co-efficient in $G(X)$ or $G(X^q)$, $d\lambda_0 = \sum_1^n \lambda_i$. It follows that $d\lambda_0=\sum_1^n \lambda_i$ for every non-zero co-efficient c_λ of H . Now set $q = p^r$, write $G = \Sigma\, a_\lambda X^\lambda$ and note that $\lambda_0 = 1$ for each a_λ . We see immediately that $H = \Pi\, \Theta_r(a_\lambda X^\lambda)$. By Theorem 4.1, $||\, c_\lambda || \le p^{-\frac{(p-1)}{pq}\lambda_0} = ||\pi||^{\frac{(p-1)^2}{pq}\lambda_0}$. The lemma follows.

In Chapter 4 we introduced an operator $\psi \circ H$ on $K[[X_0,\cdots,X_n]]$ whose matrix M had remarkable properties. (See Theorem 4.8). We shall show that $\psi \circ H$ is a nuclear operator on certain of the $L(\gamma)$. Write Θ for $\psi \circ H$.

Theorem 7.1

For $0 < \gamma < \frac{(p-1)^2}{p}$, $L(\gamma)$ is stable under Θ, and $\Theta \in C\ (L(\gamma)\ , L(\gamma))$. If M is the matrix of Θ on $\{X^\lambda\}$ in the sense of Theorem 4.8, then for all s $\mathrm{Tr}_{\mathrm{nuc}}(\Theta^s | L(\gamma)) = \mathrm{Tr}\ M^s$.

Proof: By Lemma 7.1 $H \in L(\frac{\gamma}{q})$. Now $L(\frac{\gamma}{q})$ is closed under multiplication; furthermore ψ maps $L(\frac{\gamma}{q})$ into $L(\gamma)$. Thus $(\psi \circ H)\ L(\frac{\gamma}{q}) \subset L(\gamma)$ and $L(\gamma)$ is stable under Θ. Also, $\Theta\colon L(\gamma) \longrightarrow L(\gamma)$ is the composite map $L(\gamma) \subset L(\frac{\gamma}{q}) \xrightarrow{H} L(\frac{\gamma}{q}) \xrightarrow{\psi} L(\gamma)$. Now the inclusion map $L(\gamma) \subset L(\gamma/q)$ is represented by a diagonal matrix whose entries $\longrightarrow 0$, and is thus a uniform limit of continuous maps with finite dimensional image. Also H and ψ are easily seen to be continuous. It follows that Θ is completely continuous. Now let $M = \{c_{\lambda\mu}\}$ be the matrix of Θ in the sense of Theorem 4.8; $\Theta(X^\mu) = \sum_\lambda c_{\lambda\mu} X^\lambda$. Using Lemma 7.1 we see readily that $c_{\lambda\lambda} = 0$ unless $d\lambda_0 = \sum_1^n \lambda_i$. If $d\lambda_0 = \sum_1^n \lambda_i$ let $Y^\lambda = \pi^{[\gamma\ \lambda_0]} X^\lambda$ and let $\{a_{\lambda\mu}\}$ be the matrix of $\Theta | L(\gamma)$ on the orthonormal basis $\{Y^\lambda\}$. Then $\Theta(Y^\mu) = \sum_\lambda a_{\lambda\mu} Y^\lambda$. It follows that $a_{\lambda\mu} = \pi^{[\gamma\mu_0] - [\gamma\lambda_0]} c_{\lambda\mu}$. In particular, $a_{\lambda\lambda} = c_{\lambda\lambda}$, and $\mathrm{Tr}_{\mathrm{nuc}}\ (\Theta | L(\gamma)) = \Sigma\, a_{\lambda\lambda} = \Sigma\, c_{\lambda\lambda} = \mathrm{Tr}\ M$. Replacing H by H_s and arguing similarly, we complete the proof.

In particular, if $p \neq 2$, $1 < \frac{(p-1)^2}{p}$ and Theorem 7.1 holds for $L = L(1)$. For the time being we assume $p \neq 2$; the modifications necessary to build a good nuclear operator on L for p = 2 will be discussed at the end of the Chapter.

Combining Theorems 7.1 and 4.8 we find:

Theorem 7.2

Let V^* be the affine variety defined by the equations $f(X_1,\cdots,X_n) = 0$, $\prod_1^n X_i \neq 0$. Then $q N_1(V^*) = (q-1)^n + (q-1)^{n+1} \operatorname{Tr}_{nuc}(\Theta|L)$.

Our next goal is to transform Theorem 7.2 into a formula for $N_1(U)$. We need to introduce certain closed subspaces of L, stable under Θ.

Definition If $\lambda = (\lambda_0,\cdots,\lambda_n)$ is an n+1 tuple with $d\lambda_0 = \sum_1^n \lambda_i$, then Y^λ is the element $\pi^{\lambda_0} X^\lambda$ of L. If A is a subset of $\{1,2,\cdots n\}$ let L_A be the closed subspace of L having as orthonormal base the Y^λ such that $\lambda_i > 0$ for all $i \in A$. Similarly, let L^A be the closed subspace having as orthonormal base the Y^λ such that $\lambda_i > 0$ for some $i \in A$. Let $\bar{A} = \{1,2,\cdots n\} - A$, $a = \operatorname{card} A$ and $\bar{a} = \operatorname{card} \bar{A}$.

The above construction can be generalized a little. Let S_j $(1 \leq j \leq n)$ be $\{Y^\lambda | \lambda_j > 0\}$. Let $\mathscr{A}$ be the ring of sets generated by the S_j, i.e. take unions and intersections of the S_j in all possible ways. If $X \in \mathscr{A}$, let $L(X)$ be the closed subspace of L having the elements of X as orthonormal basis; thus $L_A = L(\bigcap_A S_j)$ while $L^A = L(\bigcup_A S_j)$. Using the explicit definition of ψ we see that each $L(X)$ is stable under Θ. The matrix of $\Theta|L(X)$ is a submatrix of the matrix of Θ; thus $\Theta|L(X)$ is completely continuous, and hence nuclear.

Lemma 7.2 If A is a subset of $\{1,2,\cdots,n\}$ then Θ is nuclear both on L_A and L/L^A. Furthermore, $Tr_{nuc}(\Theta|L/L^B) = \sum_{A\subset B} (-1)^a Tr_{nuc}(\Theta|L_A)$.

Proof: If X is an element of $\mathscr{S}$ let $\varphi(X) = Tr_{nuc}(\Theta|L(X))$. An easy matrix calculation shows that $\varphi(X_1 \cup X_2) = \varphi(X_1) + \varphi(X_2) - \varphi(X_1 \cap X_2)$. By induction $\varphi(\bigcup_1^{\ell} X_i) = \sum_{1\leq i\leq \ell} \varphi(X_i) - \sum_{1\leq i<j\leq \ell} \varphi(X_i \cap X_j) + \cdots$. In particular, $Tr_{nuc}(\Theta|L^B)$

$= \sum_{\substack{A\subset B\\ A\neq\emptyset}} (-1)^{a+1} Tr_{nuc}(\Theta|L_A)$. Since $Tr_{nuc}(\Theta|L/L^B) = Tr_{nuc}(\Theta|L) - Tr_{nuc}(\Theta|L_B)$, and $L = L_{\emptyset}$, the lemma follows.

Definition If A is a subset of $\{1,2,\cdots,n\}$, let $V^*_{(A)}$ be the affine variety defined by the equations $f(X_1,\cdots,X_n) = 0$, $X_i = 0$ for $i \in A$, $X_i \neq 0$ for $i \in \bar{A}$.

Lemma 7.3 $qN_1(V^*_{(A)}) = (q-1)^{\bar{a}} + (q-1)^{\bar{a}+1} Tr_{nuc}(\Theta|L/L^A)$

Proof: Let $f_{(A)}$ be the polynomial obtained from f by replacing X_i by 0 for $i \in A$. Then $V^*_{(A)}$, thought of as a variety in affine $\bar{a}$ - space, is defined by the equations $f_{(A)} = 0$, $\prod_{i\in\bar{A}} X_i \neq 0$. We shall apply Theorem 7.2 with f replaced by $f_{(A)}$ and n replaced by $\bar{a}$. Define $F_{(A)}$, $G_{(A)}$, $H_{(A)}$, $L_{(A)}$ and $\Theta_{(A)}$ using $f_{(A)}$ in the same way that F, G, H, L and Θ were defined using f. Evidently

$H_{(A)}$ is obtained from H by replacing X_i by 0 for $i \in A$. Also $L_{(A)}$ may be viewed as spanned by those Y^λ such that $\lambda_i = 0$ for all $i \in A$; in other words $L_{(A)} \approx L/L^A$. Under this identification the operator Θ on L induces $\Theta_{(A)}$ on $L_{(A)}$. Theorem 7.2 then gives the desired result. {The above argument fails when $A = \{1,2,\cdots n\}$. But in this case $L/L^A \approx K$, Θ induces the identity map on L/L^A and the lemma reduces to $q = 1 + (q-1)$}.

<u>Lemma 7.4</u> Let U be the projective hypersurface defined by f. Then:

$$(1) \quad N_1(U) = \frac{q^{n-1}-1}{q-1} + q^{-1} \sum_A (q-1)^{\bar{a}} \operatorname{Tr}_{nuc}(\Theta|L/L^A)$$

$$(2) \quad N_1(U) = \frac{q^{n-1}-1}{q-1} + \frac{(-1)^n}{q} \sum_A (-1)^{\bar{a}} q^{\bar{a}} \operatorname{Tr}_{nuc}(\Theta|L_A)$$

<u>Proof</u>: The union of the $V^*_{(A)}$ is the affine hypersurface $f(X_1,\cdots,X_n) = 0$. Thus $(q-1)N_1(U) = -1 + \sum_A N_1(V^*_{(A)})$. Multiplying by q and applying Lemma 7.3 we find:

$$q(q-1)N_1(U) = -q + \{(q-1) + 1\}^n + \sum_A (q-1)^{\bar{a}+1} \operatorname{Tr}_{nuc}(\Theta|L/L^A)$$

Dividing by $q(q-1)$ we get (1). Now, by Lemma 7.2, $\sum_B (q-1)^{\text{card } \bar{B}} \operatorname{Tr}_{nuc}(\Theta|L/L^B) =$

$\sum_A r_A \operatorname{Tr}_{nuc}(\Theta|L_A)$ where $r_A = \sum_{B \supset A} (-1)^a (q-1)^{\text{card } \bar{B}}$. But this sum is just $(-1)^a \cdot \{(q-1) + 1\}^{\bar{a}} = (-1)^n \cdot (-1)^{\bar{a}} \cdot q^{\bar{a}}$. Substituting in (1), we get (2).

Now let K^n be an n-dimensional vector space over K with basis $\{e_i\}$.

Then $L \otimes_K \Lambda K^n$ has the structure of graded Banach space over K, and Θ operates on this space via its action on L. Let $\hat{\mathcal{L}}$ be the closed graded subspace

$$\Sigma \; L_{\overline{(i_1,\cdots i_s)}} \; e_{i_1} \wedge \cdots \wedge e_{i_s}$$

of $L \otimes_K \Lambda K^n$, the sum extending over all subsets $\{i_1,\cdots,i_s\}$ of $\{1,2,\cdots,n\}$.

Since each L_A is stable under Θ, $\hat{\mathcal{L}}$ is stable under Θ. Define a map $\alpha\colon \hat{\mathcal{L}} \to \hat{\mathcal{L}}$ by setting $\alpha_i = q^i \Theta$.

<u>Theorem</u> <u>7.3</u>

α_i is nuclear on $\hat{\mathcal{L}}_i$ and:

$$N_1(U) = \frac{q^{n-1}-1}{q-1} + \frac{(-1)^n}{q} \sum_{j=0}^{n} (-1)^j \, \mathrm{Tr}_{\mathrm{nuc}}\, \alpha_j .$$

More generally for every s we have:

$$N_s(U) = \frac{q^{(n-1)s}-1}{q^s-1} + \frac{(-1)^n}{q^s} \sum_{j=0}^{n} (-1)^j \, \mathrm{Tr}_{\mathrm{nuc}}\, \alpha_j^{\,s}$$

<u>Proof</u>: The first result is immediate from Lemma 7.4 (2) and the definitionsof $\hat{\mathcal{L}}$ and α. (Note that $\hat{\mathcal{L}}_i \approx \bigoplus_{\overline{a=i}} L_A$). The proof of the second result is similar.

Theorem 7.3 looks rather like a Lefschetz fixed point theorem "on the chain level." Our next goal is to make the graded Banach space $\hat{\mathcal{L}}$ into a complex in such a way that α becomes a chain map. Then a result analogous to Theorem 7.3 will hold on the

homology level and if we can compute the homology of $\hat{\mathcal{L}}$. we'll get information about $N_s(U)$.

Definition For $1 \leq i \leq n$, D_i is the operator $(\exp -\pi G) \circ X_i \frac{\partial}{\partial X_i} \circ (\exp \pi G)$ on $K[[X_0, \cdots, X_n]]$

Theorem 7.4

(1) The D_i commute with one another

(2) $D_i(L) \subset L$

(3) $\Theta \circ D_i = q\, D_i \circ \Theta$

Proof: (1) holds because the maps $X_i \frac{\partial}{\partial X_i}$ commute. To prove (2) note that $D_i(\varphi) = X_i \frac{\partial \varphi}{\partial X_i} + \pi\, X_i \frac{\partial G}{\partial X_i} \cdot \varphi$. Since L is stable under $X_i \frac{\partial}{\partial X_i}$ and $X_i \frac{\partial G}{\partial X_i} \varepsilon\, L$, L is stable under D_i. To prove (3) note that $\Theta = \psi \circ H = (\exp -\pi G) \circ \psi \circ (\exp \pi G)$. So it suffices to show that $\psi \circ X_i \frac{\partial}{\partial X_i} = qX_i \frac{\partial}{\partial X_i} \circ \psi$ and this is easy.

Using (1) and (2) of Theorem 7.4 we can put a "Koszul complex" structure on $L \underset{K}{\otimes} \Lambda K^n$. Namely let $\partial\, a(e_{i_0} \wedge \cdots \wedge e_{i_s}) = \sum_{j=0}^{n} (-1)^j D_{i_j}(a)(e_{i_0} \wedge \cdots \wedge \hat{e}_{i_j} \wedge \cdots e_{i_s})$.

Using (1) we see that $\partial^2 = 0$.

Theorem 7.5

$\hat{\mathcal{L}}$. is a subcomplex of $L \underset{K}{\otimes} \Lambda K^n$ and $\alpha: \hat{\mathcal{L}}. \longrightarrow \hat{\mathcal{L}}.$ is a chain map. If α_* is the map on homology induced by α we have the "Lefschetz fixed point theorem":

$$N_s(U) = \frac{q^{(n-1)s}-1}{q^s-1} + \frac{(-1)^n}{q^s} \sum_{j=0}^{n} (-1)^j \, Tr_{nuc} \, (\alpha_j)^s_*$$

Proof: Since $D_i(\varphi) = X_i \frac{\partial\varphi}{\partial X_i} + \pi X_i \frac{\partial G}{\partial X_i} \cdot \varphi$, we find that D_i maps

$L_{\overline{A \cup \{i\}}}$ into $L_{\overline{A}}$. So $\partial(\hat{\mathcal{L}}.) \subset \hat{\mathcal{L}}.$ By Theorem 7.4,(3) the diagrams

$$\begin{array}{ccc} L & \xrightarrow{D_i} & L \\ q^{j+1}\,\theta \downarrow & & \downarrow q^j\,\theta \\ L & \xrightarrow{D_i} & L \end{array}$$

all commute. It follows that α is a chain map.

The final result follows from Theorems 7.4 and 6.11.

In the same way that we built a complex of Banach spaces $(\hat{\mathcal{L}}. , \partial)$ using L we may for each $\gamma > 0$ build a complex of Banach spaces $(\hat{\mathcal{L}}.(\gamma),\partial)$, using $L(\gamma)$. For $0 < \gamma < \frac{(p-1)^2}{p}$ we get a chain map $\alpha\colon \hat{\mathcal{L}}.(\gamma) \longrightarrow \hat{\mathcal{L}}.(\gamma)$.

Theorem 7.5 remains true with L and $\hat{\mathcal{L}}.$ replaced by $L(\gamma)$ and $\hat{\mathcal{L}}.(\gamma)$. Unfortunately for $p = 2$ we must assume $\gamma < \frac{1}{2}$. We next show how to get around this restriction by modifying the definition of α and ∂ when $p = 2$.

Lemma 7.5 Over Q_2, $\exp\,(X + \frac{X^2}{2} + \frac{X^4}{4} + \frac{X^8}{8}) \in S(\frac{-5}{16})$

Proof: By Lemma 4.2, $\exp X = \prod_{n\geq 1} (1-X^n)^{\frac{-\mu(n)}{n}} = \prod_{n \text{ odd}} (1-X^n)^{\frac{-\mu(n)}{n}} (1-X^{2n})^{\frac{\mu(n)}{2n}}$.

Thus, $\exp\left(X + \frac{X^2}{2} + \frac{X^4}{4} + \frac{X^8}{8}\right) = \prod_{n \text{ odd}} (1-X^n)^{\frac{-\mu(n)}{n}} (1-X^{16n})^{\frac{\mu(n)}{16n}}$

and we may apply Lemma 4.3.

__Lemma 7.6__ Let $g = -X + 2X^2 + 16X^4$. Then, over Q_2:

(1) $\exp -2\,(g(X) - g(X^2)) \in S\left(\frac{11}{16}\right)$

(2) $\exp -2\,(g(X) - g(X^q)) \in S\left(\frac{11}{8q}\right)$, q a power of 2

__Proof:__ Replacing X by $2X$ in Lemma 7.5, we find that $\exp(2X + 2X^2 + 4X^4 + 32X^8) \in S\left(\frac{11}{16}\right)$. Now $\exp -8X^2$ and $\exp -32X^4$ are both in $S(1)$. It follows that $\exp(2X - 6X^2 - 28X^4 + 32X^8) \in S\left(\frac{11}{16}\right)$. But this is just $\exp -2\,(g(X) - g(X^2))$.

To prove (2), let $q = 2^r$, $\Phi_r(X) = \exp -2\,(g(X) - g(X^q))$ and $\Phi(X) = \Phi_1(X)$.

Then $\Phi_r(X) = \prod_{i=0}^{r-1} \Phi(X^{2^i})$, and the result follows.

If G is a polynomial and s a positive integer let $G^{(s)}$ be the polynomial obtained by raising every co-efficient of G to the s'th power. Now let $k = GF(q)$, $q = 2^r$ and let $f \in k[X_1, X_2, \cdots, X_n]$ be homogeneous of degree d. Define K, F and G as was done at the beginning of this chapter. Set $G' = -G + 2\,G^{(2)}(X^2) + 16\,G^{(4)}(X^4)$, and let $H' = \exp -2\,\{G'(X) - G'(X^q)\}$

Lemma 7.7 $H' \in L(\gamma)$ for $\gamma < \frac{11}{8q}$

Proof: For every non-zero co-efficient c_λ of H', $d\lambda_0 = \sum_1^n \lambda_i$; the proof is similar to that of Lemma 7.1. Let $G = \Sigma a_\lambda X^\lambda$. A brief calculation shows that $H' = \Pi \Phi_r (a_\lambda X^\lambda)$ with Φ_r defined as in Lemma 7.6. Since $\lambda_0 = 1$ for each a_λ , Lemma 7.6 shows that $|| c_\lambda || \leq 2^{\frac{-11}{8q}\lambda_0}$. The lemma follows.

Now let Θ' be the operator $\psi \circ H'$ on $K[[X_0, \cdots X_n]]$.

Lemma 7.8

(a) For $0 < \gamma < \frac{11}{8}$, $L(\gamma)$ is stable under Θ' , and $\Theta' \in C(L(\gamma), L(\gamma))$

(b) $\mathrm{Tr}_{nuc} (\Theta'^s | L(\gamma))$ is independent of γ

(c) For $0 < \gamma < \frac{1}{2}$, $\mathrm{Tr}_{nuc}(\Theta'^s | L(\gamma)) = \mathrm{Tr}_{nuc} (\Theta^s | L(\gamma))$

Proof: (a) follows from Lemma 7.7 in the same way that Theorem 7.1 followed from Lemma 7.1. (b) is a simple matrix calculation using the orthonormal basis $\{2^{[\gamma\lambda_0]} X^\lambda\}$ of $L(\gamma)$. To prove (c), let $R = \exp 2(G'-G)$. Evidently $R \in L(\gamma)$ for $\gamma < \frac{1}{2}$. Since $\Theta' = (\exp 2G') \circ \psi \circ (\exp -2G')$ while $\Theta = (\exp 2G) \circ \psi \circ (\exp -2G)$ $\Theta' = R \circ \Theta \circ R^{-1}$. But multiplication by R is an invertible linear transformation of $L(\gamma)$, and (c) follows.

Now θ' operates on $L \otimes_K \Lambda K^n$ via its action on L and it's easily seen that $\mathcal{L}$. is stable under θ'. Define a map $\alpha': \mathcal{L}. \longrightarrow \mathcal{L}.$ by taking $\alpha_i' = q^i \theta'$.

Then:

Theorem 7.7

Theorem 7.3 holds with α replaced by α'.

Proof: Since $p = 2$, Theorem 7.3 is not true as stated, but it is true if $\hat{\mathcal{L}}.$ is replaced by $\hat{\mathcal{L}}.(\gamma)$ with $0 < \gamma < \frac{1}{2}$. Now an easy modification of the proof of Lemma 7.8 (b) and (c) shows that $\mathrm{Tr}_{nuc}(\theta'^s|\hat{\mathcal{L}}_i) = \mathrm{Tr}_{nuc}(\theta'^s|\hat{\mathcal{L}}_i(\gamma)) = \mathrm{Tr}_{nuc}(\theta^s|\hat{\mathcal{L}}_i(\gamma))$. The theorem follows.

Now let D_i, $(1 \le i \le n)$, be the operator $(\exp 2G') \circ X_i \frac{\partial}{\partial X_i} \circ (\exp -2G')$ on $K[[X_0, \ldots, X_n]]$. Then Theorem 7.4 remains true with θ and D_i replaced by θ' and D_i'. Since the D_i' commute we may build a Koszul complex with underlying space $L \otimes_K \Lambda K^n$. Then $\Sigma\, L_{\overline{\{i_1, \cdots i_s\}}}\; e_{i_1} \wedge \cdots \wedge e_{i_s}$ is a subcomplex of this complex, and we denote it by $\hat{\mathcal{L}}.'$. The same proof that gave Theorem 7.5 gives:

Theorem 7.8

α' is a chain map $\hat{\mathcal{L}}.' \longrightarrow \hat{\mathcal{L}}.'$. If α'_* is the map on homology induced by α' we have the "Lefschetz fixed point theorem":

$$N_s(U) = \frac{q^{(n-1)s}-1}{q^s - 1} + \frac{(-1)^n}{q^s} \sum_{j=0}^{n} (-1)^j \, \mathrm{Tr}_{nuc}\, (\alpha_j')_*^s$$

We conclude this chapter by defining first an algebraic analogue to, and second a slight generalization of, the complex $\hat{\mathcal{L}}$.

<u>Definition</u> Let k be a field (of arbitrary characteristic), and $f \in k[X_1, \cdots X_n]$ be homogeneous of degree d. Build a complex $\mathcal{L}.$ in the following way. Let L be the subspace of $k[X_0, \cdots, X_n]$ spanned by X^λ with $d\lambda_0 = \sum_1^n \lambda_i$. If $A \subset \{1,2, \cdots n\}$, let L_A be the subspace of L spanned by those X^λ such that $\lambda_i > 0$ for all $i \in A$. Let $g = X_0 f$ and $D_i : L \longrightarrow L$ be the commuting operators $\varphi \longrightarrow X_i \dfrac{\partial \varphi}{\partial X_i} + X_i \dfrac{\partial g}{\partial X_i} \cdot \varphi$. Then $\mathcal{L}.$ is the subcomplex

$$\Sigma\, L_{\{i_1, \cdots i_s\}}\, e_{i_1} \wedge \cdots \wedge e_{i_s}$$

of the Koszul complex built on $L \otimes_k \Lambda k^n$ using the operators D_i, $(1 \leq i \leq n)$.

In Chapter 8 we shall compute the homology of $\mathcal{L}.$, assuming that $d \neq 0$ in k and that f defines a non-singular projective hypersurface. In Chapter 9, assuming characteristic $k = 0$, we shall relate the homology of $\mathcal{L}.$ to De Rham cohomology.

<u>Definition</u> Let K be a complete discretely normed field of characteristic 0 whose residue class field has characteristic $p > 0$. Assume further that there is an element π of K such that $\pi^{p-1} = -p$. Let F be a homogeneous element of $\mathcal{O}_K[X_1, \cdots X_n]$ of degree d. Set $G = X_0 F$ and build a complex $\hat{\mathcal{L}}.$ from G just as was done in this chapter. (The finiteness of $\overline{K}$ and the fact that the

co-efficients of F satisfy $c^q = c$ were only used in defining the map α).

In Chapter 8, we shall compute the homology of $\hat{\mathcal{L}}.$ assuming that the reduction $\bar{F}$ of F defines a non-singular projective hypersurface. In Chapter 9 we shall discuss the connections between the homology of $\hat{\mathcal{L}}.$ and the "formal cohomology theory" constructed by Washnitzer and me.

Chapter 8 - Non-Singular Hypersurfaces

In order to calculate the $H_i(\mathcal{L}.)$ and the $H_i(\hat{\mathcal{L}}.)$ we shall need to make extensive use of "Koszul complexes." Let A be an additive group and $\varphi_i (1 \leq i \leq n)$ be commuting endomorphisms of A. Then the graded group $A \otimes_Z \Lambda Z^n$ can be given the structure of a complex, just as in the construction following Theorem 7.4. We denote this complex by $K.(A;\varphi_1,\cdots,\varphi_n)$ and its homology by $H.(A;\varphi_1,\cdots,\varphi_n)$. The following well known fact is useful.

<u>Lemma 8.1</u> Suppose $\varphi_1: A \longrightarrow A$ is injective. Then $H_i(A;\varphi_1,\cdots,\varphi_n) \approx H_i(A/\varphi_1(A);\ \varphi_2,\cdots,\varphi_n)$ for all i.

We shall say that $\varphi_1,\varphi_2,\cdots,\varphi_n$ is a prime sequence on A if

$\varphi_s: A/\sum_1^{s-1} \varphi_i(A) \longrightarrow A/\sum_1^{s-1} \varphi_i(A)$ is injective for $1 \leq s \leq n$. Repeated applications of Lemma 8.1 give:

<u>Lemma 8.2</u> If $\varphi_1,\cdots,\varphi_n$ is a prime sequence on A, then $H_i(A;\varphi_1,\cdots\varphi_n) = 0$ for all $i \geq 1$.

We proceed to give an alternative description of the complex $\mathcal{L}.$ constructed at the end of Chapter 7. Let k be a field, $k[X]$ denote $k[X_1,\cdots,X_n]$ and f be a fixed element of $k[X]$, homogeneous of degree d. If $\varphi \in k[X]$ write φ_i for $\frac{\partial\varphi}{\partial X_i}$ and let Δ_i be the operator $\varphi \longrightarrow \varphi_i + f_i\varphi$ on $k[X]$. As the Δ_i commute we can form a Koszul complex, $K.(k\,[X]\ ;\Delta_1,\cdots,\Delta_n)$, or more briefly, $K.(k[X])$.

The spaces $H_i(k[X];\ \Delta_1,\cdots,\Delta_n)$ are invariant under linear change of co-ordinates.

More precisely let $T: X_i \longrightarrow \Sigma\, a_{ij} X_j$ be an invertible change of co-ordinates over k. Then T induces an isomorphism between the homology groups of the complexes $K.(k[X])$ constructed from f and $f \circ T$. One way of seeing this is by giving an alternative description of $K.(k[X])$. Let $(\Omega^{\cdot}, d)$ be the co-complex of k linear differential forms on $k[X]$, d being the exterior differentiation map. Define a new degree 1 co-boundary map Δ on $\Omega^{\cdot}$ by $\Delta(\omega) = d\omega + df \wedge \omega$. With the obvious renumbering of dimension to change a complex into co-complex, $K.(k[X]) \approx (\Omega^{\cdot}, \Delta)$. But $\Omega^{\cdot}$ is evidently invariant under linear change of co-ordinates.

If j is a integer let $k[X]^{(j)}$ be the subspace of $k[X]$ spanned by monomials of degree $\equiv j$ (d). The operators Δ_i map $k[X]^{(j)}$ into $k[X]^{(j-1)}$. It follows that $K.(k[X])$ may be written as a direct sum of d subcomplexes. We shall be particularly interested in the subcomplex $\sum_{\substack{0 \leq s \leq n \\ i_1, \cdots, i_s}} k[X]^{(s-n)} e_{i_1} \wedge \cdots \wedge e_{i_s}$.

We denote this complex by $\mathcal{L}.(f)$ and its homology by $H.(f)$. The $H_i(f)$ are invariant under a change of co-ordinates $X_i \longrightarrow \Sigma\, a_{ij} X_j$.

Theorem 8.1

$\mathcal{L}.(f)$ is isomorphic with the complex $\mathcal{L}.$ constructed at the end of Chapter 7.

Proof: Let $A = \{i_1, \cdots i_s\}$ be a subset of $\{1, 2, \cdots, n\}$ of cardinality s. There is a vector space isomorphism $k[X]^{(s-n)} \approx I_{\bar{A}}$ mapping X^λ on $X_0^j \cdot (\prod_{i \in \bar{A}} X_i) \cdot X^\lambda$ where $j = \frac{|\lambda| + n - s}{d}$. Putting these maps together we get a vector space isomorphism between $\mathcal{L}_\bullet(f)$ and $\mathcal{L}_\bullet$. It only remains to show that this a chain map, and this follows from the fact that the following diagram commutes:

$$\begin{array}{ccc}
k[X]^{(s-n)} & \xrightarrow{\approx} & L_{\{i_1,\cdots i_s\}} \\
\Delta_{i_s}\big\downarrow & & \big\downarrow D_{i_s} \\
k[X]^{(s-1-n)} & \xrightarrow{\approx} & L_{\{i_1,\cdots i_{s-1}\}}
\end{array}$$

An alternative description of $\hat{\mathcal{L}}_\bullet$ may also be given. Let K be a complete discretely normed field of characteristic 0 , and k be the residue class field of K . Let F be a fixed homogeneous element of degree d of $\mathcal{O}_K[X_1,\cdots,X_n]$ with reduction $\overline{F} \neq 0$. As above we may construct spaces $K[X]$, $K[X]^{(j)}$ and a complex $\mathcal{L}_\bullet(F)$. Now $K[X]$, $K[X]^{(j)}$ and $\mathcal{L}_i(F)$ all have the structure of normed space over K with $||\Sigma c_\lambda X^\lambda|| = \max ||c_\lambda||$. Let W , $W^{(j)}$ and $\hat{\mathcal{L}}_i(F)$ denote the completions of these spaces. The maps Δ_i: $K[X] \longrightarrow K[X]$ are continuous and prolong to linear operators on W , which we also denote by Δ_i . The boundary maps in $\mathcal{L}_\bullet(F)$ are continuous so $\hat{\mathcal{L}}_\bullet(F)$ becomes a complex of Banach spaces. Denote the homology groups of $\hat{\mathcal{L}}_\bullet(F)$ by $\hat{H}_i(F)$. Again we see that these are invariant under change of co-ordinates. (More precisely, if T: $X_i \longrightarrow \Sigma a_{ij}X_j$ is an invertible change of co-ordinates over $\mathcal{O}_K$, then T induces an isomorphism between $\hat{H}_i(F)$ and $\hat{H}_i(F \circ T)$).

Theorem 8.2

Suppose that k has characteristic $p \neq 0$, and that K contains an element π satisfying $\pi^{p-1} = -p$. Then $\hat{\mathcal{L}}.(F)$ is isomorphic (as a complex of Banach spaces) with the complex $\hat{\mathcal{L}}.$ constructed at the end of Chapter 7.

Proof: The proof is essentially the same as that of Theorem 8.1; however the map $W^{(s-n)} \xrightarrow{\approx} L_{\bar{A}}$ is given this time by $X^\lambda \longrightarrow (\pi X_0)^j \cdot (\prod_{i \varepsilon \bar{A}} X_i) \cdot X^\lambda$ where $j = \frac{|\lambda|+n-s}{d}$.

We shall say that $f \varepsilon k[X_1 \cdots X_n]$, homogeneous of degree d, is non-singular if the only common zero of f and the f_i is the origin. Our goal is to compute the $\hat{H}_i(F)$ under the assumption that $\bar{F}$ is non-singular. The calculations are a good deal simpler when $d \neq 0$ in k and we consider that case first.

Lemma 8.3 Suppose $f \varepsilon k[X]$, homogeneous of degree d, is non-singular, and that $d \neq 0$ in k. Then the f_i generate an $(X_1, \ldots, X_n)$ primary ideal in $k[X]$. Furthermore $f_1, \cdots, f_n$ is a prime sequence in $k[X]$; i.e. the associated multiplication operators form a prime sequence.

Proof: The Euler identity $df = \sum_1^n X_i f_i$ shows that every common zero of the f_i is a zero of f. Thus the only common zero of the f_i is the origin and the Nullstellensatz shows that $(f_1, \cdots, f_n)$ is $(X_1, \cdots, X_n)$ primary. Now let A be the local ring of $(X_1, \cdots, X_n)$ in $k[X]$. The maximal ideal of A is generated by the prime sequence $X_1,\cdots,X_n$. A well known theorem then tells us that any n elements of A generating an $(X_1,\cdots,X_n)$ primary ideal form a prime sequence in A , and the lemma follows easily.

Theorem 8.3

Situation as in Lemma 8.3. Then:

(a) $H_1\ (k[X];\ \Delta_1,\cdots,\Delta_s) = 0 \qquad (1 \leq s \leq n)$

(b) $H_i\ (f) = 0$ for $i > 0$

Proof: Suppose $\varphi^{(i)}$ $(1 \leq i \leq s)$ are in $k[X]$, and $\sum_1^s \Delta_i\ (\varphi^{(i)}) = 0$. We must show that there is a skew-symmetric set $\{a_{ij}\}$ $(1 \leq i,j \leq s)$ such that $\varphi^{(i)} = \sum_{j=1}^{s} \Delta_j\ (a_{ij})$. We argue by induction on $m = \max \deg \varphi^{(i)}$. Let $\theta^{(i)}$ be the degree m component of $\varphi^{(i)}$. Then $\sum_1^s f_i\ \theta^{(i)} = 0$. By Lemmas 8.2 and 8.3, $H_1(k[X]\ ;\ f_1,\cdots,f_s) = 0$. Thus there is a skew symmetric set $\{b_{ij}\}$ such that $\theta^{(i)} = \sum_1^s f_j\ b_{ij}$. We may assume b_{ij} homogeneous of degree $m-(d-1)$. Now,
$\sum_1^s \Delta_i\ \{\varphi^{(i)} - \sum_{j=1}^{s} \Delta_j(b_{ij})\} = 0$, and $\deg\ (\varphi^{(i)} - \Sigma\,\Delta_j(b_{ij})) < m$ for all i . An induction now gives (a), and Lemma 8.2 shows that $H_i(k[X]\ ;\ \Delta_1,\cdots,\Delta_n) = 0$ for $i > 0$. Since $H_i(f)$ is a direct summand of this space it vanishes too.

The calculation of $H_0(f)$ requires more machinery. If M is a finitely generated graded $k[X]$ module the Hilbert power series $P_M(t)$ is defined to be $\sum_0^\infty (\dim_k M^{(i)}) \cdot t^i$ where $M^{(i)}$ is the homogeneous part of M of degree i.

If $\mathcal{M} = M_n \longrightarrow M_{n-1} \longrightarrow \cdots \longrightarrow M_0$ is a complex of graded modules, the maps being homogeneous of degree 0, set $P_{\mathcal{M}} = \sum_j (-1)^j P_{M_j}$.

Lemma 8.4 Situation as in Lemma 8.3. Then $M = k[X]/(f_1,\ldots,f_n)$ is finite dimensional over k. If $P_M(t) = \sum_0^\infty c_j t^j$, then

$$\sum_{j \equiv -n(d)} c_j = d^{-1}\{(d-1)^n + (-1)^n(d-1)\} .$$

Proof: Let $\mathcal{M}$ be the Koszul complex $K.(k[X]\,;\, f_1,\cdots,f_n)$. Grade $\mathcal{M}$ so that the boundary maps are homogeneous of degree 0. Then $M = H_0(\mathcal{M})$, and Lemmas 8.2 and 8.3 show that $H_i(\mathcal{M}) = 0$ for $i > 0$. It follows that $P_M(t) = P_{\mathcal{M}}(t)$. Using the fact that the Hilbert polynomial of $k[X]$ itself is $(1-t)^{-n}$ one sees easily that $P_{\mathcal{M}}(t) = (1-t)^{-n} \cdot \{(1-t^{d-1})^n\}$. Thus $P_M(t) = (1+t+\ldots+t^{d-2})^n$ is a polynomial and M is finite dimensional. Let $g(t) = t^n P_M(t) = \sum a_j t^j$. Then

$$\sum_{j\equiv -n} c_j = \sum_{j \equiv 0} a_j = d^{-1} \sum_{\xi} g(\xi)$$ where ξ ranges over the d'th roots of unity.

Now $g(1) = (d-1)^n$ while $g(\xi) = (\xi + \xi^2 \cdots + \xi^{d-1})^n = (-1)^n$ if $\xi \neq 1$, and the lemma follows.

Theorem 8.3

Situation as in Lemma 8.3. Then $\dim H_0(f) = d^{-1} \cdot \{(d-1)^n + (-1)^n (d-1)\}$.

Proof: By Lemma 8.4 $\dim \{k[X]^{(-n)} / \Sigma f_i k[X]^{(1-n)}\} = d^{-1}\{(d-1)^n + (-1)^n (d-1)\}$. Let V be a homogeneous subspace of $k[X]^{(-n)}$ such that $V \oplus \Sigma f_i k[X]^{(1-n)} = k[X]^{(-n)}$. It will suffice to show that the natural map $\lambda : V \longrightarrow k[X]^{(-n)} / \Sigma \Delta_i k[X]^{(1-n)} = H_0(f)$ is bijective. Suppose that $v \in V$ and that $v = \sum_1^n \Delta_i \varphi^{(i)}$ with $\varphi^{(i)} \in k[X]^{(1-n)}$. We shall show by an induction on $m = \max \deg \varphi^{(i)}$ that $v = 0$. Let $\theta^{(i)}$ be the degree m component of $\varphi^{(i)}$. Then $\Sigma f_i \varphi^{(i)}$ is the degree $m-1+d$ component of v, belongs to $V \cap \Sigma f_i k[X]^{(1-n)}$ and must vanish. By Lemmas 8.2 and 8.3 there is a skew symmetric set $\{a_{ij}\}$ such that $\theta^{(i)} = \Sigma f_j a_{ij}$. We may assume that the a_{ij} are homogeneous of degree $m-d+1$. Now $\Sigma \Delta_i (\varphi^{(i)} - \Sigma \Delta_j (a_{ij})) = \Sigma \Delta_i (\varphi_i) = v$. An induction now shows that $v = 0$. Thus λ is injective; in a similar but simpler way one shows that λ is onto.

Putting Theorems 8.1, 8.3 and 8.4 together we find that we have computed the homology of the complex $\mathcal{L}$ introduced in Chapter 7 provided that f is non-singular and $\deg f \neq 0$ in k. Explicitly $H_i = 0$ for $i > 0$, and $\dim H_0 = d^{-1} \{(d-1)^n + (-1)^n (d-1)\}$. We next seek a similar result for the homology of $\hat{\mathcal{L}}$.

We first prove a theorem which enables us to relate algebraic and analytic homology. Let $\mathcal{O}$ be a complete discrete valuation ring with maximal ideal (π). We say that an $\mathcal{O}$-module M is flat if $\pi : M \longrightarrow M$ is injective, separated if $\cap \pi^j M = 0$. A separated $\mathcal{O}$-module, M, has an obvious metric space structure with the $\pi^j M$ a fundamental system of neighborhoods of 0. We say that M is $\mathcal{O}$-complete if it is complete in this metric.

Theorem 8.5

Let $C = C_n \longrightarrow C_{n-1} \longrightarrow \cdots \longrightarrow C_0$ be a complex of flat, separated $\mathcal{O}$-complete $\mathcal{O}$-modules (the boundary maps being $\mathcal{O}$-linear). Let $\overline{C} = C/\pi C$ be the reduction of C. Then:

(1) For any i, $H_i(\overline{C}) = 0 \Longrightarrow H_i(C) = 0$

(2) If $H_0(\overline{C})$ has dimension $\ell < \infty$ over $\mathcal{O}/(\pi)$, and $H_1(\overline{C}) = 0$, then $H_0(C)$ is a finite free $\mathcal{O}$-module of rank ℓ.

Proof: $H_i(C) = \dfrac{\ker \partial}{\operatorname{im} \partial}$. Since C_{i+1} is $\mathcal{O}$-complete, $\operatorname{im} \partial$ is also $\mathcal{O}$-complete. It follows that $\operatorname{im} \partial$ is closed in $\ker \partial$ and that $H_i(C)$ is separated. Now the exact sequence of complexes $0 \longrightarrow C \xrightarrow{\pi} C \longrightarrow \overline{C} \longrightarrow 0$ gives a long exact sequence of homology, and we find that $H_i(C)/\pi H_i(C)$ imbeds in $H_i(\overline{C})$. Thus if $H_i(\overline{C}) = 0$, $H_i(C) = \pi H_i(C)$. Since $H_i(C)$ is separated $H_i(C) = 0$.

Suppose now that we're in the situation of (2). The long exact sequence of homology shows that $H_0(C)/\pi H_0(C) \approx H_0(\overline{C})$. Using the fact that $H_0(C)$ is separated, that $\dim H_0(\overline{C}) < \infty$ and that $\mathcal{O}$ is complete we find that $H_0(C)$ is a finite $\mathcal{O}$-module. Thus it suffices to show that $H_0(C)$ has no $\mathcal{O}$-torsion. But this follows from the long exact sequence of homology since $H_1(\overline{C}) = 0$.

Theorem 8.6

Suppose that the reduction, $\overline{F}$, of F is non-singular and that the degree d of F is $\neq 0$ in k . Then:

(1) $\widehat{H}_i(F) = 0$ for $i > 0$

(2) $\dim \widehat{H}_0(F) = d^{-1}\{(d-1)^n + (-1)^n (d-1)\}$

Proof: The unit ball in $\hat{\mathcal{L}}.(F)$ is a complex of flat separated $\mathcal{O}_K$-complete $\mathcal{O}_K$-modules whose reduction is $\mathcal{L}.(\overline{F})$. The result now follows from Theorems 8.3, 8.4 and 8.5.

The condition $d \neq 0$ in k is in fact unnecessary and we next show how to get around it. If $f \in k[X]$ $(n > 1)$ is homogeneous of degree d we shall say that f is regular if f is non-singular and the "hyperplane section" $f^* = f(X_1, \cdots, X_{n-1}, 0)$ is a non-singular element of $k[X_1, \cdots, X_{n-1}]$.

Lemma 8.5 Suppose $f \in k[X]$ is regular. Then $(f_1, \cdots, f_{n-1}, f)$ is an $(X_1, \cdots, X_n)$ primary ideal in $k[X]$. Furthermore $f_1, \cdots, f_{n-1}, f$ is a prime sequence in $k[X]$.

Proof: Let P be a common zero of $f_1, \cdots, f_{n-1}$ and f . Since $df = \sum_1^n X_i f_i$, either $X_n(P) = 0$ or $f_n(P) = 0$. In the first case the non-singularity of f^* shows that P is the origin; in the second the non-singularity of f gives the same result. We continue as in the proof of Lemma 8.3.

Lemma 8.6 Suppose $f \in k[X]$ is regular. Then $H_1(k[X]; \Delta_1, \cdots, \Delta_s) = 0$ for $1 \leq s \leq n-1$.

Proof: By Lemma 8.5, $f_1, \cdots, f_s$ is a prime sequence in $k[X]$ and we may copy the proof of Theorem 8.3.

To continue further we introduce some new complexes and mappings. If j is an integer, let $\Delta_0^{(j)}: k[X]^{(j)} \longrightarrow k[X]^{(j)}$ be the map taking a monomial φ into $\{ (\frac{\deg \varphi - j}{d}) + f \} \varphi$. If j is an integer, let $\mathcal{L}.^{(j)}(f)$ be the subcomplex $\Sigma\, k[X]^{(s+j)} e_{i_1} \wedge \cdots \wedge e_{i_s}$ of $K.(k[X]; \Delta_1, \cdots \Delta_{n-1})$. Now the following diagram commutes:

$$\begin{array}{ccc} k[X]^{(j)} & \xrightarrow{\ \Delta_0^{(j)}\ } & k[X]^{(j)} \\ \Delta_i \big\downarrow & & \big\downarrow \Delta_i \\ k[X]^{(j-1)} & \xrightarrow{\ \Delta_0^{(j-1)}\ } & k[X]^{(j-1)} \end{array}$$

It follows that the mapping $\Delta_0: \mathcal{L}^{(j)}(f) \longrightarrow \mathcal{L}^{(j)}(f)$ which is $\Delta_0^{(s+j)}$ on every component in dimension s is a chain map.

Recall now the definition of the "mapping cone." If $\varphi: X \longrightarrow Y$ is a map of complexes define a new complex, Z, the mapping cone of φ by taking $Z_i = X_{i-1} \oplus Y_i$ and $\partial: Z_i \longrightarrow Z_{i-1}$ to be the map $(x,y) \longrightarrow (\partial x, \partial y + (-1)^{i+1} \varphi(x))$. The exact sequence of complexes $0 \longrightarrow Y \longrightarrow Z \longrightarrow X' \longrightarrow 0$ with X' a shift of X gives an exact homology sequence:

$$\longrightarrow H_i(X) \xrightarrow{\varphi_*} H_i(Y) \longrightarrow H_i(Z) \longrightarrow H_{i-1}(X) \xrightarrow{\varphi_*} H_{i-1}(Y) \longrightarrow$$

Now let $\mathcal{M}^{(j)}(f)$ be the mapping cone of the map $\Delta_0: \mathcal{L}^{(j)}(f) \longrightarrow \mathcal{L}^{(j)}(f)$

Lemma 8.7 Suppose $f \in k[X]$ is regular. Then:

(a) $H_1(\mathcal{M}^{(j)}(f)) = 0$

(b) $\dim H_0(\mathcal{M}^{(j)}(f)) = (d-1)^{n-1}$

Proof: (a) is proved by an explicit calculation very similar to that given in Theorem 8.3 (a). The key idea is that $\Delta_i(\varphi) = f_i\, \varphi$ + lower order terms, that $\Delta_0^{(j)}(\varphi) = f\, \varphi$ + lower order terms and that $f_1, \cdots, f_{n-1}, f$ is a prime sequence. We omit the details. To prove (b) one first shows, as in Lemma 8.4, that $P_M(t) = (1 + t + \cdots + t^{d-2})^{n-1} \cdot (1 + t + \cdots + t^{d-1})$ where $M = k[X]/(f_1, \cdots, f_{n-1}, f)$. Then, if we write $P_M(t) = \Sigma\, c_\ell t^\ell$ we find that $\sum_{\ell \equiv j(d)} c_\ell = (d-1)^{n-1}$. Now

$H_0(\mathcal{M}^{(j)}(f)) = k[X]^{(j)} / \{\Delta_0^{(j)} k[X]^{(j)} + \sum_1^{n-1} \Delta_i k[X]^{(j+1)}\}$, and we continue very much as in the proof of Theorem 8.4, again using the fact that $f_1, \cdots, f_{n-1}, f$ is a prime sequence.

The constructions we have made admit analytic analogues. Suppose then that $F \in \mathcal{O}_K[X_1, \cdots X_n]$ is homogeneous of degree d. The maps $\Delta_0^{(j)}: K[X]^{(j)} \longrightarrow K[X]^{(j)}$ are continuous and prolong to maps $W^{(j)} \longrightarrow W^{(j)}$. The complex $\mathcal{L}.^{(j)}(F)$ has a normed space structure; let $\hat{\mathcal{L}}.^{(j)}(F)$ be its completion. Then Δ_0 prolongs to a chain map of $\hat{\mathcal{L}}.^{(j)}$; let $\hat{\mathcal{M}}.^{(j)}(F)$ be the mapping cone of this map.

Lemma 8.8 Suppose that the reduction, $\bar{F}$, of F is regular. Then for all j the endomorphism $\Delta_0^{(j)}$ of $W^{(j)} / \sum_1^{n-1} \Delta_i W^{(j+1)}$ is injective. Furthermore the cokernel has dimension $(d-1)^{n-1}$.

Proof: The unit ball in $\hat{\mathcal{M}}^{(j)}(F)$ is a complex of flat separated $\mathcal{O}_K$-complete $\mathcal{O}_K$ modules with reduction $\mathcal{M}^{(j)}(\bar{F})$. Lemma 8.7 and Theorem 8.5 then show that $H_1(\hat{\mathcal{M}}^{(j)}(F)) = 0$ while $\dim H_0(\hat{\mathcal{M}}^{(j)}(F)) = (d-1)^{n-1}$. The result now follows from the long exact sequence of the mapping cone.

Lemma 8.9 Suppose that the reduction $\bar{F}$ of F is regular. Then: $\hat{H}_i(F) = 0$ for $i \geq 2$, while $\hat{H}_1(F)$ and $\hat{H}_0(F)$ are isomorphic with the kernel and cokernel of the map $\Delta_n: W^{(1-n)} / \sum_1^{n-1} \Delta_i W^{(2-n)} \longrightarrow W^{(-n)} / \sum_1^{n-1} \Delta_i W^{(1-n)}$

Proof: Using Lemma 8.6 and Theorem 8.5 we find that $H_1(W; \Delta_1, \cdots, \Delta_s) = 0$ for $s \leq n-1$. It follows that $\Delta_1, \cdots \Delta_{n-1}$ is a prime sequence on W. Repeated applications of Lemma 8.1 now show that $H_i(W; \Delta_1, \cdots, \Delta_n) \approx H_i(W/\sum_1^{n-1} \Delta_i(W); \Delta_n)$ and the lemma follows immediately.

Lemma 8.10

If $\varphi \in W^{(-n)}$, then $\sum_1^n \Delta_i (X_i \varphi) = d \Delta_0^{(-n)} (\varphi)$

If $\varphi \in W^{(1-n)}$, then $\sum_1^{n-1} \Delta_i (X_i \varphi) + X_n \Delta_n(\varphi) = d \Delta_0^{(1-n)} (\varphi)$

Proof: We may assume φ is a monomial. Then

$$\sum_1^n \Delta_i (X_i \varphi) = \sum_1^n \{\varphi + X_n \varphi_n + X_i F_i \varphi\} = (\deg \varphi + n + dF) \varphi = d \Delta_0^{(-n)} (\varphi).$$

The proof of the second result is similar.

Lemma 8.11 Suppose that the reduction, $\overline{F}$, of F is regular. Let F^* be the element $F(X_1, \cdots X_{n-1}, 0)$ of $\mathcal{O}_K[X_1, \cdots X_{n-1}]$. Then:

(1) $\hat{H}_1 (F) = 0$

(2) $\dim \hat{H}_0 (F) = (d-1)^{n-1} - \dim \hat{H}_0(F^*)$

$\underline{\text{Proof}}$: We have obvious maps $\Delta_n: W^{(1-n)} / \sum_1^{n-1} \Delta_i W^{(2-n)} \longrightarrow W^{(-n)} / \sum_1^{n-1} \Delta_i W^{(1-n)}$

and $X_n: W^{(-n)} / \sum_1^{n-1} \Delta_i W^{(1-n)} \longrightarrow W^{(1-n)} / \sum_1^{n-1} \Delta_i W^{(2-n)}$, the second map being induced by multiplication by X_n.

By Lemma 8.10, $X_n \circ \Delta_n = d \Delta_0^{(1-n)}$ while $\Delta_n \circ X_n = d \Delta_0^{(-n)}$. Since characteristic $K = 0$, Lemma 8.8 shows that these maps, and therefore Δ_n and X_n themselves, are injective. By Lemma 8.9, $\hat{H}_1(F) \approx \ker \Delta_n = 0$, while $\hat{H}_0(F) \approx \operatorname{cok} \Delta_n$. Now $\dim (\operatorname{cok} \Delta_n) = \dim \operatorname{cok} (\Delta_n \circ X_n) - \dim \operatorname{cok} (X_n)$. But $\operatorname{cok} (\Delta_n \circ X_n) = \operatorname{cok} \Delta_0^{(-n)}$ and has dimension $(d-1)^{n-1}$ by Lemma 8.8. Finally $\operatorname{cok} (X_n)$ is evidently isomorphic with $\hat{H}_0 (F^*)$.

Theorem 8.7

Suppose that the reduction, $\bar{F}$, of F is non-singular. Then:

(1) $\hat{H}_i(F) = 0$ for $i > 0$

(2) $\dim \hat{H}_0(F) = d^{-1} \{(d-1)^n + (-1)^n (d-1)\}$

(3) The image of the unit ball of $\hat{\mathcal{L}}_0(F)$ in $\hat{H}_0(F)$ is a finite $\mathcal{O}_K$-module

$\underline{\text{Proof}}$: Suppose first $n = 1$. Then $F = c X_1^d$ with c a unit in $\mathcal{O}_K$. Now it's easy to see that the complex $\hat{\mathcal{L}}.(c X_1^d)$ is essentially the same as the complex $\hat{\mathcal{L}}.(cX_1)$, the only difference being that the boundary map $\hat{\mathcal{L}}_1 \longrightarrow \hat{\mathcal{L}}_0$ is multiplied by d. Theorem 8.6 then shows that $\hat{H}_0(F) = \hat{H}_1(F) = 0$.

Suppose next $n > 1$. By replacing K by a finite extension and making an invertible change of co-ordinates $X_i \longrightarrow \Sigma\, a_{ij} X_j$ we may assume that $\bar{F}$ is regular. Lemmas 8.9 and 8.11 then give (1). Since $\bar{F}$ is regular, $\bar{F}^*$ is non-singular. Lemma 8.11 and an induction give (2). To prove (3) it suffices to show that the image of the unit ball of $W^{(-n)}$ in $W^{(-n)} / \{\sum_{1}^{n-1} \Delta_i W^{(1-n)} + \Delta_0^{(-n)} W^{(-n)}\}$ is a finite $\mathcal{O}_K$-module; i.e. that the image of the unit ball of $\hat{\mathcal{M}}^{(-n)}_0 (F)$ in $H_0(\hat{\mathcal{M}}^{(-n)}_{\cdot} (F))$ is a finite $\mathcal{O}_K$-module. Since the unit ball in $\hat{\mathcal{M}}^{(-n)}_{\cdot}(F)$ is a complex of flat separated $\mathcal{O}_K$-complete $\mathcal{O}_K$-modules this follows from Theorem 8.5 and Lemma 8.7.

Theorem 8.8

Let $k = GF(q)$ be a finite field (of characteristic $p \neq 2$) and let f be an element of $k[X_1, \cdots, X_n]$, homogeneous of degree d and defining a non-singular projective hypersurface U in $\mathbb{P}^{n-1}$.

Let $\hat{\mathcal{L}}_{\cdot}$ be the complex constructed from f in Chapter 7, and $\alpha: \hat{\mathcal{L}}_{\cdot} \longrightarrow \hat{\mathcal{L}}_{\cdot}$ the chain map constructed there. Then:

(1) $H_i(\hat{\mathcal{L}}_{\cdot}) = 0$ for $i \geq 1$

(2) $\dim H_0(\hat{\mathcal{L}}_{\cdot}) = \ell = d^{-1} \{(d-1)^n + (-1)^n (d-1)\}$

(3) If $q\,\gamma_i$ $(1 \leq i \leq \ell)$ are the eigenvalues of $(\alpha_0)_*$ on $H_0(\hat{\mathcal{L}})$, then the γ_i are non-zero algebraic integers

(4) $$N_s(U) = \frac{q^{(n-1)s}-1}{q^s-1} + (-1)^n \sum_{1}^{\ell} \gamma_i^{\,s}$$

<u>Proof</u>: (1) and (2) follow from Theorems 8.2 and 8.7. For an operator on a finite dimensional space, $\mathrm{Tr}_{\mathrm{nuc}}$ is the ordinary trace. The "Lefschetz fixed point theorem", Theorem 7.5, then gives (4). It follows that $\prod_{1}^{\ell} (1-\gamma_i t) = \{ \prod_{s=0}^{n-2} (1-q^s t) \cdot \zeta_U(t)\}^{\pm 1}$.

Thus $\prod_{1}^{\ell} (1-\gamma_i t)$ has integer co-efficients and the γ_i are algebraic integers. It remains to show that $\gamma_i \neq 0$, i.e. that $(\alpha_0)_*$ is bijective. We have a commutative diagram:

$$\begin{array}{ccc} \hat{\mathcal{L}}_0 & \xrightarrow{\ \alpha_0\ } & \hat{\mathcal{L}}_0 \\ \downarrow & & \downarrow \\ H_0(\hat{\mathcal{L}}) & \xrightarrow{\ (\alpha_0)_*\ } & H_0(\hat{\mathcal{L}}) \end{array}$$

Put a Banach space structure on the finite dimensional space $H_0(\hat{\mathcal{L}})$, taking any basis as orthonormal basis. By Theorem 8.7, the map $\hat{\mathcal{L}}_0 \longrightarrow H_0(\hat{\mathcal{L}})$ is continuous. Furthermore $\alpha_0 : \hat{\mathcal{L}}_0 \longrightarrow \hat{\mathcal{L}}_0$ has dense image. (For it suffices to show that

$\psi \circ H : L_A \longrightarrow L_A$ has dense image. This follows by factoring $\psi \circ H$ as

$L_A \subset L_A(\frac{1}{q}) \xrightarrow{\ H\ } L_A(\frac{1}{q}) \xrightarrow{\ \psi\ } L_A$ since L_A is dense in $L_A(\frac{1}{q})$, and H and ψ

are continuous and onto.) The diagram above now shows that $(\alpha_0)_*$ has dense image. So $(\alpha_0)_*$ is onto, and we're done.

To handle the case $p = 2$ we generalize the definition of the complex $\hat{\mathcal{L}}.(F)$ a little. Let d be an integer > 0 and F be an element of $\mathcal{O}_K[X_1,\cdots,X_n]$. In defining $\hat{\mathcal{L}}.(F)$ the fact that F was homogeneous of degree d was only used to show that $\Delta_i\ K[X]^{(j)} \subset K[X]^{(j-1)}$. This remains true if we only assume that every monomial occurring in F has degree a multiple of d. So in this extended context we may still speak of $\hat{\mathcal{L}}.(F)$ and $\hat{H}.(F)$.

Theorem 8.9

Suppose that characteristic $\bar{K} = p$, that every monomial occurring in F has degree either d or a multiple of pd, and that the reduction $\bar{F}$ of F has the form $f + g$ where f is homogeneous of degree d and non-singular, each monomial in g has degree $> d$, and $g_i = 0$ for all i. Then the conclusions of Theorem 8.7 remain true.

Proof: Again the proof is easiest when $p \nmid d$. For, since $g_i = 0$ for all i, the reduction of the unit ball in $\hat{\mathcal{L}}.(F)$ is just $\mathcal{L}.(f)$, and we may use Theorems 8.3, 8.4 and 8.5. To handle the general case one again has to introduce maps $\Delta_0^{(j)}: K[X]^{(j)} \longrightarrow K[X]^{(j)}$. This is done as follows. Write $F = \Sigma F^{(i)}$ with $F^{(i)}$ homogeneous of degree i. If φ is a monomial in $K[X]^{(j)}$, let

$$\Delta_0^{(j)}(\varphi) = \left\{ \frac{\deg \varphi - j}{d} + \Sigma \frac{i}{d} F^{(i)} \right\} \cdot \varphi .$$ Again, $\Delta_i \circ \Delta_0^{(j)} = \Delta_0^{(j-1)} \circ \Delta_i$,

and we may build complexes $\hat{\mathcal{L}}.^{(j)}(F)$, a chain map $\Delta_0 : \hat{\mathcal{L}}.^{(j)}(F) \longrightarrow \hat{\mathcal{L}}.^{(j)}(F)$, and the mapping cone $\hat{\mathcal{M}}^{(j)}(F)$ of Δ_0 .

Since $g_i = 0$ for all i , the reduction of the unit ball in $\hat{\mathcal{L}}.^{(j)}(F)$ is just $\mathcal{L}.^{(j)}(f)$. Since $\Sigma \frac{i}{d} F^{(i)}$ reduces to f , the reduction of Δ_0 is just $\Delta_0 : \mathcal{L}.^{(j)}(f) \longrightarrow \mathcal{L}.^{(j)}(f)$. It follows that the unit ball in $\hat{\mathcal{M}}^{(j)}(F)$ has reduction $\mathcal{M}.^{(j)}(f)$. This enables us to prove Lemma 8.8 for our more general F (assuming that f is regular). The proofs of Lemmas 8.9, 8.10, 8.11 and Theorem 8.7 now go through virtually unchanged.

Theorem 8.10

Theorem 8.8 remains true when characteristic $k = 2$, provided we replace $\hat{\mathcal{L}}.$ and α by $\hat{\mathcal{L}}.'$ and α' . (See Chapter 7 for the appropriate definitions).

Proof: Let K be the field obtained from Q_2 by adjoining the roots of $X^q = X$, and F be the Teichmüller lifting of f . Set $F' = -F - F^{(2)}(X^2) - 2F^{(4)}(X^4)$, $G = X_0 F$, and $G' = -G + 2G^{(2)}(X^2) + 16\, G^{(4)}(X^4)$. We show first that the complex $\hat{\mathcal{L}}.'$ constructed in Chapter 7 is isomorphic to $\mathcal{L}.(F')$. The map is the same as that of Theorem 8.2. In other words it is a direct sum of maps $W^{(s-n)} \xrightarrow{\approx} L_{\bar{A}}$ sending X^λ into $(-2X_0)^j \cdot (\prod_{i \in \bar{A}} X_i) \cdot X^\lambda$ where $j = \frac{|\lambda|+n-s}{d}$. To see this is a chain map we must show that the following diagram commutes:

$$
\begin{array}{ccc}
W^{(s-n)} & \longrightarrow & L_{\overline{A}} \\
\Delta_j \downarrow & & \downarrow D_j' \\
W^{(s-1-n)} & \longrightarrow & L_{\overline{A} \cup \{j\}}
\end{array}
$$

where $\Delta_j(\varphi) = \varphi_j + (F')_j \varphi$ and $D_j'(\varphi) = X_j \varphi_j - 2X_j (G')_j \varphi$. This is straightforward.

Now F' satisfies all the conditions of Theorem 8.9. It follows from Theorem 8.9 and the isomorphism above that $H_i(\hat{\mathcal{L}}.') = 0$ for $i > 0$ while $\dim H_0(\hat{\mathcal{L}}.') = \ell = d^{-1}\{(d-1)^n + (-1)^n (d-1)\}$. We now continue as in the proof of Theorem 8.8, using the Lefschetz fixed point theorem, Theorem 7.8.

Finally we give some examples to illustrate Theorems 8.8 and 8.10. Suppose first $n = 3$. Then U is a non-singular (and therefore absolutely irreducible) plane curve $f(X_1, X_2, X_3) = 0$. Also $\ell = d^{-1}\{(d-1)^3 - (d-1)\} = (d-1)(d-2) = 2g$ where g is the genus of U. Then $N_s(U) = q^s + 1 - \sum_1^{\ell} \gamma_i^s$, in accordance with the results of Chapter 2.

Suppose next that $n = 5$ and $d = 3$ so that U is a cubic 3-fold. Then $\ell = \frac{1}{3}(2^5-2) = 10$ and $N_s(U) = q^{3s} + q^{2s} + q^s + 1 - \sum_1^{10} \gamma_i^s$. Bombieri and Swinnerton-Dyer have shown in [1] that $|\gamma_i| = q^{3/2}$ in this case (at least if $p \neq 2$). Finally we have the case of the quartic surface $n = d = 4$. Then $\ell = \frac{1}{4}(3^4 + 3) = 21$ and $N_s(U) = q^{2s} + q^s + 1 + \sum_1^{21} \gamma_i^s$. For certain special quartic surfaces Dwork has recently given a remarkable proof that $|\gamma_i| = q$.

Chapter 9 - Connections with cohomology theories

In the calculation of $N_s(U)$ for a non-singular projective hypersurface U defined over $GF(q)$, certain complexes and homology groups played a key part. We shall study these complexes more closely in this chapter and try to show that there is a cohomology theory of De Rham type lurking in the wings. First we shall look at the "algebraic complex" $\mathcal{L}.$ of Chapter 7, and then go on the "analytic complex" $\hat{\mathcal{L}}.$.

Let k be a field of characteristic 0 and $f \neq 0$ an element of $k[X] = k[X_1,\cdots,X_n]$, homogeneous of degree m. In Chapter 8 we defined operators $\Delta_i: \varphi \longrightarrow \varphi_i + f_i\,\varphi$ on $k[X]$ and a subcomplex $\mathcal{L}.(f)$, with homology $H.(f)$, of the Koszul complex $K.(k[X]; \Delta_1,\cdots,\Delta_n)$. It turned out that $\mathcal{L}.(f)$ was isomorphic with the complex $\mathcal{L}.$ of Chapter 7. We shall find it more convenient in this chapter to replace $\mathcal{L}.(f)$ by an isomorphic co-complex $\mathcal{L}^{\cdot}(f)$.

To this end we define Koszul cohomology. Suppose that $\Delta_1,\cdots,\Delta_n$ are commuting endomorphisms of an abelian group A. Then $A \underset{Z}{\otimes} \Lambda Z^n$ may be given the structure of co-complex, the degree 1 coboundary map δ sending $a\, e_{i_1} \wedge \cdots \wedge e_{i_s}$ into $\sum_j D_j(a)\, e_j \wedge e_{i_1} \wedge \cdots \wedge e_{i_s}$. Denote this co-complex by $K^{\cdot}(A; \Delta_1,\cdots,\Delta_n)$, and its cohomology by $H^{\cdot}(A; \Delta_1,\cdots,\Delta_n)$. We see readily that with the obvious renumbering of dimensions the complex $K.(A)$ and the co-complex $K^{\cdot}(A)$ are isomorphic.

Now let $\mathcal{L}^{\cdot}(f)$ be the subcomplex $\sum k[X]^{(-s)}\, e_{i_1} \wedge \cdots \wedge e_{i_s}$ of $K^{\cdot}(k[X]; \Delta_1,\cdots,\Delta_n)$, and $H^{\cdot}(f)$ be the cohomology of $\mathcal{L}^{\cdot}(f)$. The isomorphism between $K.(k[X])$ and $K^{\cdot}(k[X])$ maps $\mathcal{L}.(f)$ onto $\mathcal{L}^{\cdot}(f)$. It follows that $H_i(f) \approx H^{n-i}(f)$. It will be convenient to work with a subcomplex of $\mathcal{L}^{\cdot}(f)$.

<u>Definition</u> $\mathcal{L}^i_{\#} = \mathcal{L}^i(f)$ for $i > 0$. $\mathcal{L}^0_{\#} = \{z \in \mathcal{L}^0(f) | z$ has constant term $0\}$

The cohomology of $\mathcal{L}^{\cdot}_{\#}$ will be denoted by $H^{\cdot}_{\#}(f)$. Evidently $H^i_{\#}(f) = H^i(f)$ for $i \geq 2$.

<u>Definition</u> $r: \mathcal{L}^{\cdot}_{\#} \longrightarrow \mathcal{L}^{\cdot}_{\#}$ is the degree -1 map $\varphi e_{i_1} \wedge \cdots \wedge e_{i_s} \longrightarrow \Sigma (-1)^{j+1} X_{i_j} \varphi e_{i_1} \wedge \cdots \wedge \hat{e}_{i_j} \wedge \cdots e_{i_s}$. $\Delta_0: \mathcal{L}^{\cdot}_{\#} \longrightarrow \mathcal{L}^{\cdot}_{\#}$ is the degree 0 map $\varphi e_{i_1} \wedge \cdots \wedge e_{i_s} \longrightarrow (\lambda + f) \cdot \varphi e_{i_1} \wedge \cdots \wedge e_{i_s}$, where φ is homogeneous of degree $m\lambda\text{-}s$.

<u>Lemma 9.1</u> Δ_0 is a chain map, and $\delta r + r\delta = m \Delta_0$.

<u>Proof</u>: Let $z = \varphi e_{i_1} \wedge \cdots \wedge e_{i_s}$ with φ homogeneous of degree $m\lambda\text{-}s$. Set $S = \{i_1, \cdots, i_s\}$. Then $\delta r + r\delta (z) = \{ \sum_{k \in S} \Delta_k(X_k \varphi) + \sum_{k \notin S} X_k \Delta_k (\varphi)\} e_{i_1} \wedge \cdots \wedge e_{i_s}$ + terms which cancel in pairs. This may be rewritten as $\{\sum_1^n X_k \varphi_k + s\varphi + \sum_1^n X_k f_k \varphi\} e_{i_1} \wedge \cdots \wedge e_{i_s}$. By the Euler identity, this is $m \Delta_0(z)$. So $\delta r + r\delta = m \Delta_0$. It follows that $\delta\Delta_0 = \Delta_0 \delta$.

Assuming that $f \neq 0$ we see immediately that the chain map Δ_0 has kernel 0 . We next show how to identify the cokernel of Δ_0 with a complex of differential forms. Suppose A is a k-algebra. Let $\Omega^{\cdot}(A)$ denote the exterior algebra on the A-module $\Omega^{1}_{A/k}$. $\Omega^{\cdot}(A)$ admits a degree 1 coboundary map; exterior differentiation. The cohomology of $(\Omega^{\cdot}(A),d)$ will be denoted by $H^{\cdot}_{DR}(A)$ and called the (algebraic) De Rham cohomology of A. A map of k-algebras induces mappings on $\Omega^{\cdot}$ and $H^{\cdot}_{DR}$.

Suppose now that $A = k[X]_f$; the localization of $k[X]$ with respect to the powers of f. Then $\Omega^{\cdot}(A)$ is a free exterior algebra on dX_i $(1 \leq i \leq n)$. We show how to put a grading both on A and on $\Omega^{\cdot}(A)$. If we let each X_i have weight 1, then A has the structure of graded k-algebra (the weights being negative as well as positive). Let $A_{(j)}$ denote the subspace of elements of A of weight j. Then $A_{(0)}$ is a subalgebra of A. Geometrically, $A_{(0)}$ is the co-ordinate ring of the complement in $\mathbb{P}^{n-1}$ of the projective hypersurface $f = 0$.

If we let each dX_i have weight 1, the grading on A prolongs to a grading on $\Omega^{\cdot}(A)$. Let $\Omega^{\cdot}_{(j)}(A)$ be the space of elements of weight j. Since

$\frac{\partial}{\partial X_i} : A \longrightarrow A$ are homogeneous mappings of weight -1, $d: \Omega^{\cdot}(A) \longrightarrow \Omega^{\cdot}(A)$ is homogeneous of weight 0, and the $\Omega^{\cdot}_{(j)}(A)$ are subcomplexes of $\Omega^{\cdot}(A)$.

<u>Definition</u> $R: \Omega^{\cdot}(A) \longrightarrow \Omega^{\cdot}(A)$ is the degree -1 map

$$\varphi\, d X_{i_1} \wedge \cdots \wedge d X_{i_s} \longrightarrow \Sigma\, (-1)^{j+1} X_{i_j}\, \varphi\, d X_{i_1} \wedge \cdots \widehat{d X_{i_j}} \cdots \wedge d X_{i_s}$$

<u>Lemma 9.2</u>

(1) $R\left(\frac{df}{f}\right) = m$

(2) $R(\omega \wedge \eta) = (R\, \omega \wedge \eta) + (-1)^{\deg \omega} (\omega \wedge R\, \eta)$

(3) $d\,R + R\,d\,(\omega) = j\,\omega$ for $\omega \in \Omega^{\cdot}_{(j)}(A)$

(4) The inclusion map $i: \Omega^{\cdot}_{(0)}(A) \subset \Omega^{\cdot}(A)$ is a homotopy equivalence of complexes.

<u>Proof</u>: $R(\frac{df}{f}) = R(\frac{\Sigma f_i dX_i}{f}) = f^{-1} \cdot \Sigma X_i f_i = m$ proving (1). The proof of (2) is straightforward. To prove (3) suppose $\omega = \varphi\, dX_{i_1} \wedge \cdots \wedge dX_{i_s}$; set $S = \{i_1, \cdots, i_s\}$. Then $dR + Rd\,(\omega) = \{ \sum_{k \in S} \frac{\partial}{\partial X_k} (X_k\, \varphi) + \sum_{k \notin S} X_k \frac{\partial \varphi}{\partial X_k} \} \cdot$ $dX_{i_1} \wedge \cdots \wedge dX_{i_s}$ + terms which cancel in pairs. This may be rewritten as $\{\sum_1^n X_k \frac{\partial \varphi}{\partial X_k} + s\,\varphi\}\, dX_{i_1} \wedge \cdots \wedge dX_{i_s}$. For φ homogeneous, this is precisely (weight ω) $\cdot\, \omega$. Finally, let p be the projection map $\Omega^{\cdot}(A) \longrightarrow \Omega^{\cdot}_{(0)}(A)$ and let $R' : \Omega^{\cdot}(A) \longrightarrow \Omega^{\cdot}(A)$ be the map which is 0 on $\Omega^{\cdot}_{(0)}(A)$ and $\frac{1}{j} \cdot R$ on $\Omega^{\cdot}_{(j)}(A)$ for $j \neq 0$. Using (3) we see that R' is a chain homotopy between $i \circ p$ and the identity. Thus i and p are homotopy inverses.

<u>Theorem 9.1</u>

(1) There is an exact sequence of complexes:

$$0 \longrightarrow \mathcal{L}^{\cdot}_{\#} \xrightarrow{\Delta_0} \mathcal{L}^{\cdot}_{\#} \xrightarrow{\sigma} \Omega^{\cdot}_{(0)}(A) \longrightarrow 0$$

(2) For each i one has exact sequences:

$$0 \longrightarrow H^i_{\#}(f) \xrightarrow{\sigma^*} H^i_{DR}(A) \xrightarrow{\partial} H^{i+1}_{\#}(f) \longrightarrow 0$$

(3) There is a commutative diagram:

$$\begin{array}{ccc} \mathcal{L}^{\cdot}_{\#} & \xrightarrow{\sigma} & \Omega^{\cdot}_{(0)}(A) \\ r \downarrow & & \downarrow R \\ \mathcal{L}^{\cdot}_{\#} & \xrightarrow{\sigma} & \Omega^{\cdot}_{(0)}(A) \end{array}$$

Proof: Suppose $z = \varphi\, e_{i_1} \wedge \cdots \wedge e_{i_s}$ is in $\mathcal{L}^{s}_{\#}$ with φ homogeneous of degree $m\lambda - s$. By the definition of $\mathcal{L}^{\cdot}_{\#}$, $\lambda > 0$. Let $\sigma(z) = (-1)^{\lambda-1}(\lambda-1)!\ \varphi/f^{\lambda}$. $dX_{i_1} \wedge \cdots \wedge dX_{i_s}$. Then σ is a degree 0 map $\mathcal{L}^{\cdot}_{\#} \longrightarrow \Omega^{\cdot}_{(0)}(A)$. σ is obviously onto. Since $\sigma \circ \Delta_0(z) = \sigma\,(\lambda+f)\ \varphi\, e_{i_1} \wedge \cdots \wedge e_{i_s} = 0$, $\sigma \circ \Delta_0 = 0$. It's not hard to see that $\ker \sigma = \text{image}\ \Delta$. To complete the proof of (1) we must show that $d\sigma = \sigma\delta$. Now:

$$d\sigma(z) = (-1)^{\lambda-1}(\lambda-1)!\ \{\ \Sigma\ \varphi_j/f^{\lambda}\ dX_j \wedge dX_{i_1} \wedge \cdots \wedge dX_{i_s}\} +$$

$$(-1)^{\lambda}\ \lambda!\ \ \{\ \Sigma\ \ \varphi\, f_j/f^{\lambda+1}\ dX_j \wedge dX_{i_1} \wedge \cdots \wedge dX_{i_s}\}$$

Since $\delta(z) = \Sigma\ (\varphi_j + f_j\ \varphi)\ e_j \wedge e_{i_1} \wedge \cdots \wedge e_{i_s}$, σ is indeed a chain map.

The above exact sequence of complexes gives a long exact sequence of cohomology. By Lemma 9.1 Δ_0 induces the 0 map on $H^{\cdot}_{\#}(f)$. (2) now follows from Lemma 9.2 (4). The proof of (3) is straightforward.

Corollary $H^0(f) = H^1(f) = 0$

Proof: Suppose $\varphi \in H^0(f)$. Then $\Delta_i(\varphi) = 0$ for $1 \leq i \leq n$. So

$m\Delta_0(\varphi) = \sum_1^n X_i \Delta_i (\varphi) = 0$. It follows that $\varphi = 0$, and that $H^0(f) = H^0_{\#}(f) = 0$.

Now it's easy to see that $H^0_{DR}(A) = k$. (If $\varphi \in A$, $\varphi \notin k$, then φ is part of a separating transcendence base of $k(X_1,\cdots,X_n)$ over k, there is a derivation of A non-trivial on φ, and $d\varphi \neq 0$). So by Theorem 9.1, $H^1_{\#}(f) = k$. Using the exact sequence of complexes $0 \longrightarrow \mathcal{L}^{\cdot}_{\#} \longrightarrow \mathcal{L}^{\cdot}(f) \longrightarrow k \longrightarrow 0$, we find that $H^1(f) = 0$.

Theorem 9.1 relates the $H^i(f)$ to the De Rham cohomology groups of A. One gets a nicer result by using the De Rham cohomology of $A_{(0)}$.

Lemma 9.3 The natural map $\Omega^{\cdot}(A_{(0)}) \longrightarrow \Omega^{\cdot}(A)$ is injective.

Proof: Let A' be the subring $\sum_{m|j} A_{(j)}$ of A. Then $A' = A_{(0)}[f,f^{-1}]$.

Since f is transcendental over $A_{(0)}$, A' is isomorphic with the ring $A_{(0)}[t,t^{-1}]$

So it suffices to show that $\Omega^{\cdot}(A') \longrightarrow \Omega^{\cdot}(A)$ is injective. Let K' and K be the quotient fields of A' and A; K is a finite separable extension of K'. It follows that $\Omega^{\cdot}(K') \longrightarrow \Omega^{\cdot}(K)$ is injective and that the kernel of the map $\Omega^{\cdot}(A') \longrightarrow \Omega^{\cdot}(A)$ is a torsion module. But A' is the co-ordinate ring of a non-singular k-variety. It follows that $\Omega^{\cdot}(A')$ is projective, and thus torsion free, proving the lemma. (One may also show by a direct calculation, localizing at X_j^m, that $\Omega^{\cdot}(A')$ is a locally free A' module).

From now on we shall view $\Omega^\cdot(A_{(0)})$ as a subcomplex of $\Omega^\cdot(A)$. Evidently $\Omega^\cdot(A_{(0)}) \subset \Omega^\cdot_{(0)}(A)$.

<u>Lemma 9.4</u> Any $\omega \in \Omega^\cdot_{(0)}(A)$ may be uniquely written as $\omega' + (\frac{df}{f} \wedge \omega'')$ with ω' and ω'' in $\Omega^\cdot(A_{(0)})$. If R is the map of Lemma 9.2, then R maps $\Omega^\cdot_{(0)}(A)$ into $\Omega^\cdot(A_{(0)})$.

<u>Proof</u>: Let S be the set of ω which may be written as above; S is a subalgebra of $\Omega^\cdot_{(0)}(A)$. If μ is a monomial of deg m in the X_i's , then

$$\frac{d\mu}{f} = d\left(\frac{\mu}{f}\right) + \frac{df}{f} \cdot \frac{\mu}{f}, \text{ so } \frac{d\mu}{f} \in S .$$

Let $\mu = X_i^{\,m}$ and $\mu' = X_i^{\,m-1} X_j$. Then $mX_i^{\,2m-1}\, dX_j = m\mu\, d\mu' - (m-1)\, \mu'\, d\mu$. It follows that $\frac{X_i^{\,2m-1}\, dX_j}{f^2} \in S$. From this we see that $\frac{\varphi}{f^\ell}\, dX_{i_1} \wedge \cdots \wedge dX_{i_s}$ is in S , provided $\deg \varphi = m\ell - s$ and ℓ is large. Thus $S = \Omega^\cdot_{(0)}(A)$.

Now if R is the map of Lemma 9.2, $R(A_{(0)}) = 0$. Since $dR + Rd = 0$ on $A_{(0)}$, R annihilates $dA_{(0)}$ as well. Using (1) and (2) of Lemma 9.3 we find that R annihilates $\Omega^\cdot(A_{(0)})$ and that $R(\omega) = R(\frac{df}{f}) \wedge \omega'' = m\omega''$. So ω'' is uniquely determined by ω , and the same is true of ω' . Finally, $m\omega''$ is in $\Omega^\cdot(A_{(0)})$.

<u>Theorem 9.2</u>

$$H^i_{DR}(A) \approx H^{i-1}_{DR}(A_{(0)}) \oplus H^i_{DR}(A_{(0)})$$

Proof: By Lemmas 9.3 and 9.4, $\Omega^{\cdot}_{(0)}(A)$ is a direct sum of 2 subcomplexes, one isomorphic to $\Omega^{\cdot}(A_{(0)})$ and the other isomorphic to $\Omega^{\cdot}(A_{(0)})$ shifted over by 1. Now apply Lemma 9.2, (4).

Theorems 9.1 and 9.2 suggest that $H^i_{\#}(f) \approx H^{i-1}_{DR}(A_{(0)})$. To get an explicit isomorphism we introduce one further map.

Definition Let $c_1 = 0$ and $c_\lambda = -(1 + \frac{1}{2} + \cdots + \frac{1}{\lambda-1})$ for $\lambda > 1$. Define $\gamma: \mathcal{L}^{\cdot}_{\#} \longrightarrow \mathcal{L}^{\cdot}_{\#}$ by:

$$\varphi\, e_{i_1} \wedge \cdots \wedge e_{i_s} \longrightarrow c_\lambda\ \varphi\, e_{i_1} \wedge \cdots \wedge e_{i_s}, \text{ for } \varphi \text{ homogeneous of}$$

degree $m\lambda - s$.

Lemma 9.5 If $z \in \mathcal{L}^{\cdot}_{\#}$, $\sigma(\gamma\delta - \delta\gamma)\, z = \frac{df}{f} \wedge \sigma(z)$

Proof: We may assume $z = \varphi\, e_{i_1} \wedge \cdots \wedge e_{i_s}$ with φ homogeneous of degree $m\lambda - s$. Then, $(\gamma\delta - \delta\gamma)z = (c_{\lambda+1} - c_\lambda) \cdot \sum_j f_j\, \varphi\, e_j \wedge e_{i_1} \wedge \cdots \wedge e_{i_s}$. So

$\sigma(\gamma\delta - \delta\gamma)z = (c_{\lambda+1} - c_\lambda) \cdot (-1)^\lambda \cdot \lambda! \cdot \frac{\varphi}{f^{\lambda+1}} \cdot \Sigma f_j\, dX_j \wedge dX_{i_1} \wedge \cdots \wedge dX_{i_s}$. Since $c_{\lambda+1} - c_\lambda = -\frac{1}{\lambda}$, this is just $\frac{df}{f} \wedge \sigma(z)$.

Lemma 9.6 The map $\sigma: \mathcal{L}^{\cdot}_{\#} \longrightarrow \Omega^{\cdot}_{(0)}(A)$ is chain homotopic to a map into the subcomplex $\frac{df}{f} \wedge \Omega^{\cdot}(A_{(0)})$ of $\Omega^{\cdot}_{(0)}(A)$.

Proof: $\sigma\, r\, \gamma$ is a degree -1 map $\mathcal{L}^{\cdot}_{\#} \longrightarrow \Omega^{\cdot}_{(0)}(A)$. Let us compute $d \circ (\sigma\, r\, \gamma) + (\sigma\, r\, \gamma) \circ \delta$. Since $d\sigma = \sigma\delta$, this may be rewritten as $\{\sigma\, (\delta r + r\delta)\, \gamma\} + \{\sigma r\, (\gamma\delta - \delta\gamma)\}$. By Lemma 9.1 and Theorem 9.1, $\sigma(\delta r + r\delta) = \sigma\, \Delta_0 = 0$ Furthermore $\sigma r = R\sigma$; it follows that $d \circ (\sigma\, r\, \gamma) + (\sigma\, r\, \gamma) \circ \delta$ maps z into $R\, \sigma\, (\gamma\delta - \delta\gamma)z = R\, (\frac{df}{f} \wedge \sigma\, (z))$ by Lemma 9.5. Using Lemma 9.2, we may rewrite this as $m\, \sigma\, (z) - \{\frac{df}{f} \wedge R\, \sigma\, (z)\}$. By Lemma 9.4, $R\, \sigma(z)$ is in $\Omega^{\cdot}(A_{(0)})$; it follows that $m^{-1}\, (\sigma\, r\, \gamma)$ provides the desired chain homotopy.

From now on we shall think of $H^i_{DR}(A_{(0)})$ and $H^{i-1}_{DR}(A_{(0)})$ as imbedded as complementary subspaces in $H^i_{DR}(A)$. (For an explicit description of the imbedding, look at the proof of Theorem 9.2.)

Lemma 9.7 The homomorphism ∂: $H^i_{DR}(A) \longrightarrow H^{i+1}_{\#}(f)$ of Theorem 9.1 maps $H^i_{DR}(A_{(0)})$ surjectively.

Proof: Suppose z is a cocycle in $\mathcal{L}^{i+1}_{\#}$. Set $\omega = R\, \sigma\, (z) = \sigma\, r\, (z)$. Then $\omega \in \Omega^i_{(0)}(A)$ and $d\omega = -Rd\, \sigma\, (z) = -R\, \sigma\, \delta(z) = 0$. Since $\omega \in$ image R , it represents a cohomology class in $H^i_{DR}(A_{(0)})$. Now $r\, (z)$ is a pull-back of ω by σ to $\mathcal{L}^i_{\#}$, and $\delta\, (r(z)) = (\delta r + r\delta)\, z = \Delta_0\, (z)$. The definition of the connecting homomorphism in an exact sequence of complexes then shows that ∂ maps the cohomology class of ω onto the cohomology class of z , proving the lemma.

Theorem 9.3

The map $\sigma^*: H^i_{\#}(f) \longrightarrow H^i_{DR}(A)$ of Theorem 9.1 maps $H^i_{\#}(f)$ isomorphically onto the subspace $H^{i-1}_{DR}(A_{(0)})$.

Proof: By Theorem 9.1, σ^* is injective; by Lemma 9.6 image $\sigma \subset H^{i-1}_{DR}(A_{(0)})$. Suppose $\alpha \in H^{i-1}_{DR}(A_{(0)})$. Let ∂ be the connecting homomorphism of Lemma 9.7. By Lemma 9.7 there is an α' in $H^i_{DR}(A_{(0)})$ such that $\partial(\alpha') = \partial(\alpha)$. So $\alpha - \alpha'$ is in the image of σ^*, $\alpha' = 0$, and the theorem follows.

Using the corollary to Theorem 9.1 and the fact that $H^i(f) = H^i_{\#}(f)$ for $i \geq 2$ we get:

Corollary $H^0(f) = H^1(f) = 0$. For $i \geq 2$, $H^i(f) \approx H^{i-1}_{DR}(A_{(0)})$.

Finally, since $H_i(f) \approx H^{n-i}(f)$:

Theorem 9.4

For $i \leq n-2$, $H_i(f) \approx H^{n-1-i}_{DR}(A_{(0)})$. $H_{n-1}(f) = H_n(f) = 0$.

Corollary Suppose f is non-singular. Then:

(1) $H^0_{DR}(A_{(0)}) = k$

(2) $H^i_{DR}(A_{(0)}) = 0$ for $1 \leq i \leq n-2$

(3) $H^{n-1}_{DR}(A_{(0)})$ has dimension $m^{-1}\{(m-1)^n + (-1)^n (m-1)\}$

Proof: (1) was proved in the course of proving the corollary to Theorem 9.1. (2) and (3) follow from Theorem 9.4 and the calculations of Chapter 8.

Suppose now that V is a non-singular variety over k. Then Grothendieck, (see [6]), has shown how to define algebraic De Rham cohomology groups $H^{\bullet}_{DR}(V)$; explicitly $H^{\bullet}_{DR}(V)$ is the hypercohomology of the complex of sheaves of differential forms on V. The assignment $V \longmapsto H^{\bullet}_{DR}(V)$ is functorial, and one gets a good cohomology theory for non-singular varieties. When V is affine with co-ordinate ring A, $H^i_{DR}(V) = H^i_{DR}(A)$. When k is the complexes, a comparison theorem of Grothendieck shows that $H^{\bullet}_{DR}(V)$ is just the classical cohomology of V, viewed as a complex manifold.

Now let U be the projective hypersurfacedefined by f. Theorem 9.4 shows that $H_i(f) \approx H^{n-1-i}_{DR}(A_{(0)}) \approx H^{n-1-i}_{DR}(\mathbb{P}^{n-1} - U)$ for $i \leq n-2$. So when $k = \mathbb{C}$, the $H_i(f)$ have a classical topological interpretation, and in any case they are related to a good cohomology theory for k-varieties. If U is non-singular one may use the corollary to Theorem 9.4 together with a Gysin sequence to calculate the groups $H^i_{DR}(U)$. In particular it can be shown that $H_0(f)$ imbeds as a sub-space of $H^{n-2}_{DR}(U)$ of codimension 0 or 1 according as n is odd or even. This result is due to Katz [7].

We next turn our attention to "analytic homology". Let K be a complete discretely normed field of characteristic 0 whose residue class field $\overline{K}$ has characteristic $p > 0$. Assume further that K contains a root π of $x^{p-1} = -p$. Let F be a homogeneous element of $\mathcal{O}_K[X_1, \cdots, X_n]$ of degree m such that $\overline{F} \neq 0$. In Chapter 7 we constructed a certain complex $\hat{\mathcal{L}}.$ from F; let $\hat{H}.(F)$ denote the homology of this complex.

Suppose first that the reduction $\bar{F}$ of F is non-singular and let U and $\bar{U}$ be the projective hypersurfaces determined by F and $\bar{F}$. By Theorems 8.3 and 8.7, $\dim \hat{H}_0(F) = \dim H_0(F) = m^{-1} \{(m-1)^n + (-1)^n (m-1)\}$. It's easy to see that $H_0(F) \longrightarrow \hat{H}_0(F)$ is onto and hence bijective. So we may identify $\hat{H}_0(F)$ with a subspace of $H_{DR}^{n-2}(U)$ of codimension 0 or 1. Assume now that $\bar{K} = GF(q)$, that characteristic $\bar{K} \neq 2$, and that the co-efficients of F satisfy $c^q = c$. Then we have constructed an operator α_* on $\hat{H}_0(F)$ and proved (see Theorem 8.8) that $N_s(\bar{U}) = \{q^{(n-2)s} + \cdots + 1\} + (-1)^n \operatorname{Tr}(q^{-1}\alpha_*)^s$. The Lefschetz fixed point theorem formalism then strongly suggests that $H_{DR}^{n-2}(U)$ should be thought of as an $n-2$ dimensional cohomology group of $\bar{U}$ with co-efficients in K, and that $q^{-1}\alpha_*$ should be the restriction to $\hat{H}_0(F)$ of a map $H_{DR}^{n-2}(U) \longrightarrow H_{DR}^{n-2}(U)$ induced by the Frobenius.

This circle of ideas has been developed in detail by Lubkin [8]. He has shown that if $\bar{V}$ is a non-singular projective variety over $\bar{K}$, then any two liftings of $\bar{V}$ to K have canonically isomorphic De Rham cohomology. Furthermore if $\bar{V}$ and $\bar{W}$ are non-singular projective with liftings V and W then any morphism $\bar{V} \longrightarrow \bar{W}$ induces a map $H^{\cdot}_{DR}(W) \longrightarrow H^{\cdot}_{DR}(V)$. In this way one gets a good cohomology theory $\bar{U} \longrightarrow H^{\cdot}_{Lub}(\bar{U}) = H^{\cdot}_{DR}(U)$ for liftable projective varieties over $\bar{K}$. When $\bar{U}$ is a non-singular projective hypersurface defined by $\bar{F}$, then as we have seen $\hat{H}_0(F)$ imbeds in $H_{Lub}^{n-2}(U)$. Presumably the map induced by the Frobenius in Lubkin's theory restricts to Dwork's $q^{-1}\alpha_*$.

Let us now turn to the case of an F whose reduction $\bar{F}$ may be singular. Let $\bar{U}$ be the projective hypersurface defined by $\bar{F}$. Theorem 9.4 suggests that $H_i(F)$, $(i \leq n-2)$, be thought of as an $n-1-i$ dimensional cohomology group, with co-efficients in K, of the affine variety $\mathbb{P}^{n-1}-\bar{U}$. When $\bar{F}$ is singular, the

$\hat{H}_i(F)$ are unreasonable however, and it is better to replace the complex $\hat{\mathcal{L}}.$ by a larger complex $\mathcal{L}.^+$ which we now describe.

Recall that $L \subset K[[X_0,\cdots,X_n]]$ is the Banach space having as orthonormal base the elements $\pi^{\lambda_0} X^\lambda$ with $m\lambda_0 = \sum_1^n \lambda_i$. More generally $L(\gamma)$ has as orthonormal base the elements $\pi^{[\gamma\lambda_0]} X^\lambda$ with $m\lambda_0 = \sum_1^n \lambda_i$. Let $L^+ = \bigcup_{\gamma>0} L(\gamma)$. Then L^+ is stable under the operators $D_i = (\exp -\pi X_0 F) \circ X_i \frac{\partial}{\partial X_i} \circ (\exp \pi X_0 F)$, and we may build a complex $\mathcal{L}.^+$ contained in $K.(L^+; D_1,\cdots,D_n)$ in the same way that we built $\hat{\mathcal{L}}. \subset K.(L; D_1,\cdots,D_n)$. Denote the homology of $\mathcal{L}.^+$ by $H.^+(F)$.

When $\overline{K}$ is finite one has an endomorphism $\Theta = (\exp - \pi X_0 F) \circ \psi \circ (\exp \pi X_0 F)$ of L^+ and a chain map $\alpha: \mathcal{L}.^+ \longrightarrow \mathcal{L}.^+$ as in Chapter 7. It may be shown that α_i and $(\alpha_i)_*$ are nuclear and that the Lefschetz fixed point theorem, Theorem 7.5, remains valid with $\hat{\mathcal{L}}.$ replaced by $\mathcal{L}.^+$ If $\overline{F}$ is non-singular it doesn't matter whether one works with $\hat{\mathcal{L}}.$ or $\mathcal{L}.^+$. Indeed one can show that $\hat{H}_i(F) \approx H_i^+(F)$ in this case. But this need not be true when $\overline{F}$ is singular. One final fact: the $H_i^+(F)$ only depend on the reduction of F . Indeed if F_1 and F_2 have the same reduction, then multiplication by $\exp \pi X_0 (F_1-F_2)$ sets up an isomorphism between the complexes $\mathcal{L}.^+$ attached to F_1 and F_2 .

Now for non-singular affine varieties over $\overline{K}$ (subject to a mild restriction), Washnitzer and I have developed a cohomology theory which we call "formal cohomology" ; the theory is of De Rham type and the co-efficient field is K . What one expects and can more or less prove is that the spaces $H_i^{+}(F)$ bear the same relation to formal cohomology that the $H_i(F)$ bear to De Rham cohomology. To make things more precise, let's adopt the language of [10]. If $\bar{A}$ is a $\bar{K}$-algebra which lifts very smoothly to $\mathcal{O}_K$ let $H^{\cdot}_{For}(\bar{A})$ denote the formal cohomology of $\bar{A}$ with co-efficients in K. Let $\bar{A}_{(0)}$ be the co-ordinate ring of $\mathbb{P}^{n-1} - \bar{U}$.

Theorem 9.5

Suppose that $\bar{A}_{(0)}$ lifts very smoothly. Then, for $i \leq n-2$, $H_i^{+}(F) \approx H_{For}^{n-1-i}(\bar{A}_{(0)})$. Furthermore $H_{n-1}^{+}(F) = H_n^{+}(F) = 0$.

Results of this sort were first proved by Katz in [7]. I suspect that $\bar{A}_{(0)}$ always lifts very smoothly, (it always has a weak formalization), but have been unable to prove this so far.

The proof of Theorem 9.5 is much like that of Theorem 9.4, but as it's analytically nasty we won't go into it. One final remark. Suppose that $\bar{K}$ is finite. Then under the identification of Theorem 9.5 the Dwork map $(\alpha_i)_*$ is essentially the inverse of the map induced by the Frobenius on $H_{For}^{n-1-i}(\bar{A}_{(0)})$, and the Lefschetz fixed point theorem, Theorem 7.5, becomes a special case of a result proved in [11].

Bibliography

[1] Bombieri, E. and Swinnerton-Dyer, H. P. F., "On the local zeta function of a cubic threefold," Ann. Scuola Norm. Sup. Pisa (3) 21 (1967) 1-29.

[2] Dwork, B., "On the rationality of the zeta function of an algebraic variety," Amer. Jour. Math. 82 (1960), 631-648.

[3] Dwork, B., "On the zeta function of a hypersurface," Pub. Math., I. H. E. S. Paris 12 (1962).

[4] Dwork, B., "On the zeta function of a hypersurface II," Ann. of Math. 80 (1964), 227-299.

[5] Grothendieck, A., "Sur une note de Mattuck-Tate," J. reine u. ang. Math. 200 (1958), 208-215.

[6] Grothendieck, A., "On the De Rham cohomology of algebraic varieties," Pub. Math., I. H. E. S. Paris 29 (1966).

[7] Katz, N., "On the differential equations satisfied by period matrices," Pub. Math., I. H. E. S. Paris 35 (1968).

[8] Lubkin, S., "A p-adic proof of Weil's conjectures," Ann. of Math. 87 (1968) 105-194; ibid 87 (1968) 195-225.

[9] Mumford, D., "Lectures on curves on an algebraic surface," Princeton Univ. Press (1966).

[10] Monsky, P. and Washnitzer, G., "Formal cohomology I," Ann. of Math. 88 (1968), 181-217.

[11] Monsky, P., "Formal cohomology III - Fixed point theorems," to appear in Ann. of Math.

[12] Serre, J. P., "Endomorphismes complètement continus des espaces de Banach p-adiques," Pub. Math., I. H. E. S. Paris 12 (1962).

[13] Weil, A., "Numbers of solutions of equations in finite fields," Bull. Amer. Math. Soc. 55 (1949) 497-508.

¥ 700 / $ 2.00

Printed by Akatsuki Art Printing Co. Ltd, Tokyo, Japan