PUBLICATIONS MATHÉMATIQUES DE L'I.H.É.S.

BERNARD DWORK

p-adic cycles

Publications mathématiques de l'I.H.É.S., tome 37 (1969), p. 27-115

<http://www.numdam.org/item?id=PMIHES_1969__37__27_0>

p-ADIC CYCLES

by B. DWORK

INTRODUCTION

In previous articles we studied the zeta function of a hypersurface defined over a finite field by choosing a lifting and associating certain spaces with the lifting. The basic idea of the present article is to replace a particular lifting by the set of all liftings. In this direction we consider a one-parameter family of non-singular hypersurfaces, and use the classical identification of homology classes of cycles of each fiber with period vectors relative to a fixed cohomology basis. The differential equations satisfied by these period vectors may be viewed p-adically and the space of local solutions (i.e. solutions holomorphic at all parameter values in characteristic zero with a given reduction) may be used as a model for the homology of the reduced fiber. In particular the " Frobenius " operates on the local solutions and the eigenvalues are the roots of the zeta function of the reduced fiber, if the latter is non-singular.

However the Frobenius also operates on the local solutions in the case of singular reduction and in this way the classical vanishing cycles appear in our theory. In certain cases the vanishing cycles can be prolonged p-adically. This phenomenon is used to explain a formula of Tate ([3], § 5) (also see equation (6.29) below) which gives for an algebraic family of elliptic curves the unit root of the zeta function of the reduced curves in terms of a classical formula for the period of the differential of the first kind. This is a more subtle type of result than the results of Katz and of the author ([4], [8], [17]) which give a connection between period matrices and holomorphic matrix functions which specialize to matrices whose characteristic polynomial give the zeta function. The formula of Tate may be viewed as a more precise form (in this special case) of results of Manin [11] which give a similar formula modulo p.

Very little is known as to whether a given locally presented function has an analytic continuation in the sense of Krasner [9]. In §§ 1, 2, 3, we find a narrow class of functions which have such continuations. This provides the function theoretic basis for our examples.

Although the question is still open, we do not make a precise conjecture as to whether vanishing cycles can " generally " be prolonged. In the elliptic case it is shown that there is p-adically just one vanishing cycle and that it is the only cycle that can be prolonged. For families of curves of higher genus we expect (following Manin) that there is a subspace (prolongable as a subspace) of dimension equal to the stable rank of the Hasse-Witt matrix of the reduction of the generic curve of the family.

It seems unlikely that the theory should be dominated by the Hasse-Witt matrix in the case of dimension greater than one. For surfaces we see that algebraic solutions also appear (§ 6j below) and for dimension greater than two we may expect new phenomena.

Let us understand a p-adic Zariski open subset of the parameter space to mean the

lifting to characteristic zero of a Zariski open subset of the parameter space. We can formulate the general questions:

1. Can the local solution spaces of the Fuchs-Picard differential equation be filtered in a " globally uniform way " by means of systems of differential equations of lower " ranks " with coefficients holomorphic in a p-adic Zariski open subset of the parameter space? (Of course the filtration is to be stable under the Frobenius mapping.)

2. Can this filtration be characterized locally by p-adic analytic properties such as growth conditions, boundedness, etc?

In this article we give an initial discussion of these questions. The elliptic case is discussed at some length in §§ 4, 7, 8. We are led to a p-adic analogue of $q(=e^{\pi i\tau})$ which no doubt is the same as an unpublished one proposed by Serre and Tate. We use this analogue to give (§ 7) a new proof of a conjecture of Tate along lines proposed by Katz. The main purpose of §§ 7, 8, aside from demonstrating the usefulness of this definition of q, is to investigate cycles of elliptic curves in the case of supersingular reduction. We find some evidence to support Washnitzer's suggestion that a p-adic monodromy theory depends upon behavior near supersingular moduli. Finally we note that in the elliptic case the eigenvectors themselves are found to have arithmetic significance. This seems to be a new phenomenon and its investigation in other situations should prove interesting.

The help received from N. Katz will be obvious to the reader. I am also indebted to L. Ehrenpreis, P. Griffiths and G. Washnitzer for numerous discussions of these questions.

§ o. Theory of Krasner.

For ease of reference we recall [9] some facts and definitions from Krasner's theory of uniform analytic functions. For simplicity we restrict our attention to a field Ω, of characteristic zero, complete under a non-archimedean valuation having countable value group and countable residue class field.

1. A set $\mathfrak{D}$ in $\Omega \cup \{\infty\}$ is said to be *ultra open* about $\alpha \in \Omega$ if for each $\xi \in \mathfrak{D}$, the distance $|x-\alpha|$ assumes only a finite set of values less than $|\xi-\alpha|$ as x runs through the complement of $\mathfrak{D}$.

2. The set $\mathfrak{D}$ is said to be *quasi connected* if it is ultra open about each $\alpha \in \mathfrak{D} \cap \Omega$.

3. A family $\mathfrak{F}$ of subsets of $\Omega \cup \{\infty\}$ is said to be *chained* if for each $A, B \in \mathfrak{F}$, there exist elements $C_0, C_1, \ldots, C_m$ in $\mathfrak{F}$ such that $A = C_0$, $B = C_m$ and $C_i \cap C_{i+1} \neq \emptyset$ for $i = 0, 1, \ldots, m-1$.

4. If $\mathfrak{D}$ is a quasi connected set, an *analytic element* f of *support* $\mathfrak{D}$ is a mapping of $\mathfrak{D}$ into Ω which lies in the closure under the topology of uniform convergence on $\mathfrak{D}$ of the set of all rational functions having no pole in $\mathfrak{D}$.

5. (Uniqueness Theorem). — If f, f^* are analytic elements with non-disjoint supports $\mathfrak{D}, \mathfrak{D}^*$ then f and f^* coincide on $\mathfrak{D} \cap \mathfrak{D}^*$ if they coincide on a subset which has a limit point in $\mathfrak{D} \cap \mathfrak{D}^*$.

6. Two analytic elements f, f^* of supports $\mathfrak{D}, \mathfrak{D}^*$ are said to be *equivalent* if there exists a sequence $f_0, f_1, \ldots, f_m$ of analytic elements such that $f_0 = f, f^* = f_m$, such that the intersection of the supports of f_i, f_{i+1} is non-empty for $i = 0, 1, \ldots, m-1$ and such that f_i coincides with f_{i+1} on the intersection of their supports.

7. Let F be an equivalence class of analytic elements, and let $\mathfrak{D}(F)$ be the union of the supports of the elements of the class. If $x \in \mathfrak{D}(F)$ then $f(x)$ is independent of f as f ranges over all elements of F such that x lies in support of f. Thus F is a single valued function on D(F), which is called a *uniform* analytic function of *support* D(F).

Examples. — *a)* Let $\mathfrak{D} = \mathfrak{P}$, the maximal ideal of the ring of integers $\mathfrak{O}$ of Ω. Let $f(x) = \sum_{j=0}^{\infty} a_j x^j$, $\limsup_{j \to \infty} |a_j| = 1$. Clearly f converges on $\mathfrak{P}$, but need not converge uniformly. Thus f need not be an analytic element of support $\mathfrak{P}$. However by using an infinite sequence $(n = 2, 3, \ldots)$

$$\mathfrak{D}_n = \{x \mid |x| \leq 1 - n^{-1}\}$$

of open disks which form a chained family and letting f_n be the restriction of f to $\mathfrak{D}_n$, we see that $\{f_n\}_{n \geq 2}$ lies in an equivalence class of analytic elements so that f is a uniform analytic function of support $\mathfrak{P}$.

b) The union, $\mathfrak{D}$, of the disjoint sets $\mathfrak{P}$, $1 - \mathfrak{P}$ is quasi connected. We may define a function f on $\mathfrak{D}$ by setting

$$f(x) = \sum_{j=0}^{\infty} a_j (x(1-x))^j$$

and let us again assume that $\limsup_{j \to \infty} |a_j| = 1$. The restriction of f to either $\mathfrak{P}$ or $1 - \mathfrak{P}$ is by the above remarks a uniform analytic function but these restrictions need not be equivalent.

§ 1. Binomial type numbers.

We recall that in the theory of hypergeometric series it is customary to write for arbitrary θ and each non-negative integer, n,

$$(\theta)_n = \begin{cases} 1 & \text{for } n = 0 \\ \prod_{\nu=0}^{n-1} (\theta + \nu) & \text{for } n > 0. \end{cases}$$

In this section we shall assume that p is a fixed prime number and that θ is a rational number, which is a p-adic integer but is neither zero nor a negative rational integer. Thus $(\theta)_n$ is never zero. For convenience of typography we will write $C_\theta(n)$ for $(\theta)_n$ and will investigate certain congruence properties of these numbers. We define θ' to be that unique rational number, integral at p, such that $p\theta' - \theta$ is an ordinary integer in $[0, p-1]$. (Thus for $\theta = 1, \theta' = 1$; for $\theta = 1/2, \theta' = 1/2$ $(p \neq 2)$ while for $\theta = 1/3$ $(p \neq 3)$, $\theta' = 1/3$ (resp. $2/3$) if $p \equiv 1$ (resp. -1) modulo 3.)

For each real x put

$$\rho(x)=\begin{cases}0 & \text{if } x\leq 0\\ 1 & \text{if } x>0\end{cases}$$

Lemma 1. — *If a, μ, s are non-negative ordinary integers, $0\leq a<p$ then*

$$\frac{C_\theta(a+\mu p+mp^{s+1})}{C_{\theta'}(\mu+mp^s)}\equiv\frac{C_\theta(mp^{s+1})}{C_{\theta'}(mp^s)}\,\frac{C_\theta(a+\mu p)}{C_{\theta'}(\mu)}\left(1+\frac{mp^s}{\theta'+\mu}\right)^{\rho(a+\theta-p\theta')}\quad \bmod 1+p^{s+1}, \tag{1.1}$$

(a multiplicative congruence). Furthermore

$$\frac{C_\theta(mp^{s+1})}{C_{\theta'}(mp^s)}\equiv((-p)^{p^s}u_s)^m\quad \bmod 1+p^{s+1} \tag{1.2}$$

where $u_s=+1$ unless both $p=2$, $s=1$, in which case $u_s=-1$. Finally

$$\operatorname{ord}_p\frac{C_\theta(a+\mu p)}{C_{\theta'}(\mu)}=\mu+(1+\operatorname{ord}(\mu+\theta'))\rho(a+\theta-p\theta'). \tag{1.3}$$

Proof. — From the definition

$$C_\theta(a+\mu p+mp^{s+1})/C_\theta(mp^{s+1})=\prod_{\nu=0}^{a+\mu p-1}(\theta+mp^{s+1}+\nu)$$

and hence

$$C_\theta(a+\mu p+mp^{s+1})/(C_\theta(mp^{s+1})\,C_\theta(a+\mu p))=\prod_{\nu=0}^{a+\mu p-1}\left(1+\frac{mp^{s+1}}{\theta+\nu}\right). \tag{1.4}$$

To compute this modulo p^{s+1} we need all ν such that

(i) $$0\leq\nu\leq a+\mu p-1$$

(ii) $$\theta+\nu\equiv 0\quad \bmod p.$$

The second condition implies that $\nu=(p\theta'-\theta)+pt$, $t\in\mathbf{Z}$ and the first condition implies that $t\geq 0$,

(iii) $$p(\mu-t)\geq(p\theta'-\theta)-(a-1).$$

This last condition holds for $\mu>t$, while for $\mu=t$ this holds only if $a>p\theta'-\theta$. Thus modulo $1+p^{s+1}$, the right side of (1.4) is

$$\prod_{t=0}^{\mu-1}\left(1+\frac{mp^s}{t+\theta'}\right)\cdot\left(1+\frac{mp^s}{\mu+\theta'}\right)^{\rho(a+\theta-p\theta')}.$$

Since (1.4) is also valid for all positive values of a, we have

$$C_{\theta'}(\mu+mp^s)/(C_{\theta'}(mp^s)C_{\theta'}(\mu))=\prod_{\nu=0}^{\mu-1}\left(1+\frac{mp^s}{\theta'+\nu}\right). \tag{1.5}$$

Comparing this with our evaluation of the right side of (1.4), gives (1.1).

If we put $a=0$, $\mu=p^s$ in (1.1), (since $\rho(\theta-p\theta')=0$), we obtain

$$\frac{C_\theta((m+1)p^{s+1})}{C_{\theta'}((m+1)p^s)} \equiv \frac{C_\theta(mp^{s+1})}{C_{\theta'}(mp^s)} \frac{C_\theta(p^{s+1})}{C_{\theta'}(p^s)} \mod 1+p^{s+1} \tag{1.6}$$

and hence the proof of (1.2) may be reduced to the case $m=1$ which we now consider.

Let $v_{s+1}=C_\theta(p^{s+1})/C_{\theta'}(p^s)$. We must show

$$v_{s+1} \equiv (-p)^{p^s} u_s \mod 1+p^{s+1}. \tag{1.7}$$

Case 1 ($s=0$). — $C_\theta(p)$ is a product of p factors which give a full set of representatives of the residue classes of $\mathbf{Z}$ modulo p. The product of the representatives of the non-zero classes is congruent modulo p to -1 while the representative of the zero class is $\theta+(p\theta'-\theta)=p\theta'$. Hence

$$C_\theta(p) \equiv (-p)\theta' \quad \text{modulo } 1+p.$$

Since $C_{\theta'}(1)=\theta'$, it is clear that (1.7) holds for $s=0$.

Case 2 ($s\geq 1$). — For $0\leq \nu<p^{s+1}$ we may write ν uniquely as $j+bp^s$ with $0\leq j<p^s$, $0\leq b<p$ and hence

$$C_\theta(p^{s+1}) = \prod_{j=0}^{p^s-1} \prod_{b=0}^{p-1} (\theta+j+bp^s).$$

We partition the range of j into integers congruent to $-\theta \bmod p$ and into integers not congruent to $-\theta \bmod p$, so that

$$C_\theta(p^{s+1}) = \prod_{j=0}^{p^s-1}{}' \prod_{b=0}^{p-1} (\theta+j+bp^s) \cdot \prod_{j=0}^{p^s-1}{}'' \prod_{b=0}^{p-1} (\theta+j+bp^s) \tag{1.8}$$

where, in Π', j is restricted so that $j+\theta\equiv 0 \bmod p$, and in Π'', j is restricted so that $j+\theta\not\equiv 0$.

The first product on the right side of (1.8) may be evaluated by noting that $j\equiv-\theta \bmod p$, $j\leq p^s-1$ is equivalent to the conditions $j=(p\theta'-\theta)+pt$, $0\leq t\leq p^{s-1}-1$. Thus the product in question is

$$\prod_{b=0}^{p-1} \prod_{t=0}^{p^{s-1}-1} (p\theta'+pt+bp^s) = p^{p^s} C_{\theta'}(p^s).$$

For the second factor on the right side of (1.8), we note that if x is a p-adic integer then

$$\prod_{b=0}^{p-1} (x+bp^s) \equiv \prod_{\omega^p=\omega} (x-\omega p^s) \mod p^{s+1}$$

where the right hand product is over the roots of $x^p-x=0$ in Ω, and hence is equal to $x^p-(p^s)^{p-1}x$. This is congruent mod p^{s+1} to

$$x^p \cdot \begin{cases} 1 & \text{if } p\neq 2 \\ 1+\dfrac{p^s}{x} & \text{if } p=2. \end{cases}$$

We may thus deduce from (1.8) that modulo $1+p^{s+1}$

$$v_{s+1}/p^{p^s} \equiv \prod_{j=0}^{p^s-1}{}''(\theta+j)^p \cdot \begin{cases} 1 & \text{if } p \neq 2 \\ \prod_{j=0}^{p^s-1}{}''\left(1+\frac{2^s}{\theta+j}\right) & \text{if } p=2. \end{cases} \tag{1.9}$$

In the same way the product formula for $C_\theta(p^s)$ can be decomposed

$$C_\theta(p^s) = \prod_{j=0}^{p^s-1}{}'(j+\theta) \cdot \prod_{j=0}^{p^s-1}{}''(j+\theta) \tag{1.10}$$

and the evaluation of the first product of the right hand side of (1.8) may be applied to the product Π' in (1.10) to give $p^{p^{s-1}} C_{\theta'}(p^{s-1})$ and hence

$$v_s/p^{p^{s-1}} = \prod_{j=0}^{p^s-1}{}''(\theta+j). \tag{1.11}$$

Comparing (1.9) with (1.11), we see that modulo $1+p^{s+1}$

$$v_{s+1}/v_s^p \equiv \begin{cases} 1 & p \neq 2 \\ \prod_{j=0}^{2^s-1}{}''\left(1+\frac{2^s}{\theta+j}\right) & p=2. \end{cases} \tag{1.12}$$

Now for $p=2$, the product Π'' on the right side of (1.12) is congruent mod 2^{s+1} to $1+2^s \sum_{j=0}^{2^s-1}{}'' \frac{1}{\theta+j}$, where Σ'' denotes again that $\theta+j \not\equiv 0 \bmod 2$. This means that $\theta+j \equiv 1 \bmod 2$ for each j in the range of summation and that there are 2^{s-1} terms in the sum. Thus the sum is congruent to $2^{s-1} \bmod 2$. If $s \geq 2$, the right side of (1.12) ($p=2$) reduces to $1 \bmod p^{s+1}$, while for $s=1$, we obtain $1+2 \equiv -1 \bmod 2^2$. Thus we have shown for $s \geq 1$,

$$v_{s+1} \equiv v_s^p u_s \mod 1+p^{s+1}.$$

Equation (1.7) now follows easily from the case $s=0$.

We now consider the proof of (1.3). We write

$$\theta'-1 = \sum_{s=0}^{\infty} \beta_s p^s \tag{1.13}$$

where for each s, $0 \leq \beta_s \leq p-1$. We choose α, $0 \leq \alpha \leq p-1$ such that

$$\theta-1 \equiv \alpha \mod p$$

and conclude that

$$\theta-1 = \alpha + \sum_{s=0}^{\infty} \beta_s p^{s+1} \tag{1.14}$$

since $(p-1)-\alpha$ lies in $[0, p-1]$, is an ordinary integer and is congruent to $-\theta$ modulo p. For each integer $r \geq 2$ let

$$\theta_r = 1 + \alpha + \sum_{s=0}^{r-2} \beta_s p^{s+1}$$

$$\theta'_r = 1 + \sum_{s=0}^{r-1} \beta_s p^s.$$

We first note that there exists no integer t such that $\beta_s = p-1$ for all $s \geq t$, as otherwise

$$\theta' - 1 = \sum_{s=0}^{t-1} \beta_s p^{s-1} + (p-1)p^t \sum_{j=0}^{\infty} p^j = \sum_{s=0}^{t-1} \beta_s p^{s-1} - p^t,$$

a strictly negative integer and hence θ' is an ordinary integer, $\theta' \leq 0$, and thus the same holds for $\theta = p\theta' - (p-1-\alpha)$, contrary to hypothesis.

We now observe that given an integer μ, then for r large enough

$$\mu + \sum_{s=0}^{r-2} \beta_s p^s < p^{r-1} \tag{1.15}$$

since by the previous remark there exists an integer i such that $\mu \leq p^i$ and such that $\beta_i \leq p-2$. If we choose $r \geq i+2$ then the left side of (1.15) is not greater than

$$p^i + (p-1)\sum_{s=0}^{r-2} p^s - p^i = p^{r-1} - 1 < p^{r-1}.$$

We recall the formula of Gauss

$$(p-1)\ \mathrm{ord}\ n! = n - S(n), \tag{1.16}$$

where for $n = a_0 + a_1 p + \ldots + a_{m-1}p^{m-1}$, $0 \leq a_j \leq p-1$,

$$S(n) = \sum_{j=0}^{m-1} a_i.$$

Since $C_\theta(n)$ is for fixed n, a continuous (p-adic) function of θ which never takes on the value zero, we know that both $C_\theta(n)/C_{\theta_r}(n)$ and $C_{\theta'}(n)/C_{\theta'_r}(n)$ are units for all r large enough. Since $C_{\theta_r}(n) = (\theta_r - 1 + n)!/(\theta_r - 1)!$, we conclude with the aid of (1.16) that for r large,

$$(p-1)\left(\mathrm{ord}\,\frac{C_\theta(a+\mu p)}{C_{\theta'}(\mu)} - \mu\right) = a + S(\theta'_r + \mu - 1) - S(\theta_r + a + \mu p - 1) + S(\theta_r - 1) - S(\theta'_r - 1). \tag{1.17}$$

It follows from the definitions that

$$S(\theta_r - 1) - S(\theta'_r - 1) = \alpha - \beta_{r-1}. \tag{1.18}$$

Case 1 ($a + \alpha < p$). — In this case we write

$$\theta_r - 1 + a + \mu p = (a+\alpha) + p(\mu + \sum_{s=0}^{r-2} \beta_s p^s)$$

and since $a+\alpha<p$, we have

$$\mathbf{(1.19)} \qquad S(\theta_r - 1 + a + \mu p) = a + \alpha + S(\mu + \sum_{s=0}^{r-2} \beta_s p^s).$$

On the other hand

$$\mu + \theta'_r - 1 = (\mu + \sum_{s=0}^{r-2} \beta_s p^s) + \beta_{r-1} p^{r-1},$$

and hence if r is so large that (1.15) holds, then

$$\mathbf{(1.20)} \qquad S(\mu + \theta'_r - 1) = S(\mu + \sum_{s=0}^{r-2} \beta_s p^s) + \beta_{r-1}.$$

It follows from equations (1.18), (1.19), (1.20) that the right side of (1.17) is zero in this case, which coincides with (1.3) in this case.

Case 2 ($a+\alpha>p$). — In this case we write

$$\theta_r - 1 + a + \mu p = (a + \alpha - p) + p(1 + \mu + \sum_{s=0}^{r-2} \beta_s p^s)$$

and conclude

$$\mathbf{(1.19)'} \qquad S(\theta_r - 1 + a + \mu p) = a + \alpha - p + S(1 + \mu + \sum_{s=0}^{r-2} \beta_s p^s).$$

On the other hand

$$\mu + \theta'_r = (1 + \mu + \sum_{s=0}^{r-2} \beta_s p^s) + p^{r-1} \beta_{r-1}$$

and hence if we choose r so large that (1.15) holds with μ replaced by $\mu+1$, then

$$\mathbf{(1.20)'} \qquad S(\mu + \theta'_r) = S(1 + \mu + \sum_{s=0}^{r-2} \beta_s p^s) + \beta_{r-1}.$$

It follows from equations (1.18), (1.19)', (1.20)' that the right side of (1.17) is

$$u = p + S(\theta'_r + \mu - 1) - S(\theta'_r + \mu).$$

If $\mu + \theta'_r \not\equiv 0 \bmod p$ then $S(\theta'_r + \mu - 1) = S(\theta'_r + \mu) - 1$ and hence

$$u = p - 1 = (p-1)(1 + \operatorname{ord}(\mu + \theta')).$$

If on the contrary, $\operatorname{ord}(\mu + \theta') = \nu > 0$, then for r large enough,

$$\mu + \theta'_r = p^\nu (T + 1),$$

where T is a non-negative ordinary integer, $T+1 \not\equiv 0 \bmod p$. Thus

$$\mu + \theta'_r - 1 = (p^\nu - 1) + p^\nu T$$

and hence

$$S(\mu + \theta'_r) = S(T+1)$$

$$S(\mu + \theta'_r - 1) = (p-1)\nu + S(T).$$

Since $T+1 \not\equiv 0 \bmod p$, $S(T+1)=S(T)+1$ and hence

$$u=(p-1)(1+\operatorname{ord}(\theta'+\mu)).$$

This completes the proof of (1.3) and hence of the lemma.

Corollary 1. — Again let θ be a rational number which is neither zero nor an ordinary negative integer but is a p-adic integer. Let $A_\theta(n)=C_\theta(n)/n!$, then for all n, m, s in $\mathbf{Z}_+$:

(i) $A_\theta(n)/A_{\theta'}\left(\left[\frac{n}{p}\right]\right)$ *is a p-adic integer;*

(ii) $$\frac{A_\theta(n+mp^{s+1})}{A_{\theta'}\left(\left[\frac{n}{p}\right]+mp^s\right)} \equiv \frac{A_\theta(n)}{A_{\theta'}\left(\left[\frac{n}{p}\right]\right)} \mod p^{s+1} \quad \textit{(additive congruence).}$$

Proof. — The first assertion follows from (1.3) which shows that

$$\operatorname{ord} C_\theta(n)/C_{\theta'}\left(\left[\frac{n}{p}\right]\right) \geq \left[\frac{n}{p}\right],$$

while

$$\operatorname{ord}\left(n!/\left[\frac{n}{p}\right]!\right)=\left[\frac{n}{p}\right].$$

For the second assertion, we write $n=a+\mu p$, $\theta \leq a \leq p-1$ and apply equations (1.1), (1.2) to C_θ and C_1. Since u_s is independent of θ, the left side of (ii) is congruent modulo $1+p^{s+1}$ to

$$u=(A_\theta(a+\mu p)/A_{\theta'}(\mu))\left(1+\frac{mp^s}{\theta'+\mu}\right)^{p(a+\theta-p\theta')}.$$

Assertion (ii) is now clear if $a \leq p\theta'-\theta$ (in that case the congruence is also valid multiplicatively) while if $a > p\theta'-\theta$, we use equation (1.3) to compute

$$\operatorname{ord}\frac{A_\theta(a+\mu p)}{A_{\theta'}(\mu)} = 1+\operatorname{ord}(\theta'+\mu). \tag{1.21}$$

In this case $u-A_\theta(a+\mu p)/A_{\theta'}(\mu)=\frac{A_\theta(a+\mu p)}{A_{\theta'}(\mu)}\frac{mp^s}{\theta'+\mu}$ and it follows from (1.21) that the right side is congruent to zero modulo p^{s+1}. This completes the proof.

Corollary 2. — Let $\theta_1, \ldots, \theta_r$ be rational p-adic integers, none of which are zero or ordinary negative integers. For $n \in \mathbf{Z}_+$, let

$$A(n)=\prod_{\iota=1}^{r} A_{\theta_\iota}(n), \qquad B(n)=\prod_{\iota=1}^{r} A_{\theta_\iota'}(n).$$

Then

(i) $A(n)/B\left(\left[\frac{n}{p}\right]\right)$ *is a p-adic integer;*

(ii) $A(n+mp^{s+1})/B\left(\left[\frac{n}{p}\right]+mp^s\right) \equiv A(n)/B\left(\left[\frac{n}{p}\right]\right) \mod p^{s+1}$.

§ 2. A Formal Congruence.

Our purpose (§ 3) is to exhibit a class of functions having a non-obvious analytic continuation in the Krasner sense. With this object in mind we demonstrate a formal congruence between power series. (A special case was stated in [3], equation (12).)

Theorem 2. — *Let* $A, B = B^{(0)}, B^{(1)}, B^{(2)}, \ldots$ *be a sequence of* Ω *valued functions on* $\mathbf{Z}_+$. *Put*

$$F(X) = \sum_{n=0}^{\infty} A(n)X^n, \qquad G(X) = \sum_{n=0}^{\infty} B(n)X^n.$$

To simplify the statement of our hypotheses, we write $A = B^{(-1)}$. *We assume for all* n, m, s *in* $\mathbf{Z}_+$, $i \geq -1$:

a) $$\frac{B^{(i)}(n+mp^{s+1})}{B^{(i+1)}\left(\left[\frac{n}{p}\right]+mp^s\right)} \equiv \frac{B^{(i)}(n)}{B^{(i+1)}\left(\left[\frac{n}{p}\right]\right)} \mod p^{s+1}.$$

b) $B^{(i)}(n)/B^{(i+1)}\left(\left[\frac{n}{p}\right]\right) \in \mathfrak{O}$ *for all* $i \geq -1$, $n \in \mathbf{Z}_+$.

c) $B^{(i)}(n) \in \mathfrak{O}$ *for all* $i \geq -1$, $n \in \mathbf{Z}_+$.

d) $B^{(i)}(0)$ *is a unit for all* $i \geq -1$.

Then

$$\text{(2.1)} \quad F(X) \sum_{j=mp^s}^{(m+1)p^s-1} B(j)X^{pj} \equiv G(X^p) \sum_{j=mp^{s+1}}^{(m+1)p^{s+1}-1} A(j)X^j \mod B^{(s)}(m)p^{s+1}[[X]].$$

Note. — The hypotheses are not independent, in fact *c)* is a consequence of the other three.

Proof. — Let $n = pN + a$, $0 \leq a \leq p-1$. The coefficients of X^n on the left side of (2.1) is

$$\sum_{j=mp^s}^{(m+1)p^s-1} A(n-pj)B(j),$$

while the coefficient of X^n on the right side of (2.1) is

$$\sum_{j=mp^s}^{(m+1)p^s-1} B(N-j)A(a+pj).$$

Let
$$U_a(j, N) = A(a+p(N-j))B(j) - B(N-j)A(a+pj)$$
$$H_a(m, s, N) = \sum_{j=mp^s}^{(m+1)p^s-1} U_a(j, N).$$

The theorem is equivalent to the assertion that

$$\text{(2.2)} \qquad H_a(m, s, N) \in p^{s+1}B^{(s)}(m) \quad \text{for } s \geq 0, m \geq 0, N \geq 0.$$

We may extend our functions $B^{(i)}(n)$ defined on $\mathbf{Z}_+$ to functions defined on $\mathbf{Z}$ by setting $B^{(i)}(n) = 0$ for $n < 0$, $i \geq -1$.

Since $a\in[0, p-1]$, it is clear that

$$\mathbf{(2.3)} \qquad U_a(j, N)=0 \quad \text{for } j>N$$

and hence

$$\mathbf{(2.4)} \qquad H_a(m, s, N)=0 \quad \text{for } N<mp^s.$$

In preparation for the proof of (2.2) we record and prove some elementary facts.

$$\mathbf{(2.5)} \qquad \sum_{m=0}^{T} H_a(m, s, N)=0 \quad \text{if } (T+1)p^s>N$$

$$\mathbf{(2.6)} \qquad H_a(m, s, N)=\sum_{\mu=0}^{p-1} H_a(\mu+mp, s-1, N) \quad \text{if } s\geq 1$$

$$\mathbf{(2.7)} \qquad B^{(t)}(i+mp^s)\equiv 0 \mod B^{(s+t)}(m) \quad \text{if } 0\leq i\leq p^s-1,\ t\geq -1,\ s\geq 0.$$

To prove (2.5) we first note that the left side of (2.5) is

$$\sum_{m=0}^{T} \sum_{j=mp^s}^{(m+1)p^s-1} U_a(j, N)=\sum_{j=0}^{(T+1)p^s-1} U_a(j, N),$$

and since $(T+1)p^s-1\geq N$, equation (2.3) shows that this last sum is the same as

$$\sum_{j=0}^{N} U_a(j, N).$$

From the definition $\qquad U_a(j, N)=-U_a(N-j, N)$

and hence the last mentioned sum is equal to its negative and hence is zero as asserted.

To prove (2.6), we first note that by a change in the index of summation:

$$H_a(m, s, N)=\sum_{j=0}^{p^s-1} U_a(j+mp^s, N).$$

If we now put $j=i+\mu p^{s-1}$, the sum may be written, for $s\geq 1$, as

$$\sum_{\mu=0}^{p-1} \sum_{i=0}^{p^{s-1}-1} U_a(i+(\mu+mp)p^{s-1}, N).$$

Equation (2.6) is now obvious.

For equation (2.7), we first note that the assertion is trivial for $s=0$, while for $s\geq 1$, under the hypothesis on i, $[i/p^s]=0$ and hence

$$B^{(t)}(i+mp^s)/B^{(s+t)}(m)=\prod_{\nu=0}^{s-1} B^{(t+\nu)}([i/p^\nu]+mp^{s-\nu})/B^{(t+\nu+1)}([i/p^{\nu+1}]+mp^{s-\nu-1}).$$

Since $[i/p^{\nu+1}]=[[i/p^\nu]/p]$, each of the fractions in the product (by hypothesis *b)*) lies in $\mathfrak{O}$. This proves (2.7).

We now prove (2.2) for $s=0$. By equation (2.4) we may assume $N\geq m$. By hypothesis *a)*

$$A(a+p(N-m))/B(N-m)\equiv A(a)/B(0) \mod p$$

$$A(a+pm)/B(m)\equiv A(a)/B(0) \mod p$$

and hence $$U_a(m, N)/B(m)B(N-m)\equiv 0 \mod p$$

and so by hypothesis *c)*

$$U_a(m, N)\equiv 0 \mod pB(m).$$

Equation (2.2) for $s=0$ now follows from the fact that $H_a(m, 0, N)=U_a(m, N)$.

We now use induction on s. We write the induction hypothesis

$$(\alpha)_s : H_a(m, u, N)\equiv 0 \mod p^{u+1}B^{(u)}(m) \text{ for } 0\leq u<s,\ m\geq 0, \text{ all } N\in\mathbf{Z}.$$

Since we have checked $(\alpha)_1$, we may assume $(\alpha)_s$ for fixed $s\geq 1$. The main step is to show for $0\leq t\leq s$ that

$$(\beta)_{t,s} : H_a(m, s, N+mp^s)\equiv \sum_{j=0}^{p^{s-t}-1} B^{(t)}(j+mp^{s-t})H_a(j, t, N)/B^{(t)}(j) \mod p^{s+1}B^{(s)}(m).$$

We first prove $(\beta)_{0,s}$. We know that

$$H_a(m, s, N+mp^s)=\sum_{j=0}^{p^s-1} U_a(j+mp^s, N+mp^s)$$

and

(2.8) $$U_a(j+mp^s, N+mp^s)=(A(a+p(N-j))B(j)+mp^s)-B(N-j)A(a+pj+mp^{s+1}).$$

Using hypothesis *a)*:

$$A(a+pj+mp^{s+1})=(A(a+pj)B(j+mp^s)/B(j))+X_jp^{s+1}B(j+mp^s),$$

where $X_j\in\mathfrak{O}$, so that the right side of (2.8) is

$$B(j+mp^s)((U_a(j, N)/B(j))-p^{s+1}X_jB(N-j)).$$

Since $U_a(j, N)=H_a(j, 0, N)$, it is clear that

$$H_a(m, s, N+mp^s)=\sum_{j=0}^{p^s-1} B(j+mp^s)(H_a(j, 0, N)/B(j))-p^{s+1}\sum_{j=0}^{p^s-1} X_jB(j+mp^s)B(N-j).$$

Since $X_jB(N-j)\in\mathfrak{O}$, it follows from (2.7) (since $B=B^{(0)}$) that the second sum is congruent to zero mod $p^{s+1}B^{(s)}(m)$. This proves $(\beta)_{0,s}$. With s fixed, $s\geq 1$, t fixed, $0\leq t\leq s-1$, we show that $(\beta)_{t,s}$ together with $(\alpha)_s$ imply $(\beta)_{t+1,s}$.

To do this we put $j=\mu+pi$ in the right side of $(\beta)_{t,s}$ and write it in the form

$$\sum_{\mu=0}^{p-1}\sum_{i=0}^{p^{s-t-1}-1} B^{(t)}(\mu+pi+mp^{s-t})H_a(\mu+pi, t, N)/B^{(t)}(\mu+pi),$$

noting that $s-t\geq 1$. By hypothesis *a)*:

$$B^{(t)}(\mu+pi+mp^{s-t})\equiv(B^{(t)}(\mu+pi)B^{(t+1)}(i+mp^{s-t-1})/B^{(t+1)}(i))+X_{i,\mu}p^{s-t}B^{(t+1)}(i+mp^{s-t-1})$$

where $X_{i,\mu}\in\mathfrak{O}$. Thus the general term in our double sum is

$$(B^{(t+1)}(i+mp^{s-t-1})H_a(\mu+pi,\ t,\ N)/B^{(t+1)}(i))+Y_{i,\mu}$$

where the error term,

$$Y_{i,\mu}=X_{i,\mu}p^{s-t}B^{(t+1)}(i+mp^{s-t-1})H_a(\mu+pi,\ t,\ N)/B^{(t)}(\mu+pi).$$

For this error term, since $t<s$, we may apply $(\alpha)_s$ to conclude that

$$Y_{i,\mu}\equiv 0 \mod B^{(t+1)}(i+mp^{s-t-1})p^{s+1}.$$

We now use (2.7) (since $i<p^{s-t-1}$) to conclude that

$$Y_{i,\mu}\equiv 0 \mod p^{s+1}B^{(s)}(m).$$

Thus the right side of $(\beta)_{t,s}$ is modulo $p^{s+1}B^{(s)}(m)$ the same as

$$\sum_{\mu=0}^{p-1}\sum_{i=0}^{p^{s-t-1}-1} B^{(t+1)}(i+mp^{s-t-1})H_a(\mu+pi,\ t,\ N)/B^{(t+1)}(i).$$

By reversing the order of summation and using (2.6), this last sum is the same as

$$\sum_{i=0}^{p^{s-t-1}-1} B^{(t+1)}(i+mp^{s-t-1})H_a(i,\ t+1,\ N)/B^{(t+1)}(i),$$

which proves $(\beta)_{t+1,s}$. In particular then we obtain $(\beta)_{s,s}$, which states

(2.9) $$H_a(m,\ s,\ N+mp^s)\equiv B^{(s)}(m)H_a(0,\ s,\ N)/B^{(s)}(0) \mod p^{s+1}B^{(s)}(m).$$

We now consider the hypothesis (s fixed as before)

$$\gamma_N : H_a(0,\ s,\ N)\equiv 0 \mod p^{s+1}.$$

We know γ_N is true for $N\leq 0$. Let N' (if it exists) be the minimal value of N for which $\gamma_{N'}$ fails. For $m\geq 1$, we then have by equation (2.9), since $B^{(s)}(0)$ is a unit:

$$H_a(m,\ s,\ N')\equiv B^{(s)}(m)H_a(0,\ s,\ N'-mp^s) \mod p^{s+1}$$

and hence $$H_a(m,\ s,\ N')\equiv 0 \mod p^{s+1} \quad \text{for } m>0.$$

Applying this to equation (2.5), we see that

$$H_a(0,\ s,\ N')\equiv 0 \mod p^{s+1}.$$

Thus γ_N is valid for all N, and equation (2.9) now implies $(\alpha)_{s+1}$. This proves equation (2.2) and completes the proof of the theorem.

§ 3. A class of functions with p-adic analytic continuation.

The following theorem is based on Theorem 2 but the notation is changed slightly so that the Ω-valued function $A=B^{(-1)}$ does not appear.

Theorem 3. — *Let* $B^{(0)}, B^{(1)}, \ldots$ *be a sequence of* Ω*-valued functions on* $\mathbf{Z}_+$ *satisfying conditions* a), b), c) *of Theorem* 2 (*for* $i \geq 0$) *and the further conditions*

d′) $\quad B^{(i)}(0) = 1 \quad$ *for* $i \geq 0$.

e) $\quad B^{(i+r)} = B^{(i)} \quad$ *for all* $i \geq 0$ *and some fixed* $r \in \mathbf{Z}_+$.

Let

$$F^{(i)}(X) = \sum_{j=0}^{\infty} B^{(i)}(j) X^j, \qquad i \geq 0$$

$$F_s^{(i)}(X) = \sum_{j=0}^{p^s-1} B^{(i)}(j) X^j, \qquad i \geq 0,\ s \geq 0.$$

Let $\mathfrak{D}$ *be the region in* $\mathfrak{O}$ *defined by the simultaneous conditions*

$$|F_1^{(i)}(x^{p^t})| = 1 \quad \text{for } i = 0, 1, \ldots, r-1,\ t \geq 0 \tag{3.1}$$

(if the functions $B^{(0)}, B^{(1)}, \ldots, B^{(r-1)}$ *take values in a field of finite residue class degree* a*, then* t *may be restricted to* $0 \leq t < a$*).*

Then $F^{(0)}(x)/F^{(1)}(x^p)$*, which is obviously a uniform analytic function on* $\mathfrak{P}$*, is also the restriction to* $\mathfrak{P}$ *of an analytic element* f *of support* $\mathfrak{D}$:

$$f(x) = \lim_{s \to \infty} F_{s+1}^{(0)}(x)/F_s^{(1)}(x^p),$$

which assumes unit values on $\mathfrak{D}$.

Proof. — It follows from Theorem 2 that for $i \geq 0$, $s \geq 0$:

$$F^{(i)}(X) F_s^{(i+1)}(X^p) \equiv F^{(i+1)}(X^p) F_{s+1}^{(i)}(X) \mod p^{s+1}[[X]]. \tag{3.2}$$

Since each $F^{(i)}$, $F_s^{(i)}$ is a unit in $\mathfrak{O}[[X]]$, we conclude that

$$F_{s+1}^{(i)}(X)/F_s^{(i+1)}(X^p) \equiv F^{(i)}(X)/F^{(i+1)}(X^p) \mod p^{s+1}[[X]], \tag{3.2′}$$

a result valid in particular for $s = 0$ and hence

$$F_{s+1}^{(i)}(X)/F_s^{(i+1)}(X^p) \equiv F_1^{(i)}(X) \mod p[[X]] \tag{3.3}$$

from which we deduce

$$F_{s+1}^{(i)}(X) \equiv F_s^{(i+1)}(X^p) F_1^{(i)}(X) \mod p[X] \tag{3.3′}$$

since the congruence certainly holds modulo $p[[X]]$ while both sides are polynomials. It now follows from (3.3′) by induction on s, using the periodicity of the sequence $\{F^{(j)}\}_{j=0,1,\ldots}$ that for $x \in \mathfrak{D}$, $i \geq 0$, $s \geq 0$:

$$|F_s^{(i)}(x)| = 1. \tag{3.4}$$

For $s \geq 1$, equation (3.2′) gives

$$F_{s+1}^{(0)}(X)/F_s^{(1)}(X^p) \equiv F_s^{(0)}(X)/F_{s-1}^{(1)}(X^p) \mod p^s[[X]]$$

and hence by the argument used above:

$$F_{s+1}^{(0)}(X) F_{s-1}^{(1)}(X^p) \equiv F_s^{(0)}(X) F_s^{(1)}(X^p) \mod p^s[X].$$

If we now specialize X to $x \in \mathfrak{O}$ then the congruence holds modulo $p^s\mathfrak{O}$, while if $x \in \mathfrak{D}$ then by (3.4) each factor in the congruence is a unit and hence putting

$$f_s(x) = \mathrm{F}^{(0)}_{s+1}(x)/\mathrm{F}^{(1)}_s(x^p),$$

we have

$$f_s(x) \equiv f_{s-1}(x) \mod p^s\mathfrak{O}$$

for $s \geq 1$, $x \in \mathfrak{D}$. This shows that the sequence $\{f_s\}_{s\geq 0}$ converges uniformly on $\mathfrak{D}$ and equation (3.4) shows that the limit f assumes unit values. On the other hand equation (3.2′) (with $i=0$) can be specialized at $x \in \mathfrak{P}$, showing that

$$f_s(x) \equiv \mathrm{F}^{(0)}(x)/\mathrm{F}^{(1)}(x^p) \mod p^{s+1}\mathfrak{O}.$$

This completes the proof of the theorem.

Corollary. — *Under the hypothesis of the theorem, with* $\mathfrak{D}$ *defined by* (3.1), $\mathrm{F}^{(0)}(x)/\mathrm{F}^{(0)}(x^{p^r})$ (*well defined on* $\mathfrak{P}$) *is the restriction of a uniform analytic function on* $\mathfrak{D}$ *which takes unit values on* $\mathfrak{D}$.

This follows immediately from the theorem since

$$\mathrm{F}^{(0)}(x)/\mathrm{F}^{(0)}(x^{p^r}) = \prod_{j=0}^{r-1} (\mathrm{F}^{(j)}(x^{p^j})/\mathrm{F}^{(j+1)}(x^{p^{j+1}})).$$

In the applications, the function $\mathrm{F}^{(0)}$ will be of classical type (for example generalized hypergeometric functions) while the function $\mathrm{F}^{(0)}(x)/\mathrm{F}^{(0)}(x^{p^r})$ depends formally upon p and does not appear in classical analysis. We now exhibit p-adic analytic continuation of functions which formally do not depend upon p.

Lemma **(3.1).** — *Let* q *be a power of* p, $\mathfrak{D}$ *a quasi-connected domain in* $\mathfrak{O}$ *which is stable under the* q-th *power map and at non-zero distance* d *from its complement. Let* $\mathfrak{N}$ *be a neighborhood of the origin lying in* $\mathfrak{D}$ *and let* F *be an analytic element with support* $\mathfrak{N}$ *which does not vanish at the origin. Suppose* $\mathrm{F}(x)/\mathrm{F}(x^q)$ (*obviously an analytic element with support containing a neighborhood of the origin*) *is the restriction of an analytic element* f *of support* $\mathfrak{D}$, *and that both* f *and* $1/f$ *are uniformly bounded on* $\mathfrak{D}$. *Then for each successive derivative* $\mathrm{F}^{(j)}$ *of* F, *the ratio* $\mathrm{F}^{(j)}/\mathrm{F}$ *is the restriction of an analytic element* η_j *of support* $\mathfrak{D}$. *Furthermore*

$$\mathrm{Sup}\,|\eta_j| \leq (\rho/d)^j, \tag{3.5}$$

where

$$\rho = \mathrm{Sup}\,|f|/\mathrm{Inf}\,|f|,$$

the Sup *and* Inf *being over* $\mathfrak{D}$.

Proof. — A rational function g with no pole in $\mathfrak{D}$ has a Taylor series representation at any $\alpha \in \mathfrak{D}$ which converges in the interior of a disk of radius d about α and hence the Cauchy inequality for power series gives

$$|g'(\alpha)| \leq d^{-1}\,\mathrm{Sup}\,|g|,$$

the supremum being again over $\mathfrak{D}$. Thus

$$\mathrm{Sup}\,|g'| \leq d^{-1}\,\mathrm{Sup}\,|g| \tag{3.6}$$

and by taking limits, this remains valid if g is any analytic element of support $\mathfrak{D}$.

Let δ be the differential operator $X(d/dX)$. For $x\in\mathfrak{N}$, an elementary computation gives (we may assume F has no zeros in $\mathfrak{N}$)

$$(\delta f/f)(x)=(\delta F/F)(x)-q(\delta F/F)(x^q)$$

and hence for $s\geq 1$, $x\in\mathfrak{N}$:

$$x^{-1}\sum_{j=0}^{s-1} q^j(\delta f/f)(x^{q^j})=(F'/F)(x)-x^{-1}q^s(\delta F/F)(x^{q^s}). \tag{3.7}$$

For $x\in\mathfrak{D}$, the sum on the left is bounded by ρ/d, while the general term is bounded by $(\rho/d)|q|^j$. Hence the left side converges uniformly on $\mathfrak{D}$ as $s\to\infty$. On the other hand, we may suppose that F is bounded away from zero on $\mathfrak{N}$ and that F' is bounded on $\mathfrak{N}$ and hence for each $x\in\mathfrak{N}$, the right side of (3.7) converges to $(F'/F)(x)$ as $s\to\infty$. This proves our assertions for η_1.

For $x\in\mathfrak{N}$, it is clear that

$$\eta_{j+1}=\eta_1\eta_j+\eta_j', \tag{3.8}$$

from which the lemma follows by an obvious induction argument, using (3.6), $\rho\geq 1$ and the fact that analyticity is preserved under addition, multiplication and differentiation.

Corollary. — The lemma remains valid if $\mathfrak{N}$ is a neighborhood of any point α which is fixed under the q-th power map and at which F *does not vanish.*

This follows from the fact that we may assume $\mathfrak{N}$ to be a disk of diameter less than unity and hence stable under the q-th power map.

The main significance of the lemma is that (letting $\eta=\eta_1$) the equation

$$\frac{du}{dx}=\eta u, \tag{3.9}$$

specifies for each $\alpha\in\mathfrak{D}$ a one dimensional space U_α of germs of functions holomorphic at α, with the obvious consistency condition that if $u\in U_\alpha$ and α' lies in the support of u then $u\in U_{\alpha'}$. We have assumed in the lemma that $\mathfrak{D}\subset\mathfrak{D}$, but this specification of U_α remains valid for each $\alpha\neq\infty$ in the support of η.

For each $\alpha\in\mathfrak{D}$, let $u_\alpha\in U_\alpha$ be fixed by the condition

$$u_\alpha(\alpha)=1.$$

Let Δ_α be the intersection of $\mathfrak{D}$ with the (open) disk in which u_α converges.

Lemma **(3.2).** — *Under the hypothesis of Lemma* (3.1), *let α be an element of $\mathfrak{D}$ lying in a finite orbit under the q-th power map. We conclude*

(i) *u_α has no zeros in Δ_α.*

(ii) *If* F *satisfies a linear differential equation with coefficients meromorphic on $\mathfrak{D}$, then u_α satisfies the same differential equation.*

(iii) $$u_\alpha(x)/u_{\alpha^q}(x^q)=f(x)/f(\alpha)$$

for each x in Δ_α such that x^q lies in Δ_{α^q}.

Proof. — The first assertion follows from equation (3.9) since η is analytic on $\mathfrak{D}$. For the second assertion we note that the differential equation satisfied by F may by means of (3.8) be transformed into an equivalent non-linear differential equation (independent of F) with coefficients meromorphic on $\mathfrak{D}$ and which is satisfied by $\eta(=F'/F)$. Clearly we may substitute u'_α/u_α for η and recover the original differential equation but now satisfied by u_α. This completes the proof of (ii).

For the proof of (iii) we recall from the proof of Lemma (3.1)

$$xf'/f = x\eta - qx^q\eta(x^q) \tag{3.10}$$

for all $x\in\mathfrak{N}$ and hence everywhere in $\mathfrak{D}$. Since u_α and u_{α^q} are solutions of equation (3.9), we deduce (setting $f_\alpha(x)=u_\alpha(x)/u_{\alpha^q}(x^q)$ for all $x\in\Delta_\alpha$ such that $x^q\in\Delta_{\alpha^q}$) that

$$f'_\alpha/f_\alpha = f'/f$$

and hence there exists a constant c such that

$$f_\alpha = cf$$

on a sufficiently small neighborhood of α. Clearly $f_\alpha(\alpha)=1$, and this permits the evaluation of c, which completes the proof of the lemma.

We now propose to free the theory from the " choice of zero point " which appears since the q-th power map plays so prominent a role. We may view this map on $\mathfrak{O}$ as a lifting to characteristic zero of the Frobenius map over GF[q]. Of course other liftings exist ([18]). Let φ be a power series converging everywhere in $\mathfrak{O}$ such that for all $x\in\mathfrak{O}$:

$$\varphi(x)\equiv x^q \mod \pi\mathfrak{O} \tag{3.11}$$

where π is a fixed element of $\mathfrak{P}$.

Lemma **(3.3).** — *To the hypothesis of Lemma* (3.1) *we add the additional hypothesis that* $\mathfrak{N}$ *is a neighborhood of zero which is stable under* φ, *that* F *is bounded away from zero on* $\mathfrak{N}$, *and that*

$$1 > e = (\rho/d)\,|\,\pi\,|\,p^{1/(p-1)},$$

the quantity e being defined by this relation. We conclude that the function

$$f_\varphi(x) = F(X)/F(\varphi(x))$$

defined on $\mathfrak{N}$ *is the restriction of an analytic element of support* $\mathfrak{D}$.

(*Note.* — In the examples provided by the Corollary of Theorem 3, $\rho=d=1$.)

Proof. — For $x\in\mathfrak{D}$, let $T=x^q$, $T+t=\varphi(x)$. For $x\in\mathfrak{N}$, we have

$$f_\varphi(x) = f(x).(F(T)/F(T+t)).$$

Clearly it is enough to consider the second factor. The Taylor expansion of F in $\mathfrak{N}$ gives

$$F(T+t)/F(T) = \sum_{j=0}^{\infty} \eta_j(T)t^j/j! \tag{3.12}$$

The first term on the right side is 1 and with the aid of (3.5) we check that for $x\in\mathfrak{D}, j\geq 1$

$$|\eta_j(T)t^j/j!|\leq e^j.$$

Since $e<1$ this shows that the series converges uniformly on $\mathfrak{D}$ and assumes unit values there. This completes the proof of the lemma.

We summarize most of our results in a form particularly adaptable to our application in the next section. Here $F^{(j)}$ denotes the j-th derivative of F.

Lemma **(3.4)**. — *Let* B *be a mapping of* $\mathbf{Z}_+$ *into* $\mathbf{Q}_p$ *such that*

a) $B(0)=1$.

b) $B(n+mp^{s+1})/B([n/p]+mp^s)\equiv B(n)/B([n/p]) \bmod p^{s+1}$ *for all* n, m, s *in* $\mathbf{Z}_+$.

c) $B(n)/B([n/p])\in\mathfrak{O}$ *for all* $n\in\mathbf{Z}_+$.

Let

$$F(X) = \sum_{m=0}^{\infty} B(m)X^m$$

$$F_s(X)=\sum_{m=0}^{p^s-1} B(m)X^m, \quad s\geq 0$$

$$\mathfrak{D}=\{x\in\mathfrak{O} \mid |F_1(x)|=1\}.$$

Then

(i) *There exists* f *analytic with support* $\mathfrak{D}$ *coinciding with* $F(x)/F(x^p)$ *on* $\mathfrak{P}$, *assuming unit values on* $\mathfrak{D}$ *and such that uniformly on* $\mathfrak{D}$

$$f(x)\equiv F_{s+1}(x)/F_s(x^p) \bmod p^{s+1}. \tag{3.13}$$

(ii) *For each* $j\in\mathbf{Z}_+$, *there exists* η_j *analytic with support* $\mathfrak{D}$, *coinciding with* $F^{(j)}/F$ *on* $\mathfrak{P}$, *mapping* $\mathfrak{D}$ *onto* $\mathfrak{O}$ *and such that uniformly on* $\mathfrak{D}$;

$$\eta_j\equiv F^{(j)}_{s+1}/F_{s+1} \bmod p^{s+1}. \tag{3.14}$$

(iii) *There exists a function* g *defined on*

$$\mathfrak{E}=\{(x,y)\in\mathfrak{O}\times\mathfrak{O} \mid x+y\in\mathfrak{D}\}$$

such that for $(x,y)\in\mathfrak{P}\times\mathfrak{P}$:

$$g(x,y)=F(x+y)/F(x^p+y^p)$$

and such that uniformly on $\mathfrak{E}$:

$$g(x,y)\equiv F_{s+1}(x+y)/F_s(x^p+y^p) \bmod p^{s+1}. \tag{3.15}$$

(iv) *For each* $\alpha\in\mathfrak{D}$, *the solution* u_α *of equation* (3.9) (*with initial condition* $u_\alpha(\alpha)=1$), *converges in* $\alpha+\mathfrak{P}$ *and for all* $(\alpha, t)\in\mathfrak{D}\times\mathfrak{P}$:

$$f(\alpha)u_\alpha(\alpha+t)/u_{\alpha^p}(\alpha^p+t^p)\equiv F_{s+1}(\alpha+t)/F_s(\alpha^p+t^p) \bmod p^{s+1}. \tag{3.16}$$

Proof. — Statement (i) is a direct consequence of Theorem 3. For statement (ii) we first note that by Lemma (3.1) we need only check equation (3.14). To facilitate computations, let us, for each function g defined on a subset S of Ω, write Φg for the

composed function, $x\mapsto g(x^{\varphi})$, defined on the inverse image of S under the p-th power map. Once again let δ be the differential operator $x\frac{d}{dx}$. From equation (3.13), we obtain

$$\frac{1}{x}(p\Phi)^j\frac{\delta f}{f}\equiv\frac{1}{x}(p\Phi)^j\left(\frac{\delta F_{s+1-j}}{F_{s+1-j}}-p\Phi\frac{\delta F_{s-j}}{F_{s-j}}\right)\bmod p^{s+1} \tag{3.13)'}$$

(uniformly on $\mathfrak{D}$), while equation (3.7) may be written

$$\eta_1=x^{-1}\sum_{j=0}^{\infty}(p\Phi)^j(\delta f/f). \tag{3.7)'}$$

By replacing each term in the right hand sum by the right hand side of (3.13)', we obtain equation (3.14) with $j=1$. The proof of equation (3.14) for arbitrary j is now obtained by induction with the aid of equation (3.8). This completes the proof of (ii).

For statement (iii) we use the method of Lemma (3.3). For $(x,y)\in\mathfrak{E}$, both $x+y$ and x^p+y^p lie in $\mathfrak{D}$ and hence putting $\xi=x^p+y^p$, $p\mathrm{T}=(x+y)^p-\xi$, we have

$$F_{s+1}(x+y)/F_s(x^p+y^p)=(F_{s+1}(x+y)/F_s((x+y)^p))(F_s(\xi+p\mathrm{T})/F_s(\xi)).$$

Equation (3.13) shows that the first factor on the right is congruent to $f(x+y)$ modulo p^{s+1} while the second factor is

$$1+\sum_{j=1}^{\infty}(F_s^{(j)}/F_s)(\xi)(p\mathrm{T})^j/j!$$

and by equation (3.14) (since $j-\mathrm{ord}\,j!\geq 1$ for $j\geq 1$) this is congruent mod p^{s+1} to

$$1+\sum_{j=1}\eta_j(\xi)(p\mathrm{T})^j/j!.$$

We define $g(x,y)$ to be the product of this last expression with $f(x+y)$ and check trivially that for $(x,y)\in\mathfrak{P}\times\mathfrak{P}$, $g(x,y)=F(x+y)/F(\xi)$.

To prove (iv) we first observe that since $\eta(=\eta_1)$ is a limit of rational functions with coefficients in $\mathbf{Q}_p$, η and each of its derivatives assumes at $\alpha\in\mathfrak{D}$ values in K_α, the closure of $\mathbf{Q}_p(\alpha)$ in Ω. It follows that u_α may be represented by a power series in $K_\alpha[[x-\alpha]]$ and hence the disk of convergence Δ_α of u_α has the same radius as $\Delta_{\alpha'}$ for each conjugate (over $\mathbf{Q}_p$) α' of α. In particular if $q=p^a$, $\alpha^q=\alpha$, then Δ_{α^p} is the image of Δ_α under an extension to Ω of the absolute Frobenius. Thus part (iii) of Lemma (3.2) takes the form

$$u_\alpha(x)/u_{\alpha^p}(x^p)=f(x)/f(\alpha) \tag{3.17}$$

for all $x\in\Delta_\alpha$ and hence

$$u_\alpha(x)/u_\alpha(x^q)=\prod_{j=0}^{a-1}(f(x^{p^j})/f(\alpha^{p^j}). \tag{3.17'}$$

Since the right hand side is analytic in $\alpha+\mathfrak{P}$ and u_α has non-zero radius of convergence, it follows from the radius reducing property of the q-th power map (when applied to

disks of radius strictly less than unity and center at α) that u_α must converge in $\alpha+\mathfrak{P}$. Since u_α and u_β (for $\beta\in\alpha+\mathfrak{P}$) differ only by a non-zero constant factor, it follows that u_β converges in $\beta+\mathfrak{P}$ for each $\beta\in\mathfrak{D}$.

In particular this shows that equation (3.17) remains valid for all $\alpha\in\mathfrak{D}$, $x\in\alpha+\mathfrak{P}$ (with hypothesis that $\alpha^q=\alpha$). To verify equation (3.16), we once again use the method of Lemma (3.3), put $\xi=\alpha^p+t^p$, $p\mathrm{T}=(\alpha+t)^p-\xi$ and write

(3.18) $$f(\alpha)u_\alpha(\alpha+t)/u_{\alpha^p}(\xi)=(f(\alpha)u_\alpha(\alpha+t)/u_{\alpha^p}((\alpha+t)^p))(u_{\alpha^p}(\xi+p\mathrm{T})/u_{\alpha^p}(\xi)).$$

It follows from equation (3.17) that the first factor on the right side is $f(\alpha+t)$ (for $t\in\mathfrak{P}$) while the second factor is precisely as in the proof of (iii):

$$1+\sum_{j=1}^{\infty}(u_{\alpha^p}^{(j)}/u_{\alpha^p})(\xi)(p\mathrm{T})^j/j!.$$

Since u_{α^p} is a solution of equation (3.9), it is clear that $u_{\alpha^p}^{(j)}/u_{\alpha^p}$ is the restriction of η_j to $\alpha+\mathfrak{P}$ and hence by equation (3.14), the above series is congruent mod p^{s+1} (for all $t\in\mathfrak{P}$) to

$$1+\sum_{j=1}^{\infty}(\mathrm{F}_s^{(j)}/\mathrm{F}_s)(\xi)(p\mathrm{T})^j/j!,$$

which is clearly the same as $\mathrm{F}_s(\xi+p\mathrm{T})/\mathrm{F}_s(\xi)$. The first factor on the right side of (3.18) being $f(\alpha+t)$, we see by equation (3.13) that it is congruent mod p^{s+1} to $\mathrm{F}_{s+1}(\alpha+t)/\mathrm{F}_s((\alpha+t)^p)$. The proof of equation (3.16) now follows from the definition of ξ and T.

§ 4. Cycles of elliptic curves.

It is well known that the classical periods of the differential, $\omega=d\mathrm{X}/2\mathrm{Y}$, of the first kind of the elliptic curve

(4.1) $$\mathrm{Y}^2=\mathrm{X}(\mathrm{X}-1)(\mathrm{X}-\lambda)$$

satisfy the hypergeometric differential equation

(4.2) $$\lambda(1-\lambda)u''+(1-2\lambda)u'-(1/4)u=0.$$

Igusa (*Proc. Nat. Acad. Sci. U.S.A.*, vol. 44 (1958), 312-314), noted that modulo p the only power series solutions of (4.2) are

(4.3) $$g(\lambda)=\sum_{j=0}^{(p-1)/2}\left(\left(\frac{1}{2}\right)_j/j!\right)^2\lambda^j$$

and the products of g with power series in λ^p. In lectures at the Johns Hopkins University in 1958 he gave the heuristic interpretation that in characteristic p, ω has just one period on the fiber (except in the supersingular case, when $g(\lambda)$ vanishes and then there is no period).

We adopt a similar point of view in the p-adic case and think of the cycles of the

fiber $\lambda=\lambda_0$ as being given by the locally holomorphic solutions (in the parameter space) of (4.2). Since $\partial\omega/\partial\lambda$ is a differential of the second kind, this definition of cycle gives a " period " for all differentials of the second kind.

It is natural to introduce the notion of cycle classes, that is of one dimensional subspaces of the two dimensional space of locally holomorphic solutions of (4.2).

Let
$$\mathfrak{D}_1=\{\lambda\in\mathfrak{D}\mid |g(\lambda)|=1\}$$
$$\mathfrak{D}_2=\{\lambda\mid \lambda^{-1}\in\mathfrak{D}_1\}$$
$$\mathfrak{D}=\mathfrak{D}_1\cup\mathfrak{D}_2.$$

By means of equation (3.9) we shall give a " global " definition of a distinguished cycle class. We will show that this class is characterized (locally) by being *bounded* in each disk of convergence. This cycle class appears implicitly in the theorem of Tate stated in ([2], § 5). We give a second proof of this local characterization in terms of boundedness by showing that for each $\alpha\in\mathfrak{D}$, the ratio w of solutions of (4.2) may be chosen so that

$$\exp(w)\in\mathfrak{D}[[t]],$$

where $t=\lambda-\alpha$ for $\alpha\in\mathfrak{D}_1$, $t=1/\lambda$ for $|\alpha|>1$. This result generalizes the observation of Tate that for $|j|>1$, $|q|<1$ ($j=$invariant of (4.1), $q=e^{i\pi\tau}$, as in the Jacobi theory of elliptic functions), the classical relations between j and q may be interpreted p-adically. We do not know if Tate's theory of p-adic theta functions ([13], § 1) may be generalized.

Having concluded these introductory remarks we proceed with our exposition. We know

$$F(\lambda)=F\left(\frac{1}{2},\frac{1}{2},1,\lambda\right)=\sum_{j=0}^{\infty}\left(\left(\frac{1}{2}\right)_j/j!\right)^2\lambda^j$$

is the unique solution of (4.2) holomorphic at the origin. It follows from § 1 that F satisfies the hypothesis of Lemma (3.4), while the coefficient of λ^j for $(p-1)/2<j<p$ is congruent to zero modulo p and hence

$$F_1\equiv g \mod p[\lambda].$$

Thus $\eta=F'/F$ and $f(\lambda)=F(\lambda)/F(\lambda^p)$ can be extended to analytic elements of support $\mathfrak{D}_1$. Equation (3.2) (with $s=0$) now takes the form

$$F(\lambda)\equiv F(\lambda^p)g(\lambda) \mod p[[\lambda]]$$

and hence as noted before g satisfies equation (4.2) modulo p. It is well known that g is the unique polynomial (mod p) of degree strictly less than p which satisfies (4.2) mod p. Since the differential equation is stable under $\lambda\mapsto 1-\lambda$, it follows that

$$g(1-\lambda)\equiv(-1)^{(p-1)/2}g(\lambda) \mod p \tag{4.4}$$

and similarly

$$g(\lambda) \equiv \lambda^{(p-1)/2} g(1/\lambda) \mod p \tag{4.5}$$

follows from the fact that if u is a solution of (4.2) then so is $\lambda^{-\frac{1}{2}} u(1/\lambda)$.

Thus $\mathfrak{D}_1 = 1 - \mathfrak{D}_1$, and $\mathfrak{D}_1$ has the same intersection with the group of units as $\mathfrak{D}_2$. This shows that $\eta(\lambda)$ and $\eta(1-\lambda)$ are both defined on $\mathfrak{D}_1$. For $\lambda \in \mathfrak{D}_2$, let

$$-\xi(\lambda) = (2\lambda)^{-1} + \lambda^{-2}\eta(\lambda^{-1}), \tag{4.6}$$

so that ξ is an analytic element of support $\mathfrak{D}_2$.

We claim that

$$\eta(\lambda) + \eta(1-\lambda) = 0 \quad \text{for } \lambda \in \mathfrak{D}_1 \tag{4.7}$$

$$\eta = \xi \quad \text{on } \mathfrak{D}_1 \cap \mathfrak{D}_2. \tag{4.8}$$

To prove these relations, for each $\alpha \in \mathfrak{D}_1$, let U_α be the space of functions holomorphic at α defined by equation (3.9). By part (ii) of Lemma (3.2), U_α is a subspace of V_α, the germs of holomorphic solutions at α of equation (4.2). For $\alpha = 0, 1$ the dimension of V_α is unity and hence $U_\alpha = V_\alpha$ for $\alpha = 0, 1$. In particular, U_1 is spanned by $F(1-\lambda)$ and hence equation (3.9) shows that for λ near 1,

$$F(1-\lambda)\eta = -F'(1-\lambda).$$

This proves equation (4.7) for λ close to 1 and hence by uniqueness, for all $\lambda \in \mathfrak{D}_1$.

To prove (4.8) we consider the classical solution $\lambda^{-\frac{1}{2}} F(1/\lambda)$ near infinity of (4.2). This is clearly a solution of

$$\frac{du}{d\lambda} = \xi u, \tag{4.9}$$

an equation which is non-singular at each finite point of $\mathfrak{D}_2$. Precisely as in the proof of part (ii) of Lemma (3.2), this equation defines for each finite α in $\mathfrak{D}_2$ a one-dimensional subspace U'_α of V_α. Again for $\alpha = 1$ we have $U'_\alpha = V_\alpha$ and thus for λ close to 1, $F(1-\lambda)$ is a solution of equation (4.9) which shows that

$$\xi(\lambda) = -\eta(1-\lambda)$$

in a neighborhood of 1. Equation (4.8) now follows with the aid of equation (4.7).

Thus η may be extended to a uniform analytic function of support $\mathfrak{D}$ and we have shown

$$\eta(1-\lambda) = -\eta(\lambda) \tag{4.7}'$$

$$\lambda^{-1}\eta(\lambda^{-1}) + (1/4) = -(\lambda\eta(\lambda) + 1/4) \tag{4.8}'$$

and finally we observe that equation (3.9) now defines a one-dimensional subspace U_α of V_α for each finite α in $\mathfrak{D}$. This is the distinguished cycle class mentioned in our introductory remarks. Classically it is the vanishing cycle at $\lambda = 0$, but in the p-adic

theory (contrary to the classical case) it may be identified with the vanishing cycles at $\lambda=1$ and $\lambda=\infty$.

Before proving the boundedness characterization of U_α we need a preliminary result.

Lemma **(4.1).** — *For each integer* $r\geq 1$, *let* $N_r=(p^r-1)/(p-1)$ *and let*

$$G_r(\lambda)=1/(\lambda(1-\lambda)g^{2N_r}),$$

where g *is the polynomial defined by equation* (4.3).

We assert the existence of a rational function R_r *having poles precisely at the zeros of* g *such that uniformly on* $\mathfrak{D}_1$,

$$G_r(\lambda)\equiv(\lambda(1-\lambda))^{-1}+\frac{dR_r}{d\lambda} \mod p \tag{4.10}$$

$$|p^{r-1}R_r|\leq 1. \tag{4.11}$$

Proof. — We recall that each zero β of g must be a simple zero modulo p as otherwise (since $\beta\not\equiv 0, 1$) equation (4.2) would show that all derivatives of g vanish modulo p at β and since the degree of g is strictly less than p, this would imply the triviality mod p of g.

We now consider $r=1$. We assert that

$$G_1(\lambda)=(\lambda(1-\lambda))^{-1}+\sum_\beta B(\beta)/(\lambda-\beta)^2 \mod p, \tag{4.12}$$

the sum being over all roots of g and each $B(\beta)$ is a unit. Clearly G_1 has simple poles at $\lambda=0, 1$ and by (4.4), the principal parts are $(\lambda(1-\lambda))^{-1}$. Thus we need only consider the principal part at β. Putting $z=\lambda-\beta$, we have

$$g(\lambda)/(zg'(\beta))\equiv 1+z(g''/2g')(\beta) \mod z^2$$

and hence, from the definition of G_1 we obtain

$$z^{-2}(\beta(1-\beta)(g'(\beta))^2G_1)^{-1}\equiv(1+(z/\beta))(1-(z/(1-\beta)))(1+z(g''/g')(\beta)) \mod z^2.$$

With the aid of equation (4.2) we readily see that the right side is congruent to 1 mod(p, z^2). This proves equation (4.12) and for $r=1$, equations (4.10), (4.11) follow trivially.

We now use induction on r and suppose these equations valid for a fixed value of $r\geq 1$. We note that

$$\frac{d}{d\lambda}(R_r/g^{2p^r})-g^{-2p^r}\frac{dR_r}{d\lambda}=-2p^rR_rg'/g^{2p^r+1},$$

and by (4.11) the right side is congruent to zero mod p. Since $G_{r+1}=G_r/g^{2p^r}$, we now conclude from (4.10) that

$$G_{r+1}-(\lambda(1-\lambda)g^{2p^r})^{-1}\equiv\frac{d}{d\lambda}(R_r/g^{2p^r}) \mod p. \tag{4.13}$$

We write

$$(\lambda(1-\lambda)g^{2p^r})^{-1}=(\lambda(1-\lambda))^{p^r-1}G_1^{p^r}$$

and by equation (4.12) the right side is the same mod p as

$$(\lambda(1-\lambda))^{-1}+\sum_{\beta} B(\beta)^{p^r}(\lambda(1-\lambda))^{p^r-1}/(\lambda-\beta)^{2p^r}.$$

Since $2(p^r-1)<2p^r+1$, it is clear that

$$(\lambda(1-\lambda))^{p^r-1}/(\lambda-\beta)^{2p^r}=\sum_{j=2}^{2p^r} C_j/(\lambda-\beta)^j=-\frac{d}{d\lambda}\sum_{j=2}^{2p^r}(C_j/(j-1))/(\lambda-\beta)^{j-1}$$

where each C_j is a polynomial in β with integral coefficients. Thus

$$|p^r C_j/(j-1)|\leq 1,$$

since $j-1<2p^r$ and hence cannot be divisible by p^{r+1}. The lemma now follows from (4.13) with the aid of (4.11).

Lemma **(4.2).** — U_α *is the space of all germs of holomorphic solutions at* α *of equation* (4.2) *which are bounded in their disk of convergence.*

Proof. — For $\alpha\neq 0$, $\lambda^{-\frac{1}{2}}u_\alpha(1/\lambda)$ lies in $U_{1/\alpha}$. Thus we may restrict our attention to $\alpha\in\mathfrak{D}_1$.

We note that if u_α were not bounded in Δ_α (cf. Lemma (3.2)) then the Newton polygon of u_α (as power series in $\lambda-\alpha$) shows that u_α must have one (and in fact infinitely many) zero(s) in the disk, contradicting part (i) of Lemma (3.2).

If $\alpha=0, 1$ then uniqueness is clear as there is no other single valued solution of (4.2). If $\alpha\in\mathfrak{P}$, $\alpha\neq 0$ then an explicit solution (independent of $u_\alpha=F$) is of the form $(t=\lambda-\alpha)$

(4.14)
$$G+F\log(1-\lambda)-F\log(1+(t/\alpha)),$$
$$G=2\sum_{j=1}^{\infty}\left(\left(\frac{1}{2}\right)_j/j!\right)^2\left(\sum_{r=1}^{j}\frac{1}{r}\right)\lambda^j.$$

The first two terms converge in $\mathfrak{P}$ while the third term converges in the strictly smaller disk $|t|<|\alpha|<1$, and is unbounded in that disk. By the transformation $\lambda\mapsto 1-\lambda$, a similar result holds for $\alpha-1\in\mathfrak{P}$.

We may now assume that neither α nor $1-\alpha$ lie in $\mathfrak{P}$. By Lemma (3.4) (iv), u_α converges in $\alpha+\mathfrak{P}$ and hence we may assume that $\alpha^q=\alpha$ for some $q=p^a$. We assert that u_α cannot converge in the " closed " disk of radius one about α (i.e. in $\mathfrak{O}$) since otherwise equation (3.17)′ would be valid in a neighborhood of zero, while in such a neighborhood, we may represent the right side by $F(\lambda)/F(\lambda^q)$ (since putting $\lambda=0$, the constant factor must be unity). Thus

$$(u_\alpha/F)(\lambda)=(u_\alpha/F)(\lambda^q)$$

in a neighborhood of zero, from which we deduce $u_\alpha=F$, and hence F converges in the closed unit disk, clearly a contradiction. Thus $\Delta_\alpha=\alpha+\mathfrak{P}$. We now show that there exists a solution of (4.2) holomorphic at α which converges in Δ_α and is inde-

pendent of u_α. For this, using a standard procedure, let $w \in \mathbf{Q}_p(\alpha)[[\lambda-\alpha]]$ be chosen such that

$$w' = (\lambda(1-\lambda)u_\alpha^2)^{-1}.$$

Since the right side converges in $\alpha+\mathfrak{P}$, and this is not effected by term by term integration, the same holds for w. Since u_α, wu_α span the space of locally holomorphic solutions of (4.2), we conclude that all such solutions converge in $\alpha+\mathfrak{P}$.

Equation (3.13) shows that for $\lambda \in \mathfrak{D}_1$,

$$f(\lambda) \equiv g(\lambda) \mod p.$$

For each integer r, put $\alpha^{p^r} = \alpha_r$ and let N_r be as in the previous lemma. It follows from (3.17) that

$$u_\alpha(\lambda)/u_{\alpha_r}(\lambda^{p^r}) \equiv c_r g(\lambda)^{N_r} \mod p, \tag{4.15}$$

the constant c_r being a unit in $\mathbf{Q}_p(\alpha)$.

Suppose that v_α is a solution of (4.2) which is independent of u_α and bounded in Δ_α. Then every solution of (4.2), holomorphic at α, is bounded in Δ_α. Since a basis lies in $\mathbf{Q}_p(\alpha)[[\lambda-\alpha]]$, we may suppose that v_α lies in this ring. Since $u_\alpha(\alpha)=1$, we may assume that $v_\alpha(\alpha)=0$. Thus if we put $w = v_\alpha/u_\alpha$, a standard computation using (4.2) gives

$$w'(\lambda)\lambda(1-\lambda)u_\alpha^2 = cc_r^2, \tag{4.16}$$

where c is a non-zero constant and c_r is defined by equation (4.15). Note that c depends upon r, but that its ordinal is independent of r. We may assume (since v_α is bounded in $\alpha+\mathfrak{P}$) that v_α (and hence w) is normalized so that

$$|v_\alpha| = |w| = 1,$$

the norm being the sup norm of $\alpha+\mathfrak{P}$. Clearly $c \in \mathbf{Q}_p(\alpha)$, an unramified field, while

$$|c| = |w'| \leq |w| = 1$$

and hence there exists $r \geq 1$ such that c/p^{r-1} is a unit. Thus multiplying w by a unit, we may suppose that in equation (4.16) $c = p^{r-1}$. We now write this equation in the form

$$w'(\lambda)(u_{\alpha_r}(\lambda^{p^r}))^2 = p^{r-1}c_r^2(\lambda(1-\lambda)(u_\alpha(\lambda)/u_{\alpha_r}(\lambda^{p^r}))^2)^{-1} \tag{4.16}'$$

and deduce from equation (4.15) that in the sup norm of $\alpha+\mathfrak{P}$, the right side is congruent mod p^r to $p^{r-1}G_r$. Now put

$$W(\lambda) = w(\lambda)(u_{\alpha_r}(\lambda^{p^r}))^2$$

then $|W| = 1$ and clearly the left side of (4.16)′ is congruent to $W' \bmod p^r$. With $t = \lambda - \alpha$, equation (4.10) now gives

$$\frac{d}{dt}(W - p^{r-1}R_r) \equiv p^{r-1}(\lambda(1-\lambda))^{-1} \mod p^r. \tag{4.17}$$

Since equation (4.11) holds in the sup norm of $\mathfrak{D}_1$, it certainly holds in the norm of $\alpha+\mathfrak{P}$. Thus we may write

$$W-p^{r-1}R_r=\sum_{j=0}^{\infty} a_j t^j,$$

where each $a_j\in\mathfrak{O}$. Comparing powers of t^{j-1} in equation (4.17),

$$ja_j\equiv p^{r-1}(-1)^j((\alpha-1)^{-j}-\alpha^{-j}) \mod p^r. \tag{4.18}$$

Clearly for $j=p^\nu$, $\nu\geq r$, the left side is congruent to zero modulo p^r, while the right side is the product of p^{r-1} with a unit. This contradiction shows the non-existence of any solution of (4.2) independent of u_α which is holomorphic at α and bounded in $\alpha+\mathfrak{P}$. This completes the proof of the lemma.

Before considering our strongest result in the direction of information about solutions of (4.2) which are independent of u_α, let us consider the classical solutions at $\lambda=0$. We consider the two solutions, $F(\lambda)(=u_0(\lambda))$ and

$$v_0(\lambda)=F\log\lambda-F\log(1-\lambda)-G, \tag{4.19}$$

where G is defined by equation (4.14). If we put $w_0=v_0/u_0$, then precisely as in the proof of the previous lemma,

$$w_0'\lambda(1-\lambda)F^2=c,$$

where the constant c will now be determined. We put

$$W=-w_0+\log\lambda=\log(1-\lambda)+G/F. \tag{4.20}$$

Then W has no singularity at the origin and since

$$W'=\lambda^{-1}\left(1-\frac{c}{(1-\lambda)F^2}\right),$$

it is clear that $c=1$.

Precisely as in the Tate theory of p-adic theta functions, we appeal to classical formulae ([14], pp. 85, 171)

$$16q=\lambda(1-\lambda)^{-1}e^{-G/F} \tag{4.21}$$

$$\lambda=16q\Big(\prod_{\nu=1}^{\infty}(1+q^{2\nu})/(1+q^{2\nu-1})\Big)^8. \tag{4.22}$$

We conclude that if we choose $W\in\mathbf{Q}[[\lambda]]$ such that

$$\begin{cases} W(0)=0 \\ W'(\lambda)=\dfrac{1}{\lambda}\left(1-\left(\dfrac{1}{(1-\lambda)F^2}\right)\right) \end{cases} \tag{4.23}$$

then

$$\exp W \in \mathfrak{O}[[\lambda]], \tag{4.24}$$

the coefficients being p-integral rational numbers for all $p \neq 2$.

Let K_T be the maximal unramified extension of $\mathbf{Q}_p$ in Ω, and let τ be the absolute Frobenius mapping of K_T over $\mathbf{Q}_p$. For each $\alpha \in \mathfrak{D}_1$ which lies in a finite orbit under τ, we choose a unit $F_0(\alpha)$ in K_T such that

$$F_0(\alpha)^{1-\tau} = f(\alpha). \tag{4.25}$$

Theorem 4. — *For each* $\alpha \in \mathfrak{D}_1$ $(\alpha \neq 0, 1, \infty)$, *which is fixed under an iterate of the* p-th *power map, we fix a solution* v_α, *holomorphic at* α *and independent of* u_α, *by the conditions*

$$\begin{aligned} &v_\alpha(\alpha) = 0, \qquad w_\alpha = v_\alpha / u_\alpha \\ &w'_\alpha . \lambda(1-\lambda) F_0(\alpha)^2 u_\alpha^2 = 1 \\ &u_\alpha \in U_\alpha, \qquad u_\alpha(\alpha) = 1. \end{aligned} \tag{4.26}$$

Then $\exp w_\alpha$ *lies in* $\mathfrak{O}_T[[\lambda - \alpha]]$, $\mathfrak{O}_T$ *being the ring of integers of* K_T.

Proof. — Let m, s be integers, $m \geq 1$, $s \geq 0$, $N = mp^{s+1} - 1$. We choose an integer r such that $p^r > N$. Let t be an indeterminate and let

$$H(\lambda, t) = \frac{1}{(\lambda + t)(1 - \lambda - t)(F_{s+r}(\lambda + t))^2} - \frac{t^{p-1}}{(\lambda^p + t^p)(1 - \lambda^p - t^p)(F_{s+r-1}(\lambda^p + t^p))^2}$$

$$M(\lambda) = \lambda(1 - \lambda^p) F_{s+r}(\lambda) F_{s+r-1}(\lambda^p).$$

For fixed λ not a zero of M, H is a rational function of t which is holomorphic for t near zero. Thus $H(\lambda, t)$ may be represented as a power series in t whose coefficients are rational functions of λ with poles at the zeros of M. We assert that the coefficient $h(\lambda)$ of t^N has no pole at $\lambda = 0$ and that

$$|h(\lambda)| \leq |p^{s+1}| \tag{4.27}$$

for all $\lambda \in \mathfrak{D}_1$, $\lambda \notin 1 + \mathfrak{P}$.

This, the central point of the proof, is based upon equation (4.24), which shows that

$$\exp W(\lambda + t) \in (\mathbf{Q}_p \cap \mathfrak{O})[[\lambda, t]]$$

and hence putting $\xi_j = \lambda^{p^j} + t^{p^j}$ for each $j \geq 0$,

$$pW(\xi_0) \equiv W(\xi_1) \mod p[[\lambda, t]]$$

(by [1], Lemma 1). Thus if $L_\nu(\lambda) \in \mathbf{Q}_p[[\lambda]]$ is the coefficient of t^ν in $W'(\lambda + t)$ then

$$L_{mp^{s+1}-1}(\lambda) - L_{mp^s-1}(\lambda^p) \equiv 0 \mod p^{s+1}[[\lambda]] \tag{4.28}$$

and hence the left side, viewed as a function on $\mathfrak{P}$, is bounded uniformly by $|p^{s+1}|$. We note that the left side of (4.28) is the coefficient of t^N in

$$W'(\xi_0) - W'(\xi_1) t^{p-1}$$

and since $F(\xi_r)/F(\lambda^{p^r}) \equiv 1 \bmod t^{p^r}$, the bound of the coefficient of t^N is not changed if we multiply this difference by $(F(\xi_r)/F(\lambda^{p^r}))^2$. We easily compute by means of (4.23) that

$$-W'(\xi_0)(F(\xi_r)/F(\lambda^{p^r}))^2 = A_0 + B_0$$

where

$$A_0 = \left(\frac{F_s(\xi_r)}{F(\lambda^{p^r})}\right)^2 \frac{1}{\xi_0}\left(\frac{1}{1-\xi_0}\frac{1}{(F_{s+r}(\xi_0))^2} - \left(\frac{F(\xi_r)}{F_s(\xi_r)}\right)^2\right)$$

$$B_0 = \frac{1}{F(\lambda^{p^r})^2}\frac{1}{(1-\xi_0)\xi_0}\left(\left(\frac{F(\xi_r)}{F(\xi_0)}\right)^2 - \left(\frac{F_s(\xi_r)}{F_{s+r}(\xi_0)}\right)^2\right).$$

It is to be understood that $\lambda, t \in \mathfrak{P}$, $|\lambda| > |t| \geq 0$, so that for each fixed λ both A_0 and B_0 may be represented by power series in t. The last factor in the formula for B_0 is a power series in λ, t which by equation (3.15) is uniformly bounded by $|p^{s+1}|$. Since $(1-\xi_0)$ and $F(\lambda^{p^r})$ are units, we see that by writing

$$\frac{1}{\xi_0} = \lambda^{-1}\sum_{j=0}^{\infty}(-t/\lambda)^j,$$

the coefficient of t^N in B_0 is bounded by $|p^{s+1}/\lambda^{N+1}|$. Likewise,

$$-W'(\xi_1)(F(\xi_r)/F(\lambda^{p^r}))^2 = A_1 + B_1,$$

$$A_1 = \left(\frac{F_s(\xi_r)}{F(\lambda^{p^r})}\right)^2 \frac{1}{\xi_1}\left(\frac{1}{(1-\xi_1)(F_{s+r-1}(\xi_1))^2} - \left(\frac{F(\xi_r)}{F_s(\xi_r)}\right)^2\right)$$

$$B_1 = \frac{1}{(1-\xi_1)F(\lambda^{p^r})^2}\frac{1}{\xi_1}\left(\left(\frac{F(\xi_r)}{F(\xi_1)}\right)^2 - \left(\frac{F_s(\xi_r)}{F_{s+r-1}(\xi_1)}\right)^2\right)$$

and by precisely the same argument as for B_0, we conclude that the coefficient of t^N in $t^{p-1}B_1$ is also bounded by $|p^{s+1}|/|\lambda^{N+1}|$. Thus the coefficient of t^N in $A_0 - A_1 t^{p-1}$ has this bound. By an elementary computation

(4.29) $$A_0 - A_1 t^{p-1} = (F_s(\xi_r)/F(\lambda^{p^r}))^2 C(\lambda, t) + E,$$

where

$$C = \frac{1}{\xi_0}\left(\frac{1}{(1-\xi_0)(F_{s+r}(\xi_0))^2} - 1\right) - t^{p-1}\frac{1}{\xi_1}\left(\frac{1}{(1-\xi_1)(F_{s+r-1}(\xi_1))^2} - 1\right)$$

$$E = \left(\frac{F_s(\xi_r)}{F(\lambda^{p^r})}\right)^2\left(1 - \left(\frac{F(\xi_r)}{F_s(\xi_r)}\right)^2\right)\left(\frac{1}{\xi_0} - \frac{t^{p-1}}{\xi_1}\right).$$

In the formula for E, the first two factors are congruent modulo t^{p^r} to a function of λ (which takes integral values in $\mathfrak{P}$), while the third factor has by an easy computation no term in t^N. Thus we may discard E when computing the coefficient of t^N. Likewise

the multiplier of C in equation (4.29) is congruent modulo t^{p^r} to a function of λ assuming only unit values in $\mathfrak{P}$. We note that

$$H = C + \left(\frac{1}{\xi_0} - \frac{t^{p-1}}{\xi_1}\right)$$

and the coefficient of t^N in the second term is (as noted previously) zero. Thus h is the coefficient of t^N in $C(\lambda, t)$, and now we know that

$$|h(\lambda)| \leq |p^{s+1}/\lambda^{N+1}|$$

for all $\lambda \in \mathfrak{P}$. However C is the sum of a power series in ξ_0 and a power series in ξ_1, each converging for all $(\lambda, t) \in \mathfrak{P} \times \mathfrak{P}$ and hence h is a rational function having no pole in $\mathfrak{P}$. Clearly the expression for C shows that for some integer $\nu \geq 0$,

$$h = l/(M/\lambda)^{\nu}$$

where l is a polynomial. Since M/λ assumes unit values for $\lambda \in \mathfrak{P}$, we conclude that $|\lambda^{N+1} l(\lambda)|$ is bounded by $|p^{s+1}|$ everywhere in $\mathfrak{P}$, and hence each coefficient of l is so bounded. Thus

$$|l(\lambda)| \leq |p^{s+1}|$$

for all $\lambda \in \mathfrak{O}$. Since M/λ assumes unit values at all $\lambda \in \mathfrak{D}_1$, $\lambda \notin 1 + \mathfrak{P}$, the proof of (4.27) is completed.

To prove the theorem, it is enough (by the criterion of [1], Lemma 1, as applied to an element of $K_T[[t]]$) to show that for $\alpha \in \mathfrak{D}_1$, $\alpha \neq 0, 1$, α fixed under a power of τ,

$$p w_\alpha(\alpha + t) \equiv \tau w_\alpha(\alpha + t^p) \mod p\mathfrak{O}_T[[t]],$$

where τ operates only on the coefficients. This reduces to the demonstration that (for $(m, p) = 1$, $N = mp^{s+1} - 1$, $\xi_j = \alpha^{p^j} + t^{p^j} (j \geq 0)$) the coefficient of t^N in

$$\frac{1}{\xi_0(1-\xi_0)} \frac{1}{u_\alpha(\xi_0)^2 F_0(\alpha)^2} - \frac{t^{p-1}}{\xi_1(1-\xi_1) u_{\alpha^p}(\xi_1)^2 (F_0(\alpha)^\tau)^2}$$

is bounded by $|p^{s+1}|$. Since $u_{\alpha^{p^r}}(\xi_r) \equiv 1 \mod t^{p^r}$, the coefficient is not changed if we multiply by $(u_{\alpha^{p^r}}(\xi_r))^2$. Doing this, and using equation (3.16) in the form $(\alpha_r = \alpha^{p^r})$

$$(u_\alpha(\xi_0)/u_{\alpha_r}(\xi_r)) \prod_{j=0}^{r-1} f(\alpha_j) \equiv F_{s+r}(\xi_0)/F_s(\xi_r) \mod p^{s+1}[[t]],$$

and using the definition of $F_0(\alpha)$, we conclude that the coefficient of t^N is congruent modulo p^{s+1} to its coefficient in

$$\left(\left(\prod_{j=0}^{r-1} f(\alpha_j)\right) F_s(\xi_r)/F_0(\alpha)\right)^2 H(\alpha, t).$$

Thus aside from a unit, the coefficient is congruent modulo p^{s+1} to $h(\alpha)$. The theorem now follows from equation (4.27).

Since $w_\alpha \equiv (\alpha(1-\alpha)(F_0(\alpha))^2)^{-1}t \bmod t^2$ we conclude that $\exp w_\alpha$ assumes all values in $1+\mathfrak{P}$ as t runs through $\mathfrak{P}$. This shows that w_α has p-adic behavior similar to that of the logarithm function.

We note that $F_0(\alpha)u_\alpha(\lambda)$ plays a role in Tate's model ([2], § 5) for the points near infinity of a non-supersingular elliptic curve defined over a local field. In the context of the Legendre normal form given by equation (4.1), if t is a uniformizing parameter at infinity, say $x=1/t^2$ ($|t|<1$) then the integral of the first kind may be expressed locally as dz where

$$z(t)=\sum_{n=0}^{\infty} t^{2n+1}(-1)^n \binom{-\frac{1}{2}}{n} F\left(\frac{1}{2}, n, \frac{1}{2}, n, \lambda\right) \Big/ (2n+1).$$

For $\lambda \in \alpha+\mathfrak{P}$, α as in the above theorem, $i^2=-1$, then

$$t \to \exp(z(t)/(iF_0(\alpha)u_\alpha(\lambda)))$$

gives an isomorphism (defined over $K_T(\lambda)$) between the points of (4.1) with non-integral coordinates and $1+\mathfrak{P}$. The main point in the proof is the fact that this exponential lies in $(\mathfrak{O} \cap K_T(\lambda))[[t]]$, a result which follows (as indicated in the above reference) by the methods of § 1, 2 above.

We conclude this section by noting that no information has been obtained concerning the solutions of (4.2) near roots of g, i.e. when the reduction is supersingular. Indeed all solutions are unbounded in that case as will be shown in § 8 *c)* below.

§ 5. Uniqueness of Formulae.

Let $k=GF[q]$ and let K be the unramified extension of $\mathbf{Q}_p$ with residue class field k. (We could assume K is any finite extension of $\mathbf{Q}_p$ with residue class field k). Let $\overline{\mathfrak{S}}$ be a hypersurface in affine n-space of characteristic p defined over k, let $\mathfrak{S}$ be the set of all points in $\mathfrak{O}^n$ whose reduction mod $\mathfrak{p}$ lies in $\overline{\mathfrak{S}}$, and let $\mathfrak{D}$ be the complement of $\mathfrak{S}$ in $\mathfrak{O}^n$.

We say that an Ω-valued function H is *holomorphic* on $\mathfrak{D}$ if it is the uniform limit (on $\mathfrak{D}$) of rational functions whose polar locus (in $\mathfrak{O}^n$) lies in $\mathfrak{S}$. If in addition these rational functions may be chosen in $K(X)$ ($X=(X_1, \ldots, X_n)$) then we say that H is holomorphic on $\mathfrak{D}$ and *defined* over K. For $x=(x_1, \ldots, x_n) \in \Omega^n$ we define $x^p=(x_1^p, \ldots, x_n^p)$. Our object is to prove the following theorem due to Katz.

Theorem 5. — *Let* H *be holomorphic on* $\mathfrak{D}$ *and defined over* K *with the property that*

$$\prod_{i=0}^{s-1} H(x^{q^i})=1 \quad \textit{whenever } x \in \mathfrak{D} \textit{ and } x^{q^s}=x. \tag{5.1}$$

We may then conclude that there exists G *holomorphic on* $\mathfrak{D}$, *defined over* K *and assuming unit values on* $\mathfrak{D}$ *such that*

$$H(x)=G(x)/G(x^q)$$

everywhere in $\mathfrak{D}$.

The proof of the theorem depends upon a well known consequence of the Riemann hypothesis for curves.

Lemma. — *Let* $f \in k[X_1, \ldots, X_n, t]$ *be of degree r in the variable t with no divisor in* $k[X]$. *Suppose that there exists a Zariski open set* U *in affine n-space such that for each* $x \in U$ *which is algebraic over k there exist r distinct points (rational over* $k(x)$*) on the hypersurface* $f = 0$, *whose projection on X-space is x. Then the polynomial splits over* $k(X)$ *into r distinct factors, each linear in t.*

Proof. — A trivial computation shows that the number N_s of points of the hypersurface $f = 0$ rational over $GF[q^s]$ is asymptotically

$$N_s = rq^{ns} + O(q^{(n-1)s}).$$

On the other hand the estimates of Weil and Lang [10] show that

$$N_s = r' q^{ns} + O(q^{\left(n-\frac{1}{2}\right)s})$$

where r' is the number of components irreducible over k. The conclusion is that $r = r'$. Thus f splits over k into r distinct factors, none lying in $k[X]$ and hence, in each factor, t must appear to the degree 1.

Proof of theorem. — By hypothesis there exists $h \in K(X)$ such that for $x \in \mathfrak{D}$

$$h(x) \equiv H(x) \mod p.$$

For $x^{q^s} = x$, $h(x^q)$ is the image of $h(x)$ under the Frobenius automorphism of $K(x)$ over K and hence, by (5.1), $h(x)$ is a unit. It is well known (cf. Lemma (1.2) in [12]) that if a polynomial in $\Omega[X]$ assumes unit values at a set of representatives in $\mathfrak{O}^n$ of the algebraic points of a Zariski open set in characteristic p then the polynomial lies in $\mathfrak{O}[X]$ and has non-trivial reduction mod p. Thus h must be a ratio h_1/h_2 of elements of $\mathfrak{O}_K[X]$ which have non-trivial reduction mod p. The same unicity of $h(x)$ for each $x^{q^s} = x$, $x \in \mathfrak{D}$ shows that if the hypersurface $\overline{h}_1 = 0$ (resp. $\overline{h}_2 = 0$), defined over k, has a component not contained in $\overline{\mathfrak{S}}$, then that component must lie in $\overline{h}_2 = 0$ (resp. $\overline{h}_1$) and hence the degrees of h_1 and h_2 may be reduced. We may conclude that h_1, h_2 may be chosen such that the zero loci of $\overline{h}_1$ and $\overline{h}_2$ both lie in $\overline{\mathfrak{S}}$. Thus $\overline{h} = \overline{h}_1/\overline{h}_2$ is well defined and never zero on the complement of $\overline{\mathfrak{S}}$.

If $\overline{x}$ is an algebraic point in this complement of $\overline{\mathfrak{S}}$ then by (5.1)

$$N_{k(\overline{x})/k}\overline{h}(\overline{x}) = 1$$

and hence there exists $\overline{t}$ in $k(\overline{x})$ such that

$$\overline{t}^{q-1} = \overline{h}(\overline{x}) \neq 0,$$

and since the $(q-1)$-th roots of unity lie in k, there are $q-1$ distinct points on the hypersurface $\overline{h}_2(X)t^{q-1} = \overline{h}_1(X)$, rational over $k(\overline{x})$ with projection $\overline{x}$ in X-space. The lemma therefore shows the existence of $\overline{g} \in k(X)$ such that

$$\overline{g}^{q-1} = \overline{h}.$$

Clearly the zero and polar loci of $\overline{g}$ lie in $\overline{\mathfrak{S}}$ and we have

$$\overline{g}(X^q)/\overline{g}(X)=\overline{h}(X).$$

Let g be a lifting of $\overline{g}$ to $K(X)$ obtained by lifting the numerator and denominator. Thus g maps $\mathfrak{D}$ into the unit group, and for all $x\in\mathfrak{D}$

$$H(x)\equiv g(x^q)/g(x) \mod p.$$

Thus we may assume that $H(X)\equiv 1 \mod p$ everywhere on $\mathfrak{D}$. More generally suppose $\nu\geq 1$, $H\equiv 1 \mod p^\nu$ everywhere on $\mathfrak{D}$, then we may choose $h\in K(X)$ such that on $\mathfrak{D}$

$$H\equiv 1+p^\nu h \mod p^{\nu+1}$$

and such that h assumes integral values on $\mathfrak{D}$. Thus by the argument used previously, $h=h_1/h_2$, h_1 and h_2 lie in $\mathfrak{O}_K[X]$ and $\overline{h}_2\neq 0$. Furthermore the argument used before shows that the reduced hypersurface $\overline{h}_2=0$ lies in $\overline{\mathfrak{S}}$.

If now $x\in\mathfrak{D}$, $x^{q^s}=x$ then by (5.1)

$$N_{K(x)/K}(1+p^\nu h(x))\equiv 1 \mod p^{\nu+1}$$

and hence

$$S_{K(x)/K}h(x)\equiv 0 \mod p.$$

Thus $S_{k(\overline{x})/k}\overline{h}(\overline{x})=0$ and hence there exists $\overline{t}\in k(\overline{x})$ such that

$$\overline{t}^q-\overline{t}=\overline{h}(\overline{x}).$$

Furthermore there are clearly q distinct choices for $\overline{t}$ in $k(\overline{x})$ and hence the lemma may be applied to the hypersurface

$$\overline{h}_2(X)(t^q-t)=\overline{h}_1(X),$$

showing that there exists $\overline{g}\in k(X)$ such that

$$\overline{g}^q-\overline{g}=\overline{h}$$

and by unique factorization in $k[X]$, the polar locus of $\overline{g}$ lies in $\overline{\mathfrak{S}}$. Thus g may be lifted to a polynomial g assuming integral values in $\mathfrak{D}$ such that on $\mathfrak{D}$,

$$\frac{1+p^\nu g(x^q)}{1+p^\nu g(x)}\equiv 1+p^\nu(g^q-g)\equiv 1+p^\nu h\equiv H \mod p^{\nu+1}.$$

Thus we may reduce to the case $H\equiv 1 \mod p^{\nu+1}$. Thus there exist a sequence $g_0, g_1, \ldots$ of elements of $K(X)$ such that

g_0 assumes unit values in $\mathfrak{D}$
g_i assumes integral values in $\mathfrak{D}$

and such that if we set

$$G=g_0\cdot\prod_{i=1}^{\infty}(1+p^i g_i)$$

then

$$H(x)=G(x)/G(x^q)$$

everywhere in $\mathfrak{D}$.

Corollary. — *Equation* (5.1) *is impossible if, on* $\mathfrak{D}$, H mod p *may be represented by a non-constant polynomial* $\overline{h} \in k[X]$ *of degree strictly less than* $q-1$. *Indeed, it is impossible if, on* $\mathfrak{D}$, H mod p *may be represented by a rational function which is not a* $(q-1)$*-th power* mod p.

In the applications, we shall encounter the situation in which H is a function of one variable and locally of the form $F(X)/F(X^p)$, where F is a local solution of a linear differential equation in one variable with rational coefficients, while $\mathfrak{D}$ is the complement of the union of a finite set of neighborhoods of the form $\alpha+\mathfrak{P}$. If equation (5.1) holds then we may conclude from the preceeding theorem that F is itself holomorphic on $\mathfrak{D}$. The following conjectures seem natural.

1. If all the singular points of the differential equation lie in $\mathfrak{D}$ then F must be a constant.

2. Let us say that an ordinary linear differential equation with coefficients in $\Omega(X)$ is *rigid* if there exists a solution, not in $\Omega(X)$, which is an analytic element whose support has an infinite image (in the residue class field of Ω) under reduction mod $\mathfrak{P}$. If the ceofficients of the differential equation lie in $K(X)$, where K is an algebraic number field, then for each finite prime $\mathfrak{p}$ of K there is the notion of $\mathfrak{p}$-rigidity. We conjecture that a given ordinary linear differential equation with coefficients in $K(X)$ can be $\mathfrak{p}$-rigid for not more than a finite set of primes of K.

§ 6. Analytic Theory of Frobenius Mapping.

a) Introduction.

In this section we shall consider a one parameter family defined over an algebraic number field. We shall show that the p-adic theory of zeta functions of hypersurfaces ([4], § 5) may be restated in terms of endomorphisms of solution spaces of the Fuchs-Picard differential equation (i.e. the equations satisfied by the periods of the primitive cohomology classes in the middle-dimensional cohomology group H^{n-1}) and how this may be used to decompose our model for homology into subspaces stable under our analytic formulation of the Frobenius map. In particular the rational solutions and also the locally bounded solutions provide examples of such stable subspaces.

b) Frobenius Transformation of Solutions of Fuchs-Picard Differential Equation.

We use the notation of ([4], § 5) with some slight variations as will now be noted. We shall suppose that $f(\lambda, X) \in K[\lambda, X_1, X_2, \ldots, X_{n+1}]$ (where K is an algebraic number field) and is homogeneous in X. For each rational prime p, let Ω be the completion of the algebraic closure of the p-adic rationals $\mathbf{Q}_p$, and we suppose that an imbedding of K in Ω has been chosen and that q is the cardinality of the residue class field of K for this valuation. We shall use the symbol $\mathfrak{R}_\lambda$ (resp. $\mathfrak{W}_\lambda$) for the space denoted by $\mathfrak{R}_\lambda/\mathfrak{R}_\lambda^S$ (resp. $\mathfrak{W}_\lambda^S$) in [4]. Thus $\mathfrak{R}_\lambda$ is the finite dimensional $K(\lambda)$-space of solutions of

$$\mathbf{(6.1)} \qquad D_{i,\lambda}^{*}\xi^{*}=0, \quad i=1, 2, \ldots, n+1$$

modulo those solutions which contain no monomial involving all $n+1$ variables. On the other hand, for $z\in\Omega$, the specialized form of these partial differential equations define a vector space over $K(z)$, but we shall understand $\mathfrak{R}_z$ to refer to the tensor product of that space with Ω. (Thus $\mathfrak{R}_\lambda$ is an $\Omega(\lambda)$-space, while $\mathfrak{R}_z$ is an Ω-space.)

Since we shall at times be interested in fibers, $0=f(z, X)$, with singular reductions, we must recall estimates for the representatives of the elements of $\mathfrak{R}_z$. Let

$$R(\lambda) \text{ be the resultant of the polynomials } \left\{x_i\frac{\partial f}{\partial X_i}\right\}_{i=1}^{n+1},$$

$$L_-(b)=\{\sum_{w\in\mathfrak{T}} A_w X^{-w} \mid \operatorname{ord} A_w \geq -bw_0+O(\log w_0)\}$$

$$b'(z) = \operatorname{ord} R(z)-k \operatorname{Min}(0, \operatorname{ord} z)$$

(cf. equation (5.11), [4]). Then for $R(z)\neq 0$, $\mathfrak{R}_z$ has a set of representatives in $L_-(b'(z))$.

Katz [8] has exhibited a natural isomorphism between $\mathfrak{W}_\lambda$ and the primitive cohomology classes in middle dimension and shown that under this isomorphism, the differential operator (on $\mathfrak{W}_\lambda$)

$$\sigma_\lambda=\frac{\partial}{\partial\lambda}+\pi X_0\frac{\partial f}{\partial\lambda}$$

is replaced by the operation of differentiating cohomology classes with respect to the parameter λ.

Let $\mathfrak{M}_z$ denote the field of germs of functions of λ meromorphic at z, let

$$T_{z,\lambda}=\gamma_-\circ\exp \pi X_0(f(z, X)-f(\lambda, X))$$

then the diagram

$$\begin{array}{ccc} \mathfrak{R}_z\otimes\mathfrak{M}_z & \xrightarrow{T_{z,\lambda}} & \mathfrak{R}_\lambda\otimes\mathfrak{M}_z \\ \downarrow{\scriptstyle \frac{\partial}{\partial\lambda}} & & \downarrow{\scriptstyle \sigma_\lambda^*} \\ \mathfrak{R}_z\otimes\mathfrak{M}_z & \xrightarrow{T_{z,\lambda}} & \mathfrak{R}_\lambda\otimes\mathfrak{M}_z \end{array}$$

commutes, σ_λ^* being the dual of σ_λ.

Let $\{\xi_i\}_{i=1}^N$ be a basis of $\mathfrak{W}_\lambda$ as vector space over $K(\lambda)$, let $\{\xi_{i,\lambda}^*\}_{i=1}^N$ be a set of representatives in $K(\lambda)[[X^{-1}]]$ of the dual basis of $\mathfrak{R}_\lambda$. If ω_i is the cohomology class associated by Katz with ξ_i $(i=1, 2, \ldots, N)$, then for a fixed cycle γ on the generic fiber $f(\lambda, X)=0$, if we set

(6.2) $$\mathfrak{X}_\gamma=\left(\int_\gamma\omega_1, \ldots, \int_\gamma\omega_N\right)$$

then $\mathfrak{X}_\gamma$ satisfies the Fuchs-Picard equation

(6.3) $$\frac{\partial\mathfrak{X}}{\partial\lambda}=\mathfrak{X}B$$

where B is a matrix with coefficients in $K(\lambda)$. On the other hand if for an element ξ^* of $\mathfrak{R}_z$ we write explicitly

$$\mathbf{(6.4)} \qquad T_{z,\lambda}\xi^* = \sum_{i=1}^{N} \mathfrak{X}_i \xi^*_{i,\lambda}$$

with each $\mathfrak{X}_i$ in $\mathfrak{M}_z$, then $\left(\text{since } \frac{\partial \xi^*}{\partial \lambda} = 0\right)$ once again $\mathfrak{X} = (\mathfrak{X}_1, \ldots, \mathfrak{X}_N)$ satisfies equation (6.3). This permits us to view $\mathfrak{R}_z$ as the p-adic analogue of the space of cycles of the fiber $f(z, X) = 0$, but we prefer to view the solutions of (6.3) in $\mathfrak{M}_z$ as this analogue.

It follows from equation (6.4) and our estimates that the solutions of (6.3) converge for $\lambda \in z + \mathfrak{P}$ if

$$\mathbf{(6.5)} \qquad |R(z)| = 1, \quad |z| \leq 1$$

but in general the solutions converge if

$$\mathbf{(6.6)} \qquad \text{Min ord}(f(\lambda, X) - f(z, X)) > b'(z)$$

the minimum being over all X such that $|X| = 1$.

For application to zeta functions we must explain the operation of Frobenius on solutions of (6.3). For this we set

$$F(z, X) = \exp(\pi X_0 f(z, X) - \pi X_0^q f(z^q, X^q))$$

$$\alpha_z^* = \gamma_- \circ \frac{1}{F(z, X)} \circ \Phi$$

and recall that $F(z, X)$ lies in $L(q^{-1}b(z))$ where

$$b(z) = \text{Min}\left\{\frac{p-1}{p} + qd_\lambda \text{ Min}(0, \text{ord } z), \nu_p\right\}$$

$$d_\lambda = \deg_\lambda f$$

$$\nu_p = \text{Inf ord}(a^q - a)$$

the inf being over all a in K which appear as coefficients of f. Clearly $\nu_p \geq 1$ if p is unramified in K (for the chosen imbedding of K into Ω). From this it follows that α_z^* is a well defined map of $\mathfrak{R}_{z^p}$ onto $\mathfrak{R}_z$ provided

$$\mathbf{(6.7)} \qquad b(z) > b'(z^q).$$

Equation (6.5) defines a quasi-connected domain, which is certainly non-empty if R has non-trivial reduction mod p. For z in this domain, we have the mapping

$$\alpha_\lambda^* : \mathfrak{R}_{\lambda^q} \otimes \mathfrak{M}_z \to \mathfrak{R}_\lambda \otimes \mathfrak{M}_z$$

defined by a formula similar to that for α_z^*. The matrix A_λ of this mapping relative to basis $\{\xi^*_{i,\lambda^q}\}$ (resp. $\{\xi^*_{i,\lambda}\}$) of $\mathfrak{R}_{\lambda^q}$ (resp. $\mathfrak{R}_\lambda$) is (cf. equation (5.27), [4]) a (matrix) uniform analytic function of support given by equation (6.5). To describe the action of α_z^* on cycles of the fiber, $f(z, X) = 0$, we must use the isomorphism φ of $\mathfrak{M}_{z^q}$ into $\mathfrak{M}_z$

obtained by composition with the q-th power map (i.e., for each function h of λ, $(\varphi h)(\lambda)=h^{\varphi}(\lambda)=h(\lambda^q)$). The mapping φ is onto if $z\neq 0, \infty$, as will be assumed. In the following commutative diagram, the same symbol φ denotes the mapping of $\mathfrak{K}_{\lambda}\otimes\mathfrak{M}_{z^q}$ onto $\mathfrak{K}_{\lambda^q}\otimes\mathfrak{M}_z$ induced from the mapping of $\mathfrak{M}_{z^q}[[X^{-1}]]$ onto $\mathfrak{M}_z[[X^{-1}]]$ deduced from the coefficient-wise action of φ:

$$\begin{array}{ccccc}
\mathfrak{K}_{z^q} & & \xrightarrow{\quad\alpha_z^*\quad} & & \mathfrak{K}_z \\
\Big\downarrow{\scriptstyle T_{z^q,\lambda}} & & & & \Big\downarrow{\scriptstyle T_{z,\lambda}} \\
\mathfrak{K}_{\lambda}\otimes\mathfrak{M}_{z^q} & \xrightarrow[\varphi]{} & \mathfrak{K}_{\lambda^q}\otimes\mathfrak{M}_z & \xrightarrow[\alpha_{\lambda}^*]{} & \mathfrak{K}_{\lambda}\otimes\mathfrak{M}_z
\end{array}$$

The diagram shows that

(6.8) $$\mathfrak{X}\to\mathfrak{X}^{\varphi}A_{\lambda}$$

is a monomorphism of solutions of (6.3) in $\mathfrak{M}_{z^q}$ into solutions in $\mathfrak{M}_z$, provided z satisfies condition (6.7). If neither z nor z^q is a singularity of the differential equation then this mapping is an isomorphism between the solution spaces viewed as vector spaces over Ω.

c) Singularities of Fuchs-Picard Differential Equation.

In the application we shall restrict our attention to those p for which the following hypothesis is satisfied.

Let S′ be the set of distinct zeros of R, $S=S'\cup\{\infty\}$. For each $s\in S$ let

$$t_s=\begin{cases}\lambda-s & \text{if } s\in S'\\ 1/\lambda & \text{if } s=\infty.\end{cases}$$

Hypothesis. — I. R is not zero mod $\mathfrak{P}$, its zeros all lie in $\mathfrak{O}$ and no two distinct zeros lie in the same residue class mod $\mathfrak{P}$.

II. For each $s\in S$, there exists an $N\times N$ matrix G_s with coefficients in $\mathbf{Q}$ and an $N\times N$ matrix Y_s with coefficients in $K(s)[[t_s]]$ such that Y_s converges for $|t_s|<1$ and such that $t_s^{G_s}Y_s$ is a solution matrix of equation (6.3) in $\mathfrak{M}_z$ for $0<|t_s(z)|<1$.

In the statement of this hypothesis, the symbol t^G represents for each $z\neq 0, \infty$ a solution matrix in $\mathfrak{M}_z$ of the differential equation

(6.9) $$t\frac{d\xi}{dt}=\xi G$$

and hence is unique up to multiplication by constant non-singular $N\times N$ matrices.

An explicit choice of t^G is given by $\exp(G\log(t/z))$.

The object of this section is to show that if R is not identically zero (i.e. if the generic fiber $f(\lambda, X)=0$ is non-singular in characteristic zero) then the above hypothesis is valid for almost all p.

It is clear that hypothesis I is valid for almost all p. We shall assume that hypothesis in the following.

If $|z|\leq 1$, $z\notin s+\mathfrak{P}$ for any $s\in S'$ then $|R(z)|=1$ and as noted before, equation (6.3) has a solution matrix which converges in $z+\mathfrak{P}$. Hypothesis II is a weaker form of this situation for neighborhoods of singularities. We note that the singularities of the differential equation (6.3) lie in S since the zeros of the polynomial g (cf. equation (5.7), [4]) are non-essential singularities of (6.3) (cf. Note (iii), § 10, *loc. cit.*).

The validity of Hypothesis II may be examined by considering just one point of S. Let $s\in S$, $K_1=K(s)$ and we shall suppose that s has been translated to the origin so that $s=0$ and that equation (6.3) has been modified accordingly.

It is known [5] that the singularities of (6.3) are regular (in the sense of Fuchs) and hence the classical solution matrix (near the origin) has the form

$$\lambda^G Y$$

where G is a constant matrix with coefficients in $\mathbf{C}$ and Y has coefficients in $\mathbf{C}[[\lambda]]$. However $\exp(2\pi iG)$ is the monodromy matrix for the transformation of the integral homology (in the middle dimension) of a generic fiber corresponding to a circuit in λ-space about the origin. It is known [6] that the eigenvalues of this matrix are roots of unity and hence the eigenvalues of G are rational numbers. Replacing Y by HY and λ^G by $H\lambda^G H^{-1}$ for suitable non-singular constant matrix H, we may suppose that G is in Jordan normal form,

$$G=D+N$$

where D is a diagonal matrix with rational coefficients and N is a nilpotent matrix which commutes with D.

As is well known, Y satisfies the differential equation

$$\frac{dY}{d\lambda}+\frac{G}{\lambda}Y=YB \tag{6.10}$$

with coefficients in $K_1(\lambda)$ and hence the solution Y may be chosen with coefficients in $K_1[[\lambda]]$ (instead of $\mathbf{C}[[\lambda]]$). Since (6.9) is a system of N^2 simultaneous linear differential equations, it is known [20] that for almost all p, Y converges for

$$\operatorname{ord}\lambda>N^2/(p-1). \tag{6.11}$$

If p is prime to the denominators of the entries of the matrix D, then, replacing q, if necessary, by a power,

$$(q-1)\nu\in\mathbf{Z}$$

for each eigenvalue ν of G. We assert the existence of a non-singular diagonal matrix H with the rational coefficients and of a diagonal matrix G_0 with coefficients in $\mathbf{Z}$ such that

$$qG=H^{-1}GH+G_0. \tag{6.12}$$

To prove this we note that $\mathcal{N}$ may be assumed to be the matrix of the transformation T of a vector space with basis $\{v_1, \ldots, v_r\}$ given by

$$\mathrm{T}v_i = v_{i+1} \qquad i = 1, 2, \ldots, r-1$$
$$\mathrm{T}v_r = 0.$$

Thus if we put $v_i' = q^{i-1}v_i \quad i = 1, 2, \ldots, r$

then $q\mathrm{T}v_i' = v_{i+1}' \quad i = 1, 2, \ldots, r-1$

$$q\mathrm{T}v_r' = 0$$

which shows that $q\mathcal{N} = H^{-1}\mathcal{N}H,$

where H is the matrix corresponding to the change of basis. By our choice of q, if we put $G_0 = (q-1)D$, then G_0 is diagonal with coefficients in $\mathbf{Z}$ and

$$qG = qD + q\mathcal{N} = G_0 + D + H^{-1}\mathcal{N}H.$$

The assertion (6.12) now follows as $D = H^{-1}DH$ since both D and H are diagonal.

We now show that in general Υ converges in the open unit disk.

Theorem 6. — For almost all p, Υ converges in the open unit disk with center at $\lambda = 0$. More precisely, this is the case if

(i) *The only zero of* R *in the open unit disk is at the origin.*

(ii) *The denominators of the eigenvalues of G are prime to p.*

(iii) *The lower bound (equation (6.11)) for the domain of convergence is valid.*

(iv) $$(p-1)^{-1}\mathrm{N}^2 < (p\mu)^{-1}(p-1),$$

where μ is the order of the zero of R *at the origin.*

(v) *The prime p is unramified in* K_1.

Proof. — Under these hypotheses, equation (6.7) shows that A_λ is a uniform analytic function of support given by

(6.13) $$\operatorname{ord}\lambda < (p-1)/(pq\mu).$$

For each rational $\nu > 0$, let U_ν be the space of (Ω-valued) functions analytic on the set

$$\{\lambda \in \Omega \mid \operatorname{ord}\lambda = \nu\}.$$

Let t be a rational number in the interval $\left(0, \dfrac{p-1}{p\mu}\right)$ and let $\lambda^G \Upsilon_1$ be a solution matrix of (6.3) with coefficients in $\mathfrak{M}_{z^q}$ for some z^q such that $\operatorname{ord} z^q = t$. (This means that a branch of λ^G has been chosen at z^q.) Suppose that Υ_1 has coefficients in U_t. Using λ^{qG} to denote the image of λ^G under φ, equation (6.8) shows that $\lambda^{qG}\Upsilon_1(\lambda^q)A_\lambda$ is a solution matrix of (6.3) in $\mathfrak{M}_z$, but

$$\Upsilon_1(\lambda^q)A_\lambda \in \mathrm{U}_{t/q}.$$

We now use equation (6.12) to write the solution matrix in $\mathfrak{M}_z$ in the form

$$\lambda^{H^{-1}GH}\Upsilon_2$$

where

$$\Upsilon_2(\lambda)=\lambda^{G_0}\Upsilon_1(\lambda^q)A_\lambda.$$

It is clear that Υ_2 satisfies equation (6.10) with G replaced by $H^{-1}GH$. Thus $H\Upsilon_2$ satisfies equation (6.10) in its original form. Thus

$$\tau : \Upsilon_1 \to H\Upsilon_2$$

is a linear mapping of matrix solutions of (6.10) with coefficients in U_t into matrix solutions with coefficients in $U_{t/q}$. For each integer $j \geq 0$, let V_j be the space of all $N\times N$ matrices with coefficients in U_{t/q^j} which satisfy (6.10). We may extend τ to a monomorphism of V_j into V_{j+1} for each j.

Each element of U_t is a formal Laurent series in λ with coefficients in Ω and hence each element ξ of V_j is a formal Laurent series in λ with coefficients which are $N\times N$ matrices (with coefficients in Ω) such that ξ formally satisfies (6.10). The set of all such formal Laurent series solutions constitue a finite dimensional Ω-space and we may choose an integer m, such that $V_i \subset V$ for each integer i, V being $\sum_{j=0}^{m} V_j$. Thus V is a finite dimensional space which is stable under the monomorphism τ. Thus in particular for each integer r,

$$V+\tau^r V \subset \sum_{j=r}^{r+m} V_j.$$

For each $\eta\in V$, we may uniquely write

$$\eta=\eta^+ + \eta^-$$

where the coefficients of η^+ lie in $\Omega[[\lambda]]$ and those of η^- lie in $\lambda^{-1}\Omega[[\lambda^{-1}]]$. If $\eta\in V_j$ then η^+ converges for

$$\text{ord}\,\lambda > t/q^j$$

and thus we may conclude that for each $\eta\in V$, η^+ converges in $\mathfrak{P}$. By hypothesis Υ converges in the disk defined by equation (6.11). If we choose t in the interval $((p-1)^{-1}N^2, (p\mu)^{-1}(p-1))$ then the coefficients of Υ lie in U_t and $\Upsilon\in V_0$. The theorem now follows from the fact that $\Upsilon=\Upsilon^+$.

d) Transformation matrix near singular points.

The matrix A_λ depends in a non-trivial way upon the choice of the origin. Information about the behavior of A_λ near points of S is quite useful. For our present purposes it will be enough to consider the case in which the singularity is at the origin. (This involves a slight further loss in generality as it requires that the field K be extended, as noted in the previous section.)

Naturally the discussion of this section will be based upon the hypotheses I, II of paragraph *c)*. We shall also use the following result, whose proof has been given

in an earlier article (*On p-adic Analysis*, Proc. of the Science Conference, Yeshiva University, 1966).

Lemma **(6.1).** — *Let* U *be the field of functions meromorphic on an annulus, with center at the origin. Let* $\nu_1, \ldots, \nu_r$ *be elements of* Ω *no two of which differ by a rational integer. Let* z *be an element of the annulus, let* η *be a germ at* z *of* $\log t$ *and for* $1 \leq i \leq r$ *let* ξ_i *be a germ at* z *of* t^{ν_i}. *Then* U *has a natural imbedding in* $\mathfrak{M}_z$ *and in this sense the elements* $\{\xi_i \eta^j\}$ $(j \geq 0; i = 1, 2, \ldots, r)$ *are linearly independent over* U.

In the following the matrix $G = D + \mathcal{N}$ is used in the same sense as in paragraph *c)*.

Lemma **(6.2).** — *There exist constant* $(N \times N)$ *matrices* A, θ *such that*

$$A\mathcal{N} = q\mathcal{N}A \tag{6.14}$$

$$\theta \mathcal{N}^t + \mathcal{N}\theta = 0 \tag{6.15}$$

$$q^{n+1}\theta = A\theta A^t \tag{6.16}$$

and such that in $\mathfrak{P}$

$$A_\lambda = \Upsilon(\lambda^q)^{-1} \mathfrak{A} \Upsilon(\lambda) \tag{6.17}$$

where $\mathfrak{A} = \lambda^{-qD} A \lambda^D$, *a well defined matrix whose coefficients are monomials in* λ. *Furthermore* θ *is symmetric* (resp. *skew symmetric*) *if* $n+1$ *is even* (resp. $n+1$ *odd*).

Proof. — We know that A_λ is analytic in an annulus of outer radius unity with center at the origin. Let z be a point in the annulus. We know that $\exp(G \log(\lambda/z^q)) \cdot \Upsilon$ (resp. $\exp(G \log(\lambda/z)) \cdot \Upsilon$) is a solution matrix of (6.3) with coefficients in $\mathfrak{M}_{z^q}$ (resp. $\mathfrak{M}_z$) and hence equation (6.8) shows the existence of a constant matrix H (depending on z) such that in a neighborhood of z,

$$H \exp(G \log(\lambda/z)) \Upsilon(\lambda) = \exp(qG \log(\lambda/z)) \Upsilon(\lambda^q) A_\lambda.$$

Thus (6.17) holds with

$$\mathfrak{A} = \exp(-qG \log(\lambda/z)) H \exp(G \log(\lambda/z)).$$

Equation (6.17) shows that $\mathfrak{A}$ is analytic in the annulus. Write this last relation in the form

$$\exp(qD \log(\lambda/z)) \mathfrak{A} \exp(-D \log(\lambda/z)) = \exp(-q\mathcal{N} \log(\lambda/z)) H \exp(\mathcal{N} \log(\lambda/z)).$$

Since D is diagonal, $\log \lambda$ does not appear on the left side and hence by the preceding lemma cannot appear on the right side. An easy computation shows that

$$H\mathcal{N} = q\mathcal{N}H \tag{6.14}'$$

and that the right side is just H. The relation may now be written in the form

$$\mathfrak{A} = \exp(-qD \log(\lambda/z)) H \exp(D \log(\lambda/z))$$

and again using Lemma (6.1) and the analyticity of $\mathfrak{A}$, we conclude that if ν_i $(i = 1, 2, \ldots, N)$ is the i-th diagonal element of the matrix D, then $-q\nu_i + \nu_j$ is a rational integer, which we will denote by $t_{i,j}$.

Let A be the $N\times N$ matrix whose (i,j) component is $H_{ij}/z^{i,j}$. It is natural to define $\lambda^{-qD}A\lambda^{D}$ to be the $N\times N$ matrix whose (i,j) component is obtained from the corresponding component of A by multiplication by $\lambda^{i,j}$. This shows that $\mathfrak{A}=\lambda^{-qD}A\lambda^{D}$ which completes the proof of equation (6.17). Equation (6.14) follows from (6.14)', the relation $A=z^{qD}Hz^{-D}$ and the fact that between D and N commute.

Equation (6.15) is based on ([4], Lemma (6.7)) which shows that the matrix M_λ of the $K(\lambda)$-linear map Θ_λ of $\mathfrak{R}_\lambda$ onto $\mathfrak{W}_\lambda$ can be described locally (at z) by the mapping

$$\mathfrak{R}_\lambda\otimes\mathfrak{M}_z \xrightarrow{T_{z,\lambda}^{-1}} \mathfrak{R}_z\otimes\mathfrak{M}_z \xrightarrow{\Theta_z} \mathfrak{W}_z\otimes\mathfrak{M}_z \xrightarrow{(T_{z,\lambda}^{-1})^t} \mathfrak{W}_\lambda\otimes\mathfrak{M}_z$$

where Θ_z is the specialization of Θ_λ at $\lambda=z$. With our previous notation, the matrix of $T_{z,\lambda}$ (relative to our chosen basis) is fixed by the condition that it be a solution matrix of (6.3) which reduces to the identity matrix at $\lambda=z$. Thus the matrix of $T_{z,\lambda}$ is

$$(\Upsilon(z))^{-1}\exp(G\log(\lambda/z))\Upsilon(\lambda)$$

and equation (6.15) (with $\theta=\Upsilon(z)\Theta_z\Upsilon(z)^t$) follows from Lemma (6.1) and the matrix relation between the rational matrix M_λ of Θ_λ and the product of the three matrices in the above diagram. The argument also shows that

$$\lambda^{-D}\theta\lambda^{-D}$$

is monomial and that

(6.18) $$M_\lambda=\Upsilon^{-1}\lambda^{-D}\theta\lambda^{-D}(\Upsilon^t)^{-1}.$$

Equation (6.17) follows by similar arguments using the matrix relation

(6.19) $$q^{n+1}M_{\lambda^q}=A_\lambda M_\lambda A_\lambda^t$$

proven in [4] for $|R(\lambda)|=1$, $|\lambda|\leq 1$ but obviously valid in the annulus in question by Krasner's uniqueness theorem. This completes the proof of the lemma.

The matrix A seems to have properties of the " specialization " of A_λ at $\lambda=0$ but this is not quite exact since A_λ may very well have a pole at the origin.

The methods could be used to examine the nature of the singularity of A_λ at elements of S'. These are of the form $\log(1+h(t_s))$ where $h\in t^{-1}\mathfrak{P}[t^{-1}]$. At infinity the singularity is again a pole.

e) Rational Solutions.

We now consider the rational solutions of (6.3). To examine the question of stability of these solutions under (6.8) we first consider an apparently larger space.

Let $\mathfrak{R}$ be the space of all functions ξ for which there exists $\varepsilon>0$, such that ξ is analytic on the set

(6.20) $$\{\lambda\,|\,|R(\lambda)|>1-\varepsilon,\ |\lambda|<1+\varepsilon\}.$$

Let V be the space of solutions of (6.3) in $\mathfrak{R}$. Since the coefficients of A_λ lie in $\mathfrak{R}$, it is clear that V is stable under the mapping of (6.8).

Under the hypotheses of paragraph *c)* we have:

Lemma **(6.3).** — *The space of rational solutions of* (6.3) *is* V (*and is thus stable under* (6.8)).

Proof. — Let $\mathfrak{X}$ be an element of V. By the p-adic Liouville theorem it is enough to show that $\mathfrak{X}$ can be continued to a uniform function on Ω with only poles at the points of S. It follows from equation (6.20) that we may restrict our attention to a disk, $|t_s|<1$, of center $s\in S$. By hypothesis $\mathfrak{X}$ is holomorphic in an annulus (of center s) in this disk. It follows from Hypothesis II and Lemma (6.1) that $\mathfrak{X}$ is holomorphic in the punctured disk and has at most a pole at s. This completes the proof of the Lemma.

Let $\mathfrak{R}'$ be the quotient field of $\mathfrak{R}$.

We now view α_λ^* as an $\mathfrak{R}'$-linear mapping of $\mathfrak{K}_{\lambda^q}\otimes\mathfrak{R}'$ onto $\mathfrak{K}_\lambda\otimes\mathfrak{R}'$. By the identification,

$$\mathfrak{X}\mapsto\sum_{i=1}^{N}\mathfrak{X}_i\xi_{i,\lambda}^*, \tag{6.21}$$

the rational solutions of (6.3) correspond to $\mathfrak{K}'_\lambda$, a linear subspace (defined over $K(\lambda)$) of $\mathfrak{K}_\lambda$ and we have seen that $\mathfrak{K}'_{\lambda^q}\otimes\mathfrak{R}'$ is mapped by α_λ^* onto $\mathfrak{K}'_\lambda\otimes\mathfrak{R}$. It is natural to ask for the existence of a subspace $\mathfrak{K}''_\lambda$ of $\mathfrak{K}_\lambda$ (again defined over $K(\lambda)$) which is complementary to $\mathfrak{K}'_\lambda$ and such that α_λ^* maps $\mathfrak{K}''_{\lambda^q}\otimes\mathfrak{R}'$ onto $\mathfrak{K}''_\lambda\otimes\mathfrak{R}'$. To obtain a plausible candidate for $\mathfrak{K}''_\lambda$, we recall the mapping Θ_λ of $\mathfrak{K}_\lambda$ onto $\mathfrak{W}_\lambda$ defined ([4], equation (6.8)) and referred to in the previous paragraph. We also recall the pairing $<,>$ of $\mathfrak{K}_\lambda$ with its dual space $\mathfrak{W}_\lambda$. By composition, we obtain a non-degenerate pairing

$$(\xi^*,\eta^*)\mapsto\langle\xi^*,\Theta\eta^*\rangle \tag{6.22}$$

of $\mathfrak{K}_\lambda$ with itself onto $K(\lambda)$. Let $\mathfrak{K}''_\lambda$ be the annihilator of $\mathfrak{K}'_\lambda$ under this pairing. It is clear that this subspace is defined over $K(\lambda)$ and that upon lifting the field of definition to $\mathfrak{R}'$ we obtain " stability " under α_λ^* as defined above. That $\mathfrak{K}''_\lambda$ is complementary to $\mathfrak{K}'_\lambda$ follows from work of Katz and Deligne. The latter has shown (extending results of [6]), that the space of invariant cycles have (under intersection pairing) an orthogonal complement in the space spanned by the vanishing cycles. Since the identification [8] of $\mathfrak{K}_\lambda$ with the space of middle dimensional primitive homology classes identifies $\mathfrak{K}'_\lambda$ with the space of invariant cycles, it is enough to show that the two pairings coincide. This coincidence has been proven by Katz (*On the Intersection Matrix of a Hypersurface*, to appear).

f) Stable roots.

We again let V be the space of rational solutions of (6.3). Since (6.8) is an automorphism of V, we may consider the corresponding (elementary) spectral theory.

If $\mathfrak{X}$ is an eigenvector of the mapping (6.8) then

$$\mathfrak{X}^{\varphi}A_\lambda=\varepsilon\mathfrak{X} \tag{6.23}$$

for some ε algebraic over K. Relation (6.23) can be specialized at each z not in the residue class of an element of S. In particular if $z^q = z$ then the specialized value of $\mathfrak{X}$ is an eigenvector of A_z with eigenvalue ε (independent of z). Thus ε/q is a root of the factor of the zeta function (of the reduction of the fiber $f(z, X) = 0$) corresponding to the middle dimensional cohomology. Such a root may be referred to as a *stable* root. Naturally if $z^{q^s} = z$ then the corresponding root of the zeta function of the reduced fiber (which is defined over $GF[q^s]$) is $(\varepsilon/q)^s$.

Washnitzer has proposed the far more difficult problem of showing that, conversely, each stable root corresponds to a rational solution of (6.3).

We remark that by means of Reich's trace formula [12] as applied to the endomorphism

$$\psi \circ A_\lambda$$

of $\mathfrak{R}^N$, it is possible to deduce a connection between the endomorphism (6.8) of V and the zeta function of the reduction of the ambient space

$$f(\lambda, X) \equiv 0$$

(λ now a space variable).

g) Bounded solutions.

For each residue class, $\bar{z}$, of $\mathfrak{O}$ mod $\mathfrak{P}$, let $V_{\bar{z}}$ be the space of all solutions of (6.3) bounded on annuli:

$$0 < \operatorname{ord}(\lambda - z) < b$$

for b sufficiently close to 0, z being a fixed lifting of $\bar{z}$ (say $\mathbf{Q}_p(z)$ unramified over $\mathbf{Q}_p$). (It should be understood that $\lambda - z$ is to be replaced by $1/\lambda$ if $\bar{z}$ is the infinite residue class.) If $\bar{z}$ is not the class of any element of S then neither is $\bar{z}^q$ and it is clear that (6.8) maps $V_{\bar{z}^q}$ into $V_{\bar{z}}$ since A_λ is bounded on $z + \mathfrak{P}$. This shows that the dimension of $V_{\bar{z}}$ in this case depends only on the orbit of $\bar{z}$ under the q-th power map and that furthermore $V_{\bar{z}^q}$ is mapped onto $V_{\bar{z}}$.

If $\bar{z}$ is in the class of an element of S then A_λ is bounded on an annulus of $\bar{z}$ of the type indicated and hence the stability assertions remain valid.

The elliptic case studied in § 4 below shows that this subspace need not be trivial and suggests the *conjecture*:

$V_{\bar{z}}$ is determined by the set of all solutions of a system of linear differential equations (in fewer unknowns than N) with coefficients which are analytic elements with support $\mathfrak{D}$ which contains the lifting of all but a finite set of residue classes of Ω.

In the case of curves it is natural (in view of the results of Manin [11]) to ask whether the dimension of $V_{\bar{z}}$ is the same as the stable rank of the Hasse-Witt matrix of the reduced fiber.

The conjecture also raises questions as to the existence of a preferred basis of $V_{\bar{z}}$ which is " defined on $\mathfrak{D}$ " and relative to which the mapping of (6.8) has a matrix whose coefficients are analytic with support $\mathfrak{D}$.

h) Stability of vanishing cycle.

In the case of a Lefschetz pencil of hypersurfaces of odd dimension, it is known that at a singular point (say $\lambda = 0$), equation (6.3) has $N-1$ linearly independent, locally holomorphic solutions $\mathfrak{X}^{(1)}, \ldots, \mathfrak{X}^{(N-1)}$, the vanishing cycle, say $\mathfrak{X}^{(1)}$, being characterized by the existence of a locally non-holomorphic solution of the form

$$\mathfrak{X}^{(1)} \log \lambda + \mathfrak{Y} \tag{6.24}$$

where $\mathfrak{Y}$ is locally holomorphic. Under the hypotheses of paragraph *c)*, the " vectors " $\mathfrak{X}^{(1)}, \ldots, \mathfrak{X}^{(N-1)}, \mathfrak{Y}$ are holomorphic in the open unit disk, and it is clear that this characterization of $\mathfrak{X}^{(1)}$ is preserved by the mapping (6.8). This shows the existence of a constant ε such that equation (6.23) holds with $\mathfrak{X}$ replaced by $\mathfrak{X}^{(1)}$. However there is no *a priori* reason to believe that this relation can be continued analytically beyond the open unit disk. In the following sections (§ 6, *i), j)*) we give two examples in which relations of this type can be continued (by projectivization).

Forther examples follow from § 3 and the Euler integral representation

$$F(a, b, c, \lambda) = \Gamma(c)(\Gamma(b)\Gamma(c-b))^{-1} \int_0^1 t^{b-1}(1-t)^{c-b-1}(1-t\lambda)^{-a}\, dt.$$

Indeed if $a+b=c$ (resp. $a=b$) then the vansihing cycle at $\lambda = 1$ (resp. $\lambda = \infty$) would be amenable to the theory of § 3.

In the case of a Lefschetz pencil of hypersurfaces of even dimension, the locally holomorphic solutions again form a subspace of codimension one and the vanishing cycle is characterized as the unique solution of the form $\Upsilon\sqrt{\lambda}$ where Υ is locally uniform. The stability (for $p \neq 2$) of the vanishing cycle under (6.8) is again clear.

i) Elliptic Curves.

In this section we apply the preceding theory to elliptic curves as defined by equation (4.1) with $p \neq 2$. A similar theory holds for

$$X^3 + Y^3 + Z^3 - 3\lambda XYZ = 0 \tag{6.25}$$

($p \neq 3$), which would be applicable to the case $p = 2$. The curves of equation (4.1) are not in general position, but by means of a suitable rotation this requirement could be met. We ignore this technical complication as the differential equations are not affected by the rotation.

We choose $\left(\frac{dX}{2Y}, \frac{\partial}{\partial\lambda}\left(\frac{dX}{2Y}\right)\right)$ as a basis for differentials of the second kind. By a well known computation the corresponding periods $\omega = (\omega_1, \omega_2)$ satisfy the differential equation

$$\frac{\partial\omega}{\partial\lambda} = \omega \begin{pmatrix} 0 & (4\lambda(1-\lambda))^{-1} \\ 1 & -(1-2\lambda)/((1-\lambda)\lambda) \end{pmatrix}. \tag{6.26}$$

Near $\lambda=0$ the vanishing cycle is

(6.27) $$\mathfrak{X}=(F, F')$$

where $F(\lambda)=\left(\frac{1}{2}, \frac{1}{2}, 1, \lambda\right)$, and a second solution is of the form $\mathfrak{Y}+\mathfrak{X}\log\lambda$, where $\mathfrak{Y}$ is holomorphic near zero and can be computed explicitly from equation (4.19). Thus in the terminology of paragraph *c)*,

$$G=N=\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}, \qquad \Upsilon=\begin{pmatrix}\mathfrak{Y}\\ \mathfrak{X}\end{pmatrix}.$$

The hypotheses of *c)* are easily verified for all $p\neq 2$.

In this paragraph and again in § 8, where extensive computations will appear, we drop the extraneous factor p which appears in the theory. From equation (6.14) we find $(p=q)$

$$A=\mathfrak{A}=\begin{pmatrix}p\varepsilon & b\\ 0 & \varepsilon\end{pmatrix},$$

$\varepsilon\neq 0$, and from equation (6.16), ($n+1$ replaced by $n-1=1$ since a factor p is removed from A) we find that $\varepsilon=\pm 1$. From this we conclude that

$$\mathfrak{X}^{\varphi}A_{\lambda}=\varepsilon\mathfrak{X}.$$

Write $\mathfrak{X}$ in the form $F.(1, \eta)$ where η is as defined in § 4. Using the notation of that section we now have

(6.28) $$(1, \eta)^{\varphi}A_{\lambda}=\varepsilon f(\lambda)(1, \eta).$$

This formula is valid for an annulus about the origin in $\mathfrak{P}$, but by the analyticity of η in the set $\mathfrak{D}$ of § 4, we conclude that if $z^{p^a}=z$ for some $a\in\mathbf{Z}$ and if $z\in\mathfrak{D}$ then the zeta function of the reduced curve has unit root equal to

(6.29) $$\pi(\bar{z})=\varepsilon^a f(z)f(z^p)\ldots f(z^{p^{a-1}}).$$

The value of ε may be determined by Manin's congruence,

$$\pi(\bar{z})\equiv(-1)^{\frac{p-1}{2}}g(z) \mod \mathfrak{P}$$

for $z^p=z$, g being defined by equation (4.3). Since $g(z)\equiv f(z) \bmod p$, it follows that

$$\varepsilon=(-1)^{(p-1)/2}.$$

We note the computation of the period of the differential of the first kind for the vanishing cycle reduces when $\lambda=0$ to the computation of the residue of $\frac{dX}{XY}$ at one of the two points above $x=0$ on the rational curve, $Y^2=X-1$. It is difficult to refrain from the observation that under the p-th power map these points are permuted if $p\equiv -1 \bmod 4$ and otherwise they are fixed.

Lemma (3.2) shows that the vanishing cycles at $\lambda=1$ and at $\lambda=\infty$ would give the same formula as (6.29). Indeed, aside from the determination of ε, we could have used (u_α, u'_α) for any $\alpha\in\mathfrak{D}$.

Finally we note that equation (6.29) shows that the root cannot be stable in the sense of paragraph *f)*. This follows most easily from the Manin congruence, the degree of g and the corollary to Theorem 5.

j) A surface of degree 4 $(p\neq 2, 3)$.

For our second example we consider the surface

$$\mathbf{(6.30)}\qquad X_1^4+X_2^4+X_3^4+X_4^4-4\lambda X_1X_2X_3X_4=0.$$

The middle Betti number is 22 but one root of the corresponding factor of the zeta function of the reduction $(p\neq 2, 3, \lambda^4\neq 1)$ is known to be the cardinality of the field of definition of the fiber. The differential equation (6.3) is in this case a system of 21 simultaneous equations. As basis of $\mathfrak{W}_\lambda$ we take $\{X^u\}$ where u runs over all elements of $\mathbf{Z}_+^4$ such that

$$u_1+u_2+u_3+u_4\equiv 0 \mod 4$$
$$0<u_i<4,\qquad 1\leq i\leq 4.$$

Using ([4], equation (5.17)), we find that (6.3) splits into 16 independent systems of linear differential equations. These 16 systems are of three distinct types which will now be described.

j_1) There are 12 systems consisting of a single first order equation in one unknown. In the notion of the reference (dropping πX_0 factors as superfluous),

$$\mathbf{(6.31)}\qquad (1-\lambda^4)(-4X_1X_2X_3X_4)X^u=2\lambda^3X^u+D_1A+D_2B+D_3C+D_4D$$

where $u=(1, 2, 2, 3)$,

$$A=(\lambda^2/4)X_2X_3X_4^2-\lambda^3X^u$$
$$B=-\lambda X_1^3X_3^4X_4$$
$$C=-\lambda^2X_1^4X_2X_3X_4^2$$
$$D=-X_1^2X_2^3X_3^3$$

and thus each period, ω, of the cohomology class corresponding (under the Katz identification) to X^u is a solution of

$$\mathbf{(6.32)}\qquad \frac{d\omega}{d\lambda}=\frac{2\lambda^3}{1-\lambda^4}\omega.$$

The same equation is valid for the periods of the classes corresponding to the remaining 11 distinct permutations of (1, 2, 2, 3). Thus the solution matrix splits into a direct sum of the form

$$(1-\lambda^4)^{-\frac{1}{2}}\,\Upsilon_1\oplus\Upsilon^{(1)}$$

where Υ_1 is a constant, non-singular, diagonal matrix of rank 12 and $\Upsilon^{(1)}$ is a 9×9 matrix.

j_2) By similar computations there are 3 independent systems each consisting of two simultaneous equations. A typical pair involves $u=(1, 1, 3, 3)$, $v=(3, 3, 1, 1)$ (the remaining two being obtained by permutation of variables). The corresponding differential equation is

$$(1-\lambda^4)\frac{\partial \mathfrak{X}}{\partial \lambda}=\mathfrak{X}\begin{pmatrix}\lambda^3 & \lambda\\ \lambda & \lambda^3\end{pmatrix} \tag{6.33}$$

and this system has two independent algebraic solutions

$$\begin{cases}(1+\lambda^2)^{-\frac{1}{2}}(1, -1)\\ (1-\lambda^2)^{-\frac{1}{2}}(1, 1).\end{cases} \tag{6.34}$$

There is a corresponding splitting of $\Upsilon^{(1)}$ into a direct sum of three 2×2 matrices of this type and a fourth matrix of rank 3.

j_3) The 3×3 matrix just referred to arises from the triplet

$$(1, 1, 1, 1), \quad (2, 2, 2, 2), \quad (3, 3, 3, 3).$$

The corresponding differential equation is

$$\frac{\partial \mathfrak{X}}{\partial \lambda}=\mathfrak{X}\begin{pmatrix}0 & 0 & \lambda/16(1-\lambda^4)\\ -4 & 0 & -7\lambda^2/4(1-\lambda^4)\\ 0 & -4 & 6\lambda^3/(1-\lambda^4)\end{pmatrix}. \tag{6.35}$$

There is a corresponding decomposition of A_λ deduced from the above decomposition of the solution matrix and an analysis of A_0 (which is relatively simple as equation (6.30) reduces to a diagonal form when $\lambda=0$). We have checked ([4], § 4) that for

$$u'\equiv pu \mod 4$$

we have

$$\alpha_0^*\xi_u^*=\varepsilon(u)\xi_{u'}^*. \tag{6.36}$$

In the next section (§ 6, k)) we will indicate a proof of the fact that

$$\begin{aligned}\varepsilon(u)&=\prod_{i=1}^{4} g_1\left(u_i\frac{p-1}{4}\right), \qquad p\equiv 1 \mod 4\\ \varepsilon(u)\varepsilon(u')&=\prod_{i=1}^{4} g_2\left(u_i\frac{p^2-1}{4}\right), \qquad p\equiv -1 \mod 4\end{aligned} \tag{6.37}$$

where for any pair of integers j, s, $(s>0)$, $g_s(j)$ is the Gauss sum (for the field $\mathrm{GF}[p^s]$)

$$g_s(j)=-\Sigma t^{-j}\theta_s(t) \tag{6.38}$$

the sum being over all t such that $t^{p^s-1}=1$ and θ_s being the function

$$\theta_s(t)=\exp(\pi t-\pi t^{p^s}). \tag{6.39}$$

Using the fact that the function,

$$h(\lambda)=\sqrt{(1-\lambda)/(1-\lambda^p)}$$

defined near zero by the condition $h(0)=+1$, has an analytic continuation and assumes values at $z^q=z$, $z\neq 1$ which are easily described in terms of Legendre symbols, one may, by use of the above information, obtain precise formulae for the 18 roots corresponding to the splitting described in $j_1)$ and $j_2)$ above. All of these roots are of the form $\pm q$ where q is the cardinality of the field of definition of the reduction of the fiber.

Of the three remaining roots (corresponding to equation (6.35)) one may be determined from the permutation $\omega\mapsto q^2/\omega$ of the 21 roots. The set of 18 roots ($j_1)$ and $j_2)$) are stable under the permutation and hence the set of the three remaining roots is also stable. This means that one of these is mapped into itself and hence must be $\pm q$. The sign may be determined when $\lambda=0$ by applying equations (6.36), (6.37) to $u=(2, 2, 2, 2)$ and the variation in sign (as λ varies) may be obtained from the Wronskian of (6.35) (cf. [4], § 9). The root is therefore

$$p^{-1}\left(g_1\left(\frac{p-1}{2}\right)\right)^4 h(\lambda^4)=ph(\lambda^4) \tag{6.40}$$

when the fiber is defined over GF[p] (it being understood that the formula be applied only to Teichmuller representatives for λ and extended to fibers not defined over GF[p] by the obvious modification).

If we put $\mathfrak{X}=(\mathfrak{X}_1, \mathfrak{X}_2, \mathfrak{X}_3)$ in equation (6.36), then, by an elementary computation, $\mathfrak{X}_1$ satisfies the differential equation $(t=\lambda^4)$

$$\left(4t^2(1-t)\left(\frac{d}{dt}\right)^3+(9t-15t^2)\left(\frac{d}{dt}\right)^2+\left(\frac{3}{2}-\frac{31}{4}t\right)\frac{d}{dt}-\frac{1}{16}\right)\mathfrak{X}_1=0. \tag{6.41}$$

This is the equation of the generalized hypergeometric function

$$\mathrm{F}\left(\begin{matrix}\frac{1}{4}, & \frac{1}{4}, & \frac{1}{4}, \\ & \frac{1}{2}, & \frac{3}{4}\end{matrix}\ t\right)$$

and at ∞ the differential equation in $\mathfrak{X}_1$ has the solution $\lambda^{-1}\mathrm{F}(1/\lambda^4)$ where

$$\mathrm{F}(t)=\mathrm{F}\left(\begin{matrix}\frac{1}{4}, & \frac{1}{2}, & \frac{3}{4}, \\ & 1, & 1\end{matrix}\ t\right) \tag{6.42}$$

and a full set of solutions are given by two additional ones, one involving $\log \lambda$ and the other $\log^2 \lambda$. The unique solution holomorphic at ∞ is thus the vanishing cycle,

$$\mathfrak{X} = (\mathfrak{X}_1, \mathfrak{X}_2, \mathfrak{X}_3)$$

with $\mathfrak{X}_1 = \lambda^{-1} F(1/\lambda^4)$ and by the methods of § 3, $\mathfrak{X}_2/\mathfrak{X}_1 = \rho_1$, $\mathfrak{X}_3/\mathfrak{X}_1 = \rho_2$ are holomorphic on the set $\mathfrak{D}$ defined by

$$|F_1(1/\lambda^4)| = 1, \quad |\lambda| \geq 1 \tag{6.43}$$

$F_1(t)$ being the sum of terms in $F(t)$ up to and including the term in t^{p-1}. This gives the formula

$$\omega = \varepsilon f(\lambda^4) \tag{6.44}$$

for the 20-th root, the last (21-st) being obtained from this one by the permutation $\omega \mapsto q^2/\omega$. Here f is used in the sense of § 3 as the extension to $\mathfrak{D}$ of $F(1/\lambda^4)/F(1/\lambda^{4p})$ and it is understood that the formula is valid if $\lambda = \lambda^p$, $\lambda \in \mathfrak{D}$, the case $\lambda^{p^s} = \lambda$ being given by the obvious generalization.

The constant ε cannot be obtained by specialization at $\lambda = 0$ (since $0 \notin \mathfrak{D}$) but by the method of paragraph *d)*, using the fact that the matrix G for the point at ∞ is

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

we find that $\varepsilon = \pm 1$. We know [4, § 7] that the non-trivial factor of the zeta function of the reduction of (6.30) has at most one unit root. This root must therefore be given by equation (6.44). The value of ε may now be determined as being $+1$ by means of Warning's method for obtaining a modulo p estimate for the number of rational points. Alternately we could have used the (mod p) structure sheaf cohomology [15, Theorem 5].

The vanishing cycle at z for $z^4 = 1$ is of the form

$$\sqrt{\lambda^4 - 1}\, \mathfrak{Y} \tag{6.45}$$

where $\mathfrak{Y}$ is locally uniform at z. If $z \in \mathfrak{D}$ (as is the case for example if $p = 11$) then the vanishing cycle at ∞ can be " extended " to the vicinity of z by means of a linear first order differential equation of the type

$$\mathfrak{X}_1' = \mathfrak{X}_1 \eta$$

(cf. equation (3.9)) where η is analytic on $\mathfrak{D}$. The vanishing cycle at z cannot satisfy this equation and hence (contrary to the case of elliptic curves) there is a possibility of comparing two distinct vanishing cycles p-adically. The one-dimensional space spanned by solution (6.45) is clearly stable under the mapping (6.8) and perhaps the root described by equation (6.40) may be obtained from this cycle. However the method of § 3 is not directly applicable to this solution and we do not know whether

or not $\mathfrak{Y}$ is bounded in $z+\mathfrak{P}$, nor do we know, for $\mathfrak{Y}=(\mathfrak{Y}_1, \mathfrak{Y}_2, \mathfrak{Y}_3)$, whether or not the ratios $\mathfrak{Y}_2/\mathfrak{Y}_1$, $\mathfrak{Y}_3/\mathfrak{Y}_1$ have analytic continuation beyond $z+\mathfrak{P}$.

Finally we note that none of the 21 roots analyzed here by means of the differential equation is stable in the sense of paragraph *f)*. This is checked directly for the 19 roots of the form $\pm q$, while for the root given by equation (6.44) (and hence for the product of q^2 with its reciprocal) we use the fact that $f(\lambda^4) \equiv F_1(1/\lambda^4) \bmod p$, and this cannot be a $(p-1)$-th power mod p since $F_1 \bmod p$ is by § 1 a polynomial of degree $\frac{p-1}{4}$ $\left(\text{resp. } \frac{p-3}{4}\right)$ if $p \equiv 1 \bmod 4$ (resp. $p \equiv -1 \bmod 4$). The assertion thus follows from the corollary to Theorem 5.

k) Gauss Sums (appendix).

The object of this appendix is to verify equation (6.37). The method gives similar results for any number of variables. It is well known that the indicatede igenvalues are roots of the zeta function. The purpose of this note is to show that the proper connection has been made between eigenvalue and eigenvector. By the methods of ([4], § 4, *c)*) the several variable case (diagonal forms) is reduced to an elementary type of L-series. In this way it is enough to show that in the terminology of ([4], § 4, *b)*), for $d|(q-1)$, $0<j<d$, $q=q^a$, we have

(6.46) $$\psi(\theta_a(X^d)X^j) \in \mu_j X^j + DL(b)$$

where $$D = X\frac{\partial}{\partial X} + d\pi X^d$$

$$\mu_j = g_a\left(j\frac{q-1}{d}\right).$$

We sketch the proof. For $m = j\frac{q-1}{d}$, let

(6.47) $$\alpha_j = \psi \circ (X^{-m}\theta_a(X)),$$

an endomorphism of $L(db)$. The differential operator $\left(E = X\frac{\partial}{\partial X}\right)$

(6.48) $$D_j = E + \pi X + \frac{j}{d}$$

is readily seen to satisfy the commutation condition

(6.49) $$\alpha_j \circ D_j = qD_j \circ \alpha_j.$$

Thus by the methods of [2], it is natural to consider the factor space $\mathfrak{W} = L(db)/D_jL(db)$, which is found to have dimension one, being spanned by $1 \bmod D_jL(db)$. Thus using φ in the sense of $h(t)^\varphi = h(gt)$, we find as in ([2], § 4) that

(6.50) $$\det(I - t\alpha_j)^{1-\varphi} = 1 - \lambda t,$$

where λ is the unique eigenvalue of the endomorphism of $\mathfrak{W}$ obtained from α_j by passage to quotients. On the other hand the simple p-adic trace formula [16] gives

$$(6.51) \qquad (q-1)\mathrm{Tr}\,\alpha_j = \sum_{t^{q-1}=1} \theta_a(t)t^{-m} = -g_a(m).$$

Hence we conclude

$$(6.52) \qquad \det(\mathrm{I}-t\alpha_j)^{1-\varphi} = \exp\left\{-\sum_{s=1}^{\infty}\frac{t^s}{s}g_{as}(m_s)\right\}$$

where

$$m_s = m(q^s-1)/(q-1).$$

Comparing this with (6.50), we have

$$(6.53) \qquad \lambda^s = g_{as}(m_s),$$

a well known formula of Hasse and Davenport. In particular

$$\lambda = g_a(m).$$

However, by definition,

$$(6.54) \qquad \alpha_j(1) \in \lambda + \mathrm{D}_j\mathrm{L}(db).$$

Equation (6.46) follows from this upon replacing X by X^d.

§ 7. Deligne's Theorem.

a) Introduction.

The object of the next two sections is to show a close connection between the local solutions of equation (4.2), in particular the eigenvectors of appropriate powers of the mapping of equation (6.8), and the modular equation of degree p ([14], p. 237). In particular the theory of § 4 will be extended to the case of supersingular reduction.

The main impetus for this extension has been the recent results of P. Deligne concerning the existence of a " globally holomorphic " solution of the modular equation. I am indebted to N. Katz for much of the exposition and in particular for the method of proof of Lemma (7.1).

We recall that in terms of the elliptic modular function $j(\tau)$ the modular equation $\mathrm{F}_p(\mathrm{X}, \mathrm{Y})$ is defined to be the polynomial of minimal degree representing the curve (defined over $\mathbf{C}$) whose generic point is $(j(p\tau), j(\tau))$. It is known that

$$\mathrm{F}_p(\mathrm{X}, j(\tau)) = (\mathrm{X}-j(p\tau))\prod_{a=0}^{p-1}\left(\mathrm{X}-j\left(\frac{\tau+a}{p}\right)\right),$$

that $\mathrm{F}_p(\mathrm{X}, \mathrm{Y}) \in \mathbf{Z}[\mathrm{X}, \mathrm{Y}]$ and is symmetric in X and Y and that

$$(7.1) \qquad \mathrm{F}_p(\mathrm{X}, \mathrm{Y}) = (\mathrm{Y}^p-\mathrm{X})(\mathrm{Y}-\mathrm{X}^p)+p\sum_{\mu=0}^{p}\sum_{\nu=0}^{p}a_{\mu,\nu}\mathrm{X}^\mu\mathrm{Y}^\nu,$$

where $a_{p,p}=0$ and each $a_{\mu,\nu} \in \mathbf{Z}$.

Classically with $q=e^{\pi i\tau}$, $\operatorname{Im}\tau>0$, we have

$$j=q^{-2}\sum_{s=0}^{\infty}a_s q^{2s}\in\mathbf{Z}[[q^2]], \tag{7.2}$$

$a_0=1$, $a_1=744$, $a_2=196\,884$, while for $j'=j(p\tau)$,

$$j'=q^{-2p}\sum_{s=0}^{\infty}a_s q^{2ps}. \tag{7.3}$$

From this we may deduce that for $|j|>1$,

$$j'=j^p+pk(j)+p\sum_{n=1}^{\infty}B_n/j^n, \tag{7.4}$$

where each $B_n\in\mathbf{Z}$ and where k is a polynomial of degree $p-1$ (its leading term is $-744j^{p-1}$) with coefficients in $\mathbf{Z}$. Thus equation (7.4) gives a solution of the equation

$$F_p(X,j)=0 \tag{7.5}$$

which is holomorphic in the punctured disk, $1<|j|<\infty$. This implies an identity in $\mathbf{Z}((j^{-1}))$ from which we may deduce that (7.4) is a p-adically holomorphic solution of (7.5) for $|j|>1$ (with pole of order p at infinity) and that this is the only solution with this property since the remaining classical solutions are given by

$$j_\nu=q^{2/p}\zeta^\nu\sum_s a_s(q^{2/p}\zeta^\nu)^s,\qquad \nu=0,1,\ldots,p-1$$

where ζ is a primitive p-th root of unity and these are also p-adically solutions of (7.5) which are algebraic and not rational over the field of functions meromorphic in the disk, $|j|>1$.

It was conjectured by Tate, proven by him for $p=2$ and proven generally by Deligne that the solution (7.4) can be extended p-adically to a uniform analytic function on the set

$$\mathfrak{D}_3=\{j\mid \operatorname{ord}(j-\beta_i)<\frac{p}{p+1},\quad i=1,2,\ldots,r\}$$

where $\{\beta_1,\ldots,\beta_r\}$ is a set of representatives in an unramified field of the j-invariants in characteristic p of supersingular elliptic curves. If we use χ to denote this extended mapping, then the p-adic Mittag-Leffler theorem gives

$$\chi(j)=h_\infty(j)+\sum_{i=1}^{r}h_i(j), \tag{7.6}$$

where $h_\infty=j^p+pk$, the principal part at infinity described previously, and for $i=1,2,\ldots,r$,

$$h_i(j)=\sum_{n=1}^{\infty}A_n^{(i)}/(j-\beta_i)^n, \tag{7.7}$$

the principal part of χ at β_i. Furthermore, Deligne showed that for $n \geq 1$, $i = 1, 2, \ldots, r$,

$$\text{(7.8)} \qquad \begin{aligned} \operatorname{ord} A_n^{(i)} &\geq \frac{1}{p+1} + n\frac{p}{p+1} \\ \operatorname{ord} A_1^{(i)} &\geq 1 + \delta_0 \end{aligned}$$

with $\delta_0 = 0$ and that for $\beta = 0$ (resp. 1 728) the symbol n in equation (7.8) may be replaced by $3n$ (resp. $2n$).

We shall give a proof of this result (valid for $p \neq 2$) which is based on Theorem 4 (§ 4) and shall show that it is impossible for equation (7.8) to be valid with $\delta_0 > 0$ if $p > 3$ (except for the exceptional $\beta = 0$, $\beta = 1\,728$ which do not appear exceptional if the results are stated in terms of the modulus λ).

b) Modular equation for λ.

We shall in this section explicitly use the modular equation for j but it will be useful (since § 4 is based on the modulus λ) to recall the corresponding modular equation for λ. There are two methods of proceeding:

(i) Let $\Gamma = \mathrm{SL}(2, \mathbf{Z})/(\pm I)$ and let Γ_2 be the principal congruence subgroup of Stufe 2. Then $\mathbf{Q}(\lambda(p\tau), \lambda(\tau))$ is the fixed field under $\Gamma_2 \cap \beta\Gamma_2\beta^{-1}$ while $\mathbf{Q}(j(p\tau), \lambda(\tau))$ is the fixed field under $\Gamma_2 \cap \beta\Gamma\beta^{-1}$ where

$$\beta = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}.$$

From this the equality of the two fields may be deduced. Thus if for $|q| < 1$ we put $\lambda' = \lambda(p\tau)$, $j' = j(p\tau)$ then λ' is a rational function of j' and λ while conversely j' is a rational function of λ'. Thus the extension of the mapping $\lambda \mapsto \lambda'$ implies the extension of the function $j \mapsto j'$ and conversely.

(ii) The modular equation relating λ and λ' may be constructed *ab initio* by well-known methods [14]. Similar modular equations are described in detail (e.g. $\sqrt[4]{\lambda(\tau)}/q^{1/8}$ is treated in [21], p. 496). We discuss the modular equation for λ briefly.

By standard methods, we compute the disjoint union

$$\Gamma_2\beta\Gamma_2 = \bigcup_{a=0}^{p} \Gamma_2\beta\Delta_a$$

where

$$\Delta_a = \begin{pmatrix} 1 & 2a \\ 0 & 1 \end{pmatrix} \quad \text{if } 0 \leq a \leq p-1$$

$$\Delta_a = \begin{pmatrix} p & 2\varepsilon \\ \dfrac{p-\varepsilon}{2} & \varepsilon \end{pmatrix} \quad \text{if } a = p, \quad (\varepsilon = (-1)^{(p-1)/2})$$

and therefore $\left\{\lambda\left(\dfrac{\tau+2a}{p}\right)\right\}_{a=0}^{p-1}$ together with $\lambda(p\tau)$ form a full set of conjugates over $\mathbf{C}(\lambda(\tau))$. Since each conjugate vanishes as $\lambda(\tau) \to 0$ (i.e. $\tau \to i\infty$) and since λ may

assume all values other than 0, 1 for $\operatorname{Im}\tau>0$, we conclude that the modular equation $G_p(X, \lambda)$ (satisfied by $\lambda(p\tau)$) is of degree $p+1$ in X, rational in λ with pole only at $\lambda=1$. With the aid of the transformations ([14], p. 148)

$$\lambda(-1/\tau)=1-\lambda(\tau)$$
$$\lambda(\tau+1)=-\lambda/(1-\lambda)$$
$$\lambda(-\tau/(\tau-1))=1/\lambda$$

it is not difficult to establish that $G_p\in\mathbf{C}[X, Y]$ with symmetry properties

(7.9) $$G_p(X, Y)=G_p(Y, X)=G_p(1-X, 1-Y)=(XY)^{p+1}G_p(X^{-1}, Y^{-1}).$$

Furthermore with the aid of equation (4.22), we obtain

(7.10) $$G_p(X, Y)=(X^p-Y)(X-Y^p)+p\sum_{\mu=1}^{p}\sum_{\nu=1}^{p}c_{\mu\nu}X^\mu Y^\nu,$$

where each $c_{\mu,\nu}$ lies in the ring of rational numbers which are integral at all odd primes and explicitly

$$c_{11}=(1-16^{p-1})/p$$
$$c_{21}=16^{p-1}/2$$

It will be apparent that the methods applied below to F_p work equally well for G_p.

c) Proof of Deligne's Theorem.

We first restrict our attention to the region

$$\mathfrak{D}_e=\left\{j\,|\,\operatorname{ord}(j^{p^2}-j)\leq\frac{p}{p+1}-e\right\}$$

where e is strictly positive, but small (say $e<p^{-1}(p+1)^{-1}$). Let

$$\mathfrak{D}_4=\left\{j\,|\,\operatorname{ord}(j^{p^2}-j)<\frac{p}{p+1}\right\}.$$

Lemma **(7.1)**. — *χ is a uniform analytic function of support $\mathfrak{D}_4$.*

Proof. — We define $\xi(j)=p^{-1}F_p(j, j^p)\in\mathbf{Z}[j]$. Equation (7.1) may be written

$$F_p(j, j^p+t)=t^{p+1}+tz+p\xi+pth(j, t)$$

where $z=j^{p^2}-j$, $h\in\mathbf{Z}[j, t]$. If we now let $t=p\xi T/z$ then a solution of the modular equation will certainly be given by j^p+t if T is a zero of the polynomial

(7.11) $$H(T)=1+T+T^{p+1}(p\xi)^p/z^{p+1}+p(T/z)h(j, p T\xi/z).$$

Let R_e be the ring of rational functions of j whose restrictions to $\mathfrak{D}_e$ have sup norms strictly less than unity. We assert

(7.12) $$H(T)-(1+T)\in R_e[T].$$

To verify this we partition $\mathfrak{D}_e$ into two sets which are discussed seperately.

Case 1. — $j\in\mathfrak{D}_e\cap\mathfrak{O}$.

In this case ξ lies in $\mathfrak{O}$ and uniform estimates are obtained from equation (7.11) using the inequality

$$(p+1)e\leq \mathrm{Min}(\mathrm{ord}((p\xi)^p/z^{p+1}),\ \mathrm{ord}(p/z)), \tag{7.13}$$

which is a consequence of the definition of $\mathfrak{D}_e$ and the upper bound for e.

Case 2. — $j\notin\mathfrak{O}$.

We assert that in this case the coefficients of the left side of equation (7.12) are bounded from above by $|p/j|$. To prove this we use equation (7.1) to compute H explicitly and reduce the assertion to the verification that for $j\in\mathfrak{O}$, $1\leq s<p$, we may conclude that $(p\xi)^p/z^{p+1}$, $(p/z)j^{ps}(p\xi/z)^{p-s}$, $(p/z)a_{\mu,\nu}\binom{\nu}{s}j^{\mu+p(\nu-s)}(p\xi/z)^{s-1}$ all lie in $(p/j)\mathfrak{O}$. This is verified by noting

$$\deg\xi\leq p^2+p-1$$

and hence for $j\notin\mathfrak{O}$

$$\begin{cases}\mathrm{ord}\,\xi\geq(p^2+p-1)\mathrm{ord}\,j\\ \mathrm{ord}\,z=p^2\,\mathrm{ord}\,j\end{cases} \tag{7.14}$$

and using the fact that $(\mu,\nu)\neq(p,p)$, μ and ν not greater than p. This completes the proof of (7.12).

Clearly $T=-1$ is an approximate root of H and Newton's recursive procedure may be used to find a precise root which is a limit of rational functions converging uniformly in $\mathfrak{D}_e$. This solution is meromorphic for j in the complement of $\mathfrak{O}$ and hence (by the uniqueness of the meromorphic solution at infinity) must coincide with (7.4) in this region. The solution may trivially be prolonged to a uniform analytic function of support $\mathfrak{D}_4$. This completes the proof of the lemma.

Before examining the growth conditions we first extend the lemma to regions of the form $j_0+\mathfrak{P}$ where $j_0^{p^2}=j_0$ but $j_0 \bmod \mathfrak{P}$ is not the j invariant of a supersingular elliptic curve. We now assume that $p\neq 2$ and using either of the two procedures outlined before, translate the above lemma into a corresponding statement concerning the mapping $\lambda\mapsto\lambda'$ (which we again denote by χ). It is clear that if $\lambda=\alpha$ is a modulus corresponding to a j_0 for which $j_0^{p^2}=j_0$, then χ is certainly holomorphic on an annulus

$$1-e<|\lambda-\alpha|<1. \tag{7.15}$$

We may assume that $|\alpha|\leq 1$, α fixed under a power of the p-th power map. In the following statement g refers to equation (4.3).

Lemma (7.2). — *χ is holomorphic on $\alpha+\mathfrak{P}$ if $|g(\alpha)|=1$.*

Proof. — The classical relation for λ' in terms of $q=e^{\pi i\tau}$, gives (in the notation of equation (4.20))

$$(\lambda/16)^p\exp(-pW(\lambda))=(\lambda'/16)\exp(-W(\lambda')) \tag{7.16}$$

and p-adically this clearly gives the unique solution of

$$G_p(\chi, \lambda)=0$$

which is holomorphic for $|\lambda|<1$. From equation (4.23), by differentiation,

$$p^{-1}\frac{d\lambda'}{d\lambda}=\frac{\lambda'(1-\lambda')}{\lambda(1-\lambda)}\left(\frac{F(\lambda')}{F(\lambda)}\right)^2. \tag{7.17}$$

This relation may be extended by a method of § 4 to the annulus (7.15) on which χ is defined, since

$$F(\lambda')/F(\lambda)=f(\lambda)^{-1}\sum_{s=0}^{\infty}\eta_s(\lambda^p)(\lambda'-\lambda^p)^s/s!$$

which is holomorphic in (7.15) if $\operatorname{ord}(\lambda'-\lambda^p)>(p-1)^{-1}$, which, by the proof of Lemma (7.1) is certainly true if e is small enough. (We are assuming here that $g(\alpha)$ is a unit.) It follows from Lemma (3.2) that the right side coincides on the annulus with $u_{\alpha^p}(\lambda')/(u_\alpha(\lambda)f(\alpha))$. Since the annulus lies in the support of χ, we deduce that

$$\frac{d\lambda'}{d\lambda}=p\frac{\lambda'(1-\lambda')(u_{\alpha^p}(\lambda')F_0(\alpha)^\tau)^2}{\lambda(1-\lambda)(u_\alpha(\lambda)F_0(\alpha))^2}, \tag{7.18}$$

(τ now referring to the Frobenius automorphism). Let us again define w_α on $\alpha+\mathfrak{P}$ by means of equation (4.26) and define W_α on $\alpha^p+\mathfrak{P}$ by

$$\begin{aligned} W_\alpha(\alpha^p)&=0\\ W'_\alpha\lambda(1-\lambda)(F_0(\alpha)^\tau u_{\alpha^p}(\lambda))^2&=1. \end{aligned} \tag{7.19}$$

Equation (7.18) shows that there exists a constant c such that

$$W_\alpha(\lambda')=c+pw_\alpha(\lambda) \tag{7.20}$$

for all λ in the annulus. Put q_α (resp. Q_α) equal to $\exp(w_\alpha(\lambda))$ (resp. $\exp W_\alpha(\lambda)$) for $\lambda\in\alpha+\mathfrak{P}$ (resp. $\lambda\in\alpha^p+\mathfrak{P}$). Since $(F_0(\alpha)^\tau)^{1-\tau}=f(\alpha^p)$, Theorem 4 shows that Q_α is a biholomorphic map of $\alpha^p+\mathfrak{P}$ onto $1+\mathfrak{P}$. Equation (7.20) shows that $Q_\alpha(\lambda')/q_\alpha(\lambda)^p$ is constant for λ in the annulus. Thus there exists $\gamma\in 1+\mathfrak{P}$ such that

$$Q_\alpha(\lambda')=\gamma q_\alpha(\lambda)^p$$

everywhere in the annulus, but using Q_α^{-1} to represent the inverse (in sense of composition) of Q_α, we have

$$\lambda'=Q_\alpha^{-1}(\gamma q_\alpha(\lambda)^p). \tag{7.21}$$

This formula valid in the annulus (7.15) gives an explicit continuation of χ to the disk $\alpha+\mathfrak{P}$. This completes the proof of the lemma.

d) Canonical lifting and p-adic q theory.

It may be verified by means of equation (7.8) that if $g(\alpha)$ is a unit, then $\chi(\lambda) \equiv \lambda^p \bmod p$ for all $\lambda \in \alpha + \mathfrak{P}$ and thus the canonical lifting [1] α_{can} of $\alpha \bmod \mathfrak{P}$ defined by means of the ν-th iterate of χ,

$$\chi^{(\nu)}(\alpha_{\text{can}}) = \alpha_{\text{can}}$$

where $\alpha^{p^\nu} = \alpha$, has the property $\operatorname{ord}(\alpha_{\text{can}} - \alpha) \geq 1$. Thus with w_α defined by equation (4.26), $\operatorname{ord} w_\alpha(\alpha_{\text{can}}) \geq 1$ and therefore $\exp w_\alpha(\alpha_{\text{can}})$ is well defined. Thus we may define

$$\tilde{q}_\alpha(\lambda) = \exp(w_\alpha(\lambda) - w_\alpha(\alpha_{\text{can}}))$$

for all λ in $\alpha + \mathfrak{P}$. Similarly $\tilde{Q}_\alpha$ may be defined by translating Q_α by $Q_\alpha((\alpha^p)_{\text{can}})$ so that equation (7.21) assumes the more natural form

$$\tilde{Q}_\alpha(\lambda') = \tilde{q}_\alpha(\lambda)^p, \tag{7.22}$$

an obvious generalization of equation (7.16). We further observe that if $\alpha^{p^\nu} = \alpha$ as above, then letting $\mu = (F_0(\alpha)^{\tau^\nu - 1})^2$ (which by equation (6.29) is the reciprocal of the square of the unit root of the zeta function of the reduced elliptic curve defined over $GF[p^\nu]$) we have

$$\begin{aligned} \tilde{q}_\alpha(\chi^{(\nu)}(\lambda)) &= \tilde{q}_\alpha(\lambda)^{\mu p^\nu} \\ \tilde{q}_\alpha(\alpha_{\text{can}}) &= 1. \end{aligned} \tag{7.23}$$

We shall show that these properties together with the fact that $\tilde{q}_\alpha$ is a one to one biholomorphic map of $\alpha + \mathfrak{P}$ onto $1 + \mathfrak{P}$ uniquely characterize q_α up to an exponent which is a unit in $\mathbf{Q}_p$.

John Tate and J.-P. Serre have kindly informed me of an unpublished theory of liftings of homomorphisms between nonsupersingular elliptic curves (generalizing [19], p. IV-34) which is based on an intrinsic definition of q for liftings of such curves. It seems quite likely that their definition coincides with ours and that the unique characterization property mentioned above gives the method of proof of coincidence. An alternate (and perhaps simpler) characterization of $\tilde{q}_\alpha$ is given in a note following Lemma (8.2) below.

To prove the uniqueness property, let K_T again be the maximal unramified extension of $\mathbf{Q}_p$, then translating α_{can} to the point 1, the question may be reduced to the following lemma.

Lemma **(7.3).** — *Let* H_1, H_2, h *be biholomorphic maps of* $1 + \mathfrak{P}$ *onto itself which are defined over* K_T *and which have the property that for some rational p-adic integer* m $(m \neq 1)$,

$$\begin{aligned} h(1) &= H_i(1) = 1 \\ H_i(h(x)) &= H_i(x)^m \end{aligned}$$

---

[1] J. Lubin, J.-P. Serre and J. Tate, Elliptic curves and formal groups, *Woods Hole Summer Institute*, 1964 (mimeographed notes), and J.-P. Serre, Groupes p-divisibles (d'après J. Tate), *Séminaire Bourbaki*, n° 318 (1966-1967).

for $i=1, 2$, *and all* x *in* $1+\mathfrak{P}$. *Then there exists a unit* b *in* $\mathbf{Q}_p$ *such that*

$$H_1(x)=H_2(x)^b$$

everywhere in $1+\mathfrak{P}$.

Proof. — Let $t=H_2(x)$ so that $H_1(x)=H_1(H_2^{-1}(t))$. We write

$$\xi(t)=H_1(H_2^{-1}(t)),$$

and since $t^m=H_2(x)^m=H_2(h(x))$, we have $h(x)=H_2^{-1}(t^m)$ and therefore

$$\xi(t)^m=H_1(x)^m=H_1(h(x))=H_1(H_2^{-1}(t^m)).$$

Thus

$$\xi(t)^m=\xi(t^m),$$

for all t in $1+\mathfrak{P}$. To simplify still further, we suppose t close to 1, make the change in variable $t=\exp z$, put $\eta(z)=\log \xi(\exp z)$ and deduce

$$m\eta(z)=\eta(mz)$$

for z close to zero. Since all these functions are defined over K_T, we conclude that $\eta(z)=bz$, for some b in K_T. We thus find that for x close to 1,

$$H_1(x)=\exp(b \log H_2(x)).$$

Using the fact that $t=H_2(x)$ is a holomorphic change of variable in $1+\mathfrak{P}$ and that H_1 is a holomorphic map of $1+\mathfrak{P}$ onto itself, we see that the formal power series $(1+Y)^b \in \mathfrak{O}[[Y]]$. Since $b \in K_T$, the criterion [1] shows that

$$bp \log(1+Y) \equiv b^\tau \log(1+Y^p) \mod p\mathfrak{O}[[Y]].$$

By checking the coefficient of Y^{p^s}, we find that $b \equiv b^\tau \bmod p^s$ and hence $b^\tau=b$. By checking the coefficient of Y, we find that $b \in \mathfrak{O}$. Thus b must be an integer in $\mathbf{Q}_p$. To show that b is a unit, we use the above argument and the fact that

$$H_2(x)=\exp(b^{-1} \log H_1(x)).$$

This completes the proof of the lemma.

e) Equation (7.8).

We now examine equation (7.8). The more precise statements for $j=0, j=1\,728$ could be obtained by doing the analysis in terms of the modulus λ, taking into account that $j_0=0$ corresponds to $\lambda_0=-\zeta_3, -\zeta_3^{-1}$ where ζ_3 is a primitive 3-rd root of unity and that locally $j \sim (\lambda-\lambda_0)^3$ for λ near λ_0, while $j_0=1\,728$ corresponds to $\lambda_0=\frac{1}{2}, 2, -1$ and $j-1\,728 \sim (\lambda-\lambda_0)^2$ for λ near λ_0.

While certain simplifications would ensue from the use of the modulus λ, we shall continue our discussion in terms of j.

For $|j|>1$, equation (7.12) implies that

$$T=\sum_{s=0}^{\infty} b_s/j^s$$

and $$\operatorname{ord}(b_0+1)\geq -\operatorname{ord} j$$

for all $|j|>1$. Thus $b_0=-1$ and similarly $\operatorname{ord} b_s\geq 1$ for $s\geq 1$. Thus

$$\chi(j)-j^p\in\frac{-p\xi(j)}{j^{p^2}-j}\left(1+\frac{p}{j}\mathfrak{D}\left[\frac{1}{j}\right]\right). \tag{7.24}$$

Lemma (7.4). — *Equation* (7.8) *is valid* (*with* $\delta_0=0$).

Proof. — Lemma (7.2) shows that χ has non-trivial principal parts only at infinity and at liftings of supersingular j-values. It follows from Lemma (7.1) that for $j_0^{p^2}=j_0$, the principal part at j_0 converges for $\operatorname{ord}(j-j_0)<\frac{p}{p+1}$. Furthermore equation (7.12) shows that $\operatorname{ord} T(j)=0$ everywhere in $\mathfrak{D}_4$ and hence in $\mathfrak{D}_4$ we have

$$\operatorname{ord}(\chi(j)-j^p)=\operatorname{ord}\frac{p\xi}{z}. \tag{7.25}$$

In particular then for $0<\operatorname{ord}(j-j_0)<p/(p+1)$, we have

$$\operatorname{ord}(\chi(j)-j^p)\geq 1-\operatorname{ord}(j-j_0)$$

and each term in the Laurent series in $(j-j_0)$ which represents $\chi(j)-j^p$ in this annulus has this bound. Specifically for the principal part, given by equation (7.7) (replacing j_0 by β_i), we have

$$\operatorname{ord} A_n^{(i)}-n\operatorname{ord}(j-\beta_i)\geq 1-\operatorname{ord}(j-\beta_i)$$

and the assertion of the lemma follows by letting $\operatorname{ord}(j-\beta_i)$ approach $p/(p+1)$ from below.

It is well known that supersingular j invariants (in characteristic p) lie in $GF[p^2]$. Thus we may, with no loss in generality, assume for $i=1, 2, \ldots, r$, $\beta_i^{p^2}=\beta_i$.

We now examine the possibility that equation (7.8) holds with $\delta_0>0$ (say) for $i=1$. In the following, ξ is the polynomial defined in the proof of Lemma (7.1).

Lemma (7.5). — *If* $\operatorname{ord} A_1^{(1)}>1$ *then* $\xi(\beta_1)\equiv 0 \bmod p$.

Note. — It follows from the proof that if $\beta^{p^2}=\beta$, but β not a lifting of a supersingular j invariant, then $\xi(\beta)\equiv 0 \bmod p$.

Proof. — We restrict our attention to the annulus

$$0<\operatorname{ord}(j-\beta_1)<p/(p+1).$$

Suppose the assertion false. Since ξ has coefficients in $\mathbf{Z}$ this implies that $\operatorname{ord}\xi(\beta_1)=0$ and hence ξ assumes unit values in the annulus. Thus by equation (7.25),

$$\operatorname{ord}(\chi(j)-j^p)=1-\operatorname{ord}(j-\beta_1).$$

Equation (7.8) shows that for $i=2, 3, \ldots, r$, we have $\operatorname{ord} h_i(j)\geq 1$ and thus

$$\operatorname{ord}(\chi(j)-j^p-h_1(j))\geq 1.$$

This shows that

$$\operatorname{ord} h_1(j)=1-\operatorname{ord}(j-\beta_1) \tag{7.26}$$

everywhere in the annulus. The contradiction is now easily obtained from consideration of the Newton polygon of h_1. Explicitly, choose $\delta\in(0, p/(p+1))$ such that

$$\operatorname{ord} A_n^{(1)}\geq 1+\delta.$$

For $\operatorname{ord}(j-\beta_1)=\dfrac{p}{p+1}-\delta$, we check that

$$\operatorname{ord}(A_n^{(1)}/(j-\beta_1)^n)\geq(1-\operatorname{ord}(j-\beta_1))+\delta$$

for $n\geq 1$; the computation for $n=1$ is immediate, and for $n\geq 2$ the assertion follows from equation (7.8) (with $\delta_0=0$). This estimate contradicts equation (7.26) and this completes the proof of the lemma.

We now prove a strong converse to the preceding lemma.

Lemma **(7.6)**. — *If* $\xi(\beta_1)\equiv 0 \bmod \mathfrak{P}$ *(and hence* $\bmod p$*) then there exists* β_1' *congruent to* $\beta_1 \bmod p$ *such that* χ *is holomorphic for*

$$0<\operatorname{ord}(j-\beta_1')<\frac{3}{2}$$

and if we replace β_1 *by* β_1' *in equation* (7.7), *then for* $i=1$, *equation* (7.8) *may be replaced by*

$$\operatorname{ord} A_n^{(1)}\geq\frac{1}{2}+\frac{3}{2}n.$$

Proof. — (The following proof does not apply to the case $p=2$. More precise statements will be given shortly for $p=2, 3$.)

We rewrite the initial step of the proof of Lemma (7.1) in the form

$$F_p(j, j^p+t)=t^{p+1}+tz_0+p\xi+pt^2h_0(j, t) \tag{7.27}$$

where

$$z_0=j^{p^2}-j+p\sum_{\mu=0}^{p}\sum_{\nu=0}^{p}\nu a_{\mu\nu}j^{\mu+p(\nu-1)}=\left(\frac{\partial}{\partial Y}F_p\right)(j, j^p)$$

and h_0 is again an element of $\mathbf{Z}[j, t]$. Clearly the p^2 zeros of z_0 lie in distinct residue classes and are unramified over $\mathbf{Q}_p$. We define β' to be the zero of z_0 which is congruent to $\beta_1 \bmod p$. Repeating the argument of Lemma (7.1), set $t=p(\xi/z_0)T$ and now consider the polynomial

$$H_0(T)=1+T+T^{p+1}(p\xi)^p/z_0^{p+1}+(p/z_0)(p\xi/z_0)T^2h_0(j, pT\xi/z_0). \tag{7.28}$$

We again estimate $H_0(-1)$ and $H_0'(-1)-1$, but now we need only consider j in a neighborhood of β_1, $\beta_1+\mathfrak{P}$.

Let $\mathfrak{S}$ be the ring of rational functions u (of j) such that for j in the annulus

$$\text{(7.29)} \qquad 0<\operatorname{ord}(j-\beta')<3/2,$$

we have

$$\operatorname{ord} u(j)\geq \operatorname{Min}(2-\operatorname{ord}(j-\beta'),\ 3-2\operatorname{ord}(j-\beta')).$$

We assert

$$\text{(7.30)} \qquad H_0(T)-(1+T)\in\mathfrak{S}[T].$$

Since β' is unramified over $\mathbf{Q}_p$ and $\xi(\beta')\in\mathfrak{P}$, we have $\operatorname{ord}\xi(\beta')\geq 1$. Since

$$\xi(j)\in\xi(\beta')+(j-\beta')\mathfrak{O}[j-\beta'],$$

we have

$$\text{(7.31 } a\text{)} \qquad \operatorname{ord}\xi(j)\geq\operatorname{Min}(1,\operatorname{ord}(j-\beta')),$$

while for $j\in\beta'+\mathfrak{P}$ we have

$$\text{(7.31 } b\text{)} \qquad \operatorname{ord} z_0(j)=\operatorname{ord}(j-\beta').$$

For j in the annulus (7.29) we conclude that $p\xi/z_0$ lies in $\mathfrak{O}$ and equation (7.30) follows from (7.28) and (7.31). The approximate solution $T=-1$ of H_0 may thus be made precise by the Newton method if $0<\operatorname{ord}(j-\beta')<3/2$. We conclude that for j in the annulus

$$\operatorname{ord}(\chi(j)-j^p)=\operatorname{ord} p\xi/z_0\geq\operatorname{Min}(1,\ 2-\operatorname{ord}(j-\beta')).$$

The lemma follows immediately.

By substituting (7.2) and (7.3) in (7.1) and examining the coefficients of $1/q^{p^2+p-1}$ and $1/q^{p^2+p-2}$ it is found that

$$a_{p,p-1}=8.3.31$$

and that for $p\neq 2$,

$$a_{p,p-2}=4.3^3.1\,823-(p-1)(744)^2/2.$$

This shows that neither

$$F_p(x,y)\equiv(x^p-y)(x-y^p)\mod p^2$$

nor

$$F_p(x,x^p)\equiv 0\mod p^2$$

can hold unless $p=2, 3$. However explicit formulae for F_2, F_3 are available [21] and these show that both congruences are valid for $p=2, 3$. Thus for these two primes, the hypothesis of the previous lemma are certainly satisfied. In these two cases the only supersingular invariants are at $j_0=0$. An examination of the explicit formulae shows that the unique root β' of z_0 in $\mathfrak{P}$ satisfies

$$\operatorname{ord}\beta'=\begin{cases}8 & p=2\\ 3 & p=3\end{cases}$$

and that for $\operatorname{ord} j>0$

$$\operatorname{ord} p\xi \geq \begin{cases} \operatorname{Min}(12,\ 4+2\operatorname{ord} j) & p=2 \\ \operatorname{Min}(3+\operatorname{ord} j,\ 2+3\operatorname{ord} j) & p=3. \end{cases}$$

The method of the preceding lemma now shows that the support of χ is

$$\operatorname{ord}(j-\beta') < \begin{cases} 13/2 & \text{if } p=2 \\ 7/2 & \text{if } p=3 \end{cases}$$

and that for the principal part at β', equation (7.8) takes the form (for $n\geq 1$)

$$\operatorname{ord} A_n \geq \begin{cases} \frac{11}{2}+\frac{13}{2}n & p=2 \\ \frac{5}{2}+\frac{7}{2}n & p=3. \end{cases}$$

§ 8. Cycles of Elliptic Curves (Part II).

a) *Application of Deligne's Theorem.*

We are now in a position to extend the results of § 4 to the region of validity of Deligne's theorem and in particular to obtain considerable information concerning the local solutions of (4.2).

The main idea of this section is to view $\chi : \lambda \mapsto \lambda'$ as a lifting to characteristic zero of the Frobenius and to define a mapping similar to equation (6.8) but using χ instead of the p-th power map. Our first object is to find the relation between these two forms of equation (6.8).

It is convenient to restrict our attention to a set $\mathfrak{D}_e$ lying in the support of χ. If g denotes the Hasse invariant (as in § 4) let

$$\mathfrak{D}_e = \{\lambda \mid e > \operatorname{Max}(\operatorname{ord}\lambda,\ \operatorname{ord}\lambda^{-1},\ \operatorname{ord}(1-\lambda),\ \operatorname{ord} g(\lambda))\}.$$

(Thus in this section, $\mathfrak{D}_e$ does not have the same meaning as in § 7.) In the following it will be assumed that e is positive but sufficiently small.

For $z\in\mathfrak{D}_e$ put

(8.1) $$\tilde{F}(z, X) = \exp(\pi X_0 f(z, X) - \pi X_0^p f(z', X^p))$$

where

(8.2) $$f(\lambda, X) = X_1(X_1-X_3)(X_1-\lambda X_3) - X_2^2 X_3$$

and $z'=\chi(z)$. Let

(8.3) $$p\tilde{\alpha}_z^* = \gamma_- \circ \frac{1}{\tilde{F}(z, X)} \circ \Phi,$$

(recall that in § 6, *i)* we also dropped the factor p from α_z^* and this will be continued in this section). Then $\tilde{\alpha}_z^*$ is a mapping of $\mathfrak{R}_{z'}$ onto $\mathfrak{R}_z$ and (cf. § 6, *b)*) if $\hat{\chi}$ is used to denote

the mapping of $\mathfrak{M}_{z'}$ onto $\mathfrak{M}_z$ obtained by composition with χ, then the following diagram is commutative. (Here as in § 6, *i)*, φ denotes composition with the p-th power map i.e. $h(\lambda)^{\varphi}=h(\lambda^p)$.)

$$\begin{array}{ccccc}
\mathfrak{R}_\lambda\otimes\mathfrak{M}_{z'} & \xrightarrow{\hat{\chi}} & \mathfrak{R}_{\lambda'}\otimes\mathfrak{M}_z & \xrightarrow{\tilde{\alpha}^*_\lambda} & \mathfrak{R}_\lambda\otimes\mathfrak{M}_z \\
\uparrow{\scriptstyle T_{z',\lambda}} & & & & \uparrow{\scriptstyle T_{z,\lambda}} \\
\mathfrak{R}_{z'} & & \xrightarrow{\tilde{\alpha}^*_z} & & \mathfrak{R}_z \\
\downarrow{\scriptstyle T_{z',z^p}} & & & & \| \\
\mathfrak{R}_{z^p} & & \xrightarrow{\alpha^*_z} & & \mathfrak{R}_z \\
\downarrow{\scriptstyle T_{z^p,\lambda}} & & & & \downarrow{\scriptstyle T_{z,\lambda}} \\
\mathfrak{R}_\lambda\otimes\mathfrak{M}_{z^p} & \xrightarrow[\varphi]{} & \mathfrak{R}_{\lambda^p}\otimes\mathfrak{M}_z & \xrightarrow[\alpha^*_\lambda]{} & \mathfrak{R}_\lambda\otimes\mathfrak{M}_z
\end{array}$$

Thus if $\tilde{A}_\lambda$ denotes the matrix of $\tilde{\alpha}^*_\lambda$, then precisely as § 6,

$$\tilde{\rho} : \mathfrak{X} \to (\mathfrak{X}\circ\chi)\tilde{A}_\lambda \tag{8.4}$$

is a monomorphism of solutions of (6.26) in $\mathfrak{M}_{z'}$ onto solutions in $\mathfrak{M}_z$. The only point to check is the growth conditions for $\tilde{\mathrm{F}}$, which are essentially the same as those for $\mathrm{F}(z, \mathrm{X})$ as may be shown by applying equation (7.8) to determine the growth conditions satisfied by the ratio $\tilde{\mathrm{F}}(z, \mathrm{X})/\mathrm{F}(z, \mathrm{X})$.

We shall use ρ to denote the mapping of § 6 (with $q=p$)

$$\rho : \mathfrak{X} \mapsto \mathfrak{X}^{\varphi} A_\lambda$$

of solutions of (6.26) in $\mathfrak{M}_{z^p}$ into solutions in $\mathfrak{M}_z$.

Lemma (**8.1**). — *For e sufficiently small, $e>0$,*

(i) *$\tilde{A}_\lambda$ is a uniform analytic matrix function of support $\mathfrak{D}_e$.*

(ii) *The mapping $\tilde{\rho}$ of (8.4) may be naturally identified with the mapping ρ for all $z\in\mathfrak{D}_e$.*

Proof. — The first assertion follows precisely as the proof of the similar property for A_λ, using the explicit formula ([4], equation (5.27)) and the analytic properties of the function χ.

For the second assertion, let $\mathfrak{S}$ be the union of $\mathfrak{P}$ with its images under the mappings $\lambda\mapsto 1-\lambda$, $\lambda\mapsto 1/\lambda$. For $z\notin\mathfrak{S}$ the solutions of (6.26) in $\mathfrak{M}_z$ are in fact holomorphic in $z+\mathfrak{P}$ and therefore solutions in $\mathfrak{M}_{z'}$ may certainly be identified in a natural way with those in $\mathfrak{M}_{z^p}$ (naturally provided $z\in\mathfrak{D}_e$). The assertion follows in this case from the previously mentioned commutative diagram. For $z\in\mathfrak{S}$ the same argument applies

provided $\log(z'/z^p)$ (resp. $\log(z'-1)/(z^p-1)$, resp. both $\log(z'/z^p)$ and $\sqrt{z'/z^p}$) is (are) well defined for z (resp. $1-z$, resp. $1/z$) in $\mathfrak{P}$. This is certainly valid if $z\in\mathfrak{D}_e$.

Our main result is the explicit computation of the matrix $\widetilde{A}_\lambda$. As in § 4 we use F to denote the hypergeometric function $F\left(\frac{1}{2}, \frac{1}{2}, 1, \lambda\right)$. Let $\varepsilon=(-1)^{(p-1)/2}$.

Theorem **(8.1)**. — *For* $\lambda\in\mathfrak{P}$, *the matrix* $\widetilde{A}_\lambda$ *of* $\widetilde{\alpha}_\lambda^*$, *relative to the basis used in* § 6 *i)*, *is given by*

$$\varepsilon\widetilde{A}_\lambda=\begin{pmatrix} F(\lambda)/F(\lambda') & \frac{d}{d\lambda}(F(\lambda)/F(\lambda')) \\ 0 & \left(\frac{d\lambda'}{d\lambda}\right)F(\lambda)/F(\lambda') \end{pmatrix}.$$

Note. — (The condition $\lambda\in\mathfrak{P}$ is clearly too conservative. The extension will be considered after the completion of the proof.)

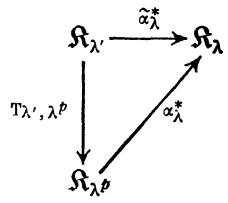
Proof. — Let us denote the right side of this asserted equality by the symbol L. Our basis has been chosen so that for $e>\operatorname{ord} z>0$, the solution matrix in $\mathfrak{M}_z$ is of the form

$$\exp\left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\log(\lambda/z)\right)\Upsilon(\lambda) \tag{8.6}$$

where (letting $D=\lambda(1-\lambda)$ and using equations (4.19), (4.23))

$$\Upsilon=\begin{pmatrix} -FW & (DF)^{-1}-F'W \\ F & F' \end{pmatrix}. \tag{8.7}$$

In an obvious sense, viewing λ as a variable element of Ω close to z, we have the commutative diagram



The matrix of $T_{z,\lambda}$ is

$$(T_{z,\zeta})=\Upsilon(z)^{-1}\exp\left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\log(\lambda/z)\right)\Upsilon(\lambda) \tag{8.8}$$

since this is the solution matrix which specializes to the identity when λ specializes to z. Thus

$$(T_{\lambda',\lambda^p})=\Upsilon(\lambda')^{-1}\exp\left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\log(\lambda^p/\lambda')\right)\Upsilon(\lambda^p). \tag{8.9}$$

Using equation (6.17) and the commutative diagram we obtain

$$\widetilde{A}_\lambda = \Upsilon(\lambda')^{-1} \exp\left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \log(\lambda^p/\lambda')\right) \mathfrak{A}\Upsilon(\lambda). \tag{8.10}$$

We recall that in § 6, *i)* we computed

$$\mathfrak{A} = \varepsilon \begin{pmatrix} p & b \\ 0 & 1 \end{pmatrix} \tag{8.11}$$

where b is a constant whose value will be shown shortly to be $\log 16^{1-p}$.

Substituting (8.7) in (8.10), using $\overline{\mathrm{F}}$, $\overline{\mathrm{W}}$, etc., to denote $\mathrm{F}\circ\chi$, $\mathrm{W}\circ\chi$, etc., and using H to denote $\overline{\mathrm{W}} - p\mathrm{W} + \log(\lambda^p/\lambda')$, we obtain

$$\varepsilon\widetilde{A}_\lambda = Q_1 + (b + \mathrm{H})\overline{\mathrm{D}}Q_2 \tag{8.12}$$

where

$$Q_1 = \begin{pmatrix} \mathrm{F}/\overline{\mathrm{F}} & -p(\overline{\mathrm{F}}'/\mathrm{F})(\overline{\mathrm{D}}/\mathrm{D}) + \mathrm{F}'/\overline{\mathrm{F}} \\ 0 & p(\overline{\mathrm{F}}/\mathrm{F})(\overline{\mathrm{D}}/\mathrm{D}) \end{pmatrix}. \tag{8.13}$$

$$Q_2 = \begin{pmatrix} -\mathrm{F}\overline{\mathrm{F}}' & -\mathrm{F}'\overline{\mathrm{F}}' \\ \mathrm{F}\overline{\mathrm{F}} & \overline{\mathrm{F}}\mathrm{F}' \end{pmatrix}. \tag{8.14}$$

By means of equation (7.17) it is obvious that $Q_1 = L$ and hence

$$\varepsilon\widetilde{A}_\lambda - L = (b + \mathrm{H})\overline{\mathrm{D}}Q_2. \tag{8.15}$$

We must show that the right side is zero. The central point is that equation (7.16) shows that

$$\mathrm{H} = \log 16^{p-1} \tag{8.16}$$

and hence $\mathrm{H} + b$ is a constant. Let $\mathfrak{D}'_e = \{\lambda \in \mathfrak{D}_e \mid \operatorname{ord} g(\lambda) = 0\}$. We have noted in the proof of Lemma (7.2) that $\mathrm{F}(\lambda')/\mathrm{F}(\lambda)$ has a holomorphic extension to $\mathfrak{D}'_e$ and thus both L and $\widetilde{A}_\lambda$ are uniform analytic matrix functions of support containing this set. We conclude that the same holds for the right side of equation (8.15) and hence either $\mathrm{H} + b = 0$ or $\mathrm{F}\overline{\mathrm{F}}$ also is uniform analytic function with this support. In the second event F^2 would also have support $\mathfrak{D}'_e$ and this would imply that the right side of equation (6.29) is ± 1, contradicting the Riemann hypothesis for elliptic curves. This implies the vanishing of $\mathrm{H} + b$. This proves the theorem and also demonstrates

$$b = \log 16^{1-p}. \tag{8.17}$$

Since the support of $\mathrm{F}(\lambda)/\mathrm{F}(\lambda')$ certainly contains the set $\mathfrak{S}$ introduced in the proof of Lemma (8.1), and since the support $\mathfrak{D}_e$ of $\widetilde{A}_\lambda$ has non-trivial intersection with the quasi-connected set $\mathfrak{S}$, we conclude that both $\mathrm{F}(\lambda)/\mathrm{F}(\lambda')$ and the coefficients of $\widetilde{A}_\lambda$ may be extended to uniform analytic functions of support containing $\mathfrak{D}_e \cup \mathfrak{S}$. Thus the conclusion of the theorem is valid for λ in this union.

We shall show (Lemma (8.4) below) that the support contains the support of χ. We note in passing that the singularities of A_λ are of necessity restricted to neighborhoods of 0, 1, ∞ and by the methods of § 6 *d)*, (i), the only singularity of A_λ is in fact located at $\lambda=1$ with principal part of the form

$$\log\frac{(\lambda-1)^p}{\lambda^p-1}.$$

We have just noted that $F(\lambda)/F(\lambda')$ may be extended to a function f_1 of support $\mathfrak{D}_e$. Similarly, for each integer s, we define

$$f_s(\lambda)=f_1(\lambda)f_1(\lambda')\dots f_1(\lambda^{(s-1)})$$

holomorphic on $\mathfrak{D}_e$ (where e may have to be reduced in a manner depending on s) and where $\lambda^{(s)}$ is defined inductively by $\chi(\lambda^{(s-1)})=\lambda^{(s)}$.

If $\beta=\beta^{p^\nu}$, $\beta\neq 0, 1, \infty$, then $\rho^\nu(=\tilde{\rho}^\nu)$ is an endomorphism of solutions of (6.26) holomorphic in $\beta+\mathfrak{P}$. We know from § 6 *i)* that the eigenvalues of ρ^ν are the zeros of the zeta function of the reduced elliptic curve (defined over $GF[p^\nu]$) of modulus $\beta \bmod \mathfrak{P}$. If c_1, c_2 are the zeros of the zeta function then we may choose (choice enters because we may have $c_1=c_2$) two linearly independent eigenvectors, (u_i, u_i') $(i=1, 2)$ and conclude from Theorem (8.1) that for $\lambda\in\mathfrak{D}_e\cap(\beta+\mathfrak{P})$

$$\varepsilon^\nu u_i(\lambda^{(\nu)})f_\nu(\lambda)=c_i u_i(\lambda). \tag{8.18}$$

Naturally there is no need to distinguish between solutions u of (4.2) and solutions (u, u') of (6.26). Thus we may say that ρ operates on solutions of (4.2).

For possible future use we record the matrix $\tilde{A}^{(\nu)}$ associated with ρ^ν (i.e. $\rho^\nu : (u, u')\to(u(\lambda^{(\nu)}), u'(\lambda^{(\nu)}))\tilde{A}^{(\nu)}$):

$$\tilde{A}^{(\nu)}=\varepsilon^\nu\begin{pmatrix} f_\nu(\lambda) & f_\nu'(\lambda) \\ 0 & f_\nu(\lambda)\dfrac{d\lambda^{(\nu)}}{d\lambda}\end{pmatrix}. \tag{8.19}$$

b) *Non-supersingular reduction.*

We now assume that $\beta \bmod \mathfrak{P}$ is a non-supersingular modulus and that there are ν elements in the orbit of β under the p-th power map. Let c_1 be the unit root and $c_2=p^\nu/c_1$ be the non-unit root of the zeta function of the corresponding elliptic curve. Since f_ν assumes only unit values for λ in $\beta+\mathfrak{P}$, it follows from equation (8.18) that u_1 is the unique bounded solution of (4.2) of support $\beta+\mathfrak{P}$ and hence u_2 is unbounded. We assert that u_2 has interesting arithmetic properties, namely the zeros of u_2 form the set of all moduli λ in $\beta+\mathfrak{P}$ corresponding to curves isogeneous to the canonical lifting.

Lemma **(8.2).** — *The zero set of u_2 consists of all $\lambda\in\beta \bmod \mathfrak{P}$ such that for some s, $\lambda^{(s\nu)}=\beta_{can}$, the canonical lifting of $\beta \bmod \mathfrak{P}$* (cf. § 7 *d*). *Thus each zero is an algebraic number.*

Proof. — Equation (8.18) shows that for $\lambda \in \beta + \mathfrak{P}$:

$$\frac{u_2}{u_1}(\lambda^{(v)}) = \frac{c_2}{c_1}\frac{u_2}{u_1}(\lambda). \tag{8.20}$$

Since β_{can} is a fixed point of $\chi^{(v)}$ and $c_2 \neq c_1$, it follows that β_{can} is a zero of u_2. Conversely if z is a zero of u_2 then the equation shows that for each integer s, $\chi^{(vs)}(z)$ is again a zero of u_2. For given z, s large enough, $\chi^{(vs)}(z) = z_s$ lies in $\beta + p\mathfrak{O}$. This set contains only a finite number of zeros of u_2. Thus there exist s, t, $t > 0$ such that $z_s = z_{s+t}$. Hence z_s is a fixed point of $\chi^{(tv)}$ in $\beta + \mathfrak{P}$. The Newton polygon of $\chi^{(tv)}$ may be used to show that this mapping has only one fixed point in $\beta + \mathfrak{P}$. Since β_{can} is such a fixed point, we conclude that $z_s = \beta_{can}$. This completes the proof of the lemma.

Note. — By suitable normalization, say

$$u_1(\beta_{can}) = 1, \qquad u_2'(\beta_{can}) = (\beta_{can}(1 - \beta_{can}))^{-1}(\tilde{F}_0(\beta))^{-2}$$

where $\tilde{F}_0(\beta)$ is chosen, as was $F_0(\alpha)$ in (4.25), to satisfy $\tilde{F}_0(\beta)^{1-\tau} = f_1(\beta_{can})$, we obtain $\exp(u_2/u_1) = \tilde{q}_\alpha$ as used in equation (7.22). This lemma provides a characterization of $\tilde{q}_\alpha$ which may be simpler than that of (7.23), namely $\tilde{q}_\alpha$ is determined up to a unit exponent in $\mathbf{Q}_p$ by the condition that it map $\beta + \mathfrak{P}$ holomorphically into $1 + \mathfrak{P}$ and that its value is a p-th power root of unity at the points indicated in the lemma.

Finally we observe that the unit root of the zeta function of the reduced elliptic curve is $c_1 = \varepsilon^v f_v(\beta_{can})$.

c) *Supersingular Reduction* ($p \neq 2, 3$).

We suppose that β is fixed under an iterate of the p-th power map and that β is a zero mod $\mathfrak{P}$ of the Hasse invariant g, given by equation (4.3). It is well known (cf. note following Lemma (8.7) below) that $\beta^{p^2} = \beta$.

Our main purpose (cf. Lemmas (8.14), (8.15) below) is to investigate the arithmetic properties of the eigenvectors of ρ^2 as endomorphism of solutions of equation (4.2) of support $\rho + \mathfrak{P}$. Two by-products of this investigation are

(i) the semisimplicity of ρ^2 (proven in Lemma (8.14) and again by a different method in section 8 *d)* below);

(ii) more complete information concerning the behavior of χ in $\beta + \mathfrak{P}$ (cf. Theorem (8.2), Lemma (8.11), and § 8 *d)* below).

A conceptual proof of (i) has been obtained by Katz, and results of type (ii) have been obtained by J. Lubin by means of the theory of formal groups. The methods of both Katz and Lubin have the advantage of being less dependent upon the choice of model (such as (4.1)).

We shall use the fact that the eigenvalues of ρ^2 (as endomorphism of solutions of (4.2) of support $\rho + \mathfrak{P}$) are equal. A proof will be given in § 8, *d)*. This result was brought to our attention by Lubin who showed that the zeta function of a super-

singular elliptic curve over $GF[p^2]$ has equal roots if and only if the points of order two are rational over $GF[p^2]$.

Thus for the present application there are just two possibilities, either $\nu=1$ and the eigenvalues of ρ are $\pm\sqrt{-p}$, or $\nu=2$ and the eigenvalues are equal. Thus the ratio c of eigenvalues is $(-1)^\nu$.

In the following we shall restrict our attention to the disk $\beta+\mathfrak{P}$. It will be convenient to introduce the notation for disks:

$$C(a)=\{\lambda \mid \operatorname{ord}(\lambda-\beta)>a\}$$

and for annuli $$\mathfrak{A}(a,b)=\{\lambda \mid a<\operatorname{ord}(\lambda-\beta)<b\}.$$

We write the principal part of χ at β in the form

(8.21) $$h(\lambda)=\sum_{n=1}^{\infty} A_n/(\lambda-\beta)^n$$

and recall that for $n\geq 1$

$$\operatorname{ord} A_n \geq \frac{1}{p+1}+n\frac{p}{p+1}.$$

Our first object (Theorem (8.2) below) is to show that $\operatorname{ord} A_1=1$. This will require considerable preparation.

Lemma **(8.3)**. —

$$\operatorname{ord}(\chi(\lambda)-\beta^p)\begin{cases} =p\operatorname{ord}(\lambda-\beta) & \text{if } \lambda\notin C(1/(p+1)) \\ \geq p/(p+1) & \text{if } \operatorname{ord}(\lambda-\beta)=1/(p+1) \\ =1-\operatorname{ord}(\lambda-\beta) & \text{if } \operatorname{ord} A_1=1 \\ \geq \operatorname{Min}(1, p\operatorname{ord}(\lambda-\beta)) & \text{if } \operatorname{ord} A_1>1 \end{cases} \lambda\in\mathfrak{A}\left(\frac{1}{p+1},\frac{p}{p+1}\right).$$

Proof. — In any case

$$\operatorname{ord} h(\lambda)\geq 1-\operatorname{ord}(\lambda-\beta)$$
$$\operatorname{ord}(\chi(\lambda)-\lambda^p-h(\lambda))\geq 1.$$

For $\operatorname{ord}(\lambda-\beta)<1/(p+1)$, we have

$$\operatorname{ord}(\lambda^p-\beta^p)=p\operatorname{ord}(\lambda-\beta)<1-\operatorname{ord}(\lambda-\beta),$$

which proves the first assertion. The second assertion follows from the same argument. For the third assertion we use the fact that if $\operatorname{ord} A_1=1$ then $\operatorname{ord} h(\lambda)=1-\operatorname{ord}(\lambda-\beta)$, while for the annulus in question:

$$\operatorname{ord}(\lambda^p-\beta^p)\geq \operatorname{Min}(p\operatorname{ord}(\lambda-\beta),\ 1+\operatorname{ord}(\lambda-\beta))>1-\operatorname{ord}(\lambda-\beta).$$

Finally if $\operatorname{ord} A_1>1$ then by Lemma (7.5):

$$\operatorname{ord} h(\lambda)\geq 2-\operatorname{ord}(\lambda-\beta)$$

and hence in the indicated annulus, $\operatorname{ord} h(\lambda)>1$. The assertion then follows from the estimate for $\operatorname{ord}(\lambda^p-\beta^p)$. This completes the proof of the lemma.

This shows that $\chi^{(s)}$, the s-fold iterate of χ with itself, is holomorphic in the annulus, $\mathfrak{A}\left(0, \frac{1}{p^{s-1}} \frac{p}{p+1}\right)$.

Lemma **(8.4).** — *The support of* $\tilde{A}_\lambda$ *in* $\beta+\mathfrak{P}$ *contains the support of* χ.

Proof. — We know that if M is a solution matrix of (6.26) holomorphic in $\beta^p+\mathfrak{P}$ then

$$M(\lambda')\tilde{A}_\lambda = M_1(\lambda),$$

a solution matrix holomorphic in $\beta+\mathfrak{P}$. The assertion follows by writing $\tilde{A}_\lambda$ in terms of $M_1(\lambda)$ and $M(\lambda')$.

We now obtain approximate estimates for $f_1(\lambda)$ in $\beta+\mathfrak{P}$.

Lemma **(8.5).** —

$$\left.\begin{aligned} &\operatorname{ord}\frac{d\lambda'}{d\lambda} \geq 1-2\operatorname{ord}(\lambda-\beta) \\ &\operatorname{ord} f_1(\lambda) \leq \operatorname{ord}(\lambda-\beta) \end{aligned}\right\} \quad \text{for} \quad \lambda \in \mathfrak{A}\left(0, \frac{p}{p+1}\right)$$

$$\operatorname{ord} f_s(\lambda) \leq \frac{p^s-1}{p-1}\operatorname{ord}(\lambda-\beta) \quad \text{for} \quad \lambda \in \mathfrak{A}\left(0, \frac{1}{p^{s-1}}\frac{p}{p+1}\right),\ s \geq 1.$$

Proof. — Since $\beta \neq 0, 1$, equation (7.17) gives

$$-2\operatorname{ord} f_1(\lambda) = -1 + \operatorname{ord}\frac{d\lambda'}{d\lambda}$$

while equation (8.21) shows that

$$\operatorname{ord} h'(\lambda) \geq 1-2\operatorname{ord}(\lambda-\beta)$$

and the second equation in the proof of Lemma (8.3) gives the same estimate for $\operatorname{ord}\frac{d\lambda'}{d\lambda}$. The first two assertions follow directly. This shows that

$$\operatorname{ord} f_s(\lambda) \leq \sum_{n=0}^{s-1} \operatorname{ord}(\lambda^{(n)}-\beta^{p^n}).$$

The last assertion now follows from Lemma (8.3).

Lemma **(8.6).** — *Each solution of* (4.2) *holomorphic in* $\beta+\mathfrak{P}$ *becomes unbounded as* $\operatorname{ord}(\lambda-\beta)$ *approaches zero.*

Proof. — We first consider the situation in which u is a solution of (4.2) which satisfies the conclusion of the lemma while v is a solution (also holomorphic in $\beta+\mathfrak{P}$) such that for some constant c_1:

$$(\rho^\nu - c_1)(v, v') = (u, u').$$

We assert that v also satisfies the conclusion of this lemma. Since

$$u(\lambda) = f_\nu(\lambda)v(\lambda^{(\nu)}) - c_1 v(\lambda),$$

it is clear that if v remains bounded then $f_\nu(\lambda)$ must be unbounded and hence $\dfrac{d\lambda^{(\nu)}}{d\lambda}$ must approach zero as $\operatorname{ord}(\lambda-\beta)$ approaches zero, which could be used to show that $\lambda^{(\nu)}$ is constant, which is impossible.

Thus it is enough to show that eigenvectors of ρ^ν satisfy the conclusion of the lemma. If (u, u') is an eigenvector of ρ^ν, then equation (8.18) shows that for $s\geq 1$:

$$\operatorname{ord} u(\lambda^{(s\nu)})+\operatorname{ord} f_{s\nu}(\lambda)=\frac{\nu s}{2}+\operatorname{ord} u(\lambda), \tag{8.22}$$

and hence by the preceding lemma:

$$\operatorname{ord} u(\lambda)\leq \operatorname{ord} u(\lambda^{(s\nu)})-\frac{\nu s}{2}+\frac{p^{s\nu}-1}{p-1}\operatorname{ord}(\lambda-\beta),$$

for $\operatorname{ord}(\lambda-\beta)$ sufficiently close to zero. We now let $s\to\infty$, keep $\lambda^{(s\nu)}$ fixed so that $\operatorname{ord}(\lambda-\beta)\to 0$ and observe that $u(\lambda)$ becomes unbounded as asserted.

Lemma **(8.7)**. — χ *cannot have support containing* $\beta+\mathfrak{P}$.

Proof. — Otherwise $h(\lambda)=0$ and hence everywhere in $\beta+\mathfrak{P}$:

$$\operatorname{ord}(\chi(\lambda)-\lambda^p)\geq 1.$$

It would then follow that there exists $\beta_0\in\beta+\mathfrak{P}$ such that $\beta_0^{(\nu)}=\beta_0$. The proof of Lemma (8.5) would also show that

$$\operatorname{ord} f_1(\lambda)\leq 0.$$

Thus equation (8.18) would give (if (u, u') were eigenvector of ρ^ν):

$$\operatorname{ord} u(\lambda)\leq -\frac{\nu}{2}+\operatorname{ord} u(\lambda^{(\nu)}),$$

and hence $u(\beta_0)=0$, thus showing that up to a constant factor, there can be but one eigenvector (and hence ρ^ν is not semisimple). Thus as in the proof of Lemma (8.6) we may choose an independent solution v, such that

$$u(\lambda)=f_\nu(\lambda)v(\lambda^{(\nu)})-c_1 v(\lambda)$$

where $c_1=\pm p$. In particular then, $(f_\nu(\beta_0)-c_1)v(\beta_0)=0$ while $\operatorname{ord} f_\nu(\beta_0)\leq 0$ which shows that $v(\beta_0)=0$, which contradicts the independence of u and v. This completes the proof of the lemma.

Note. — The preceding sequence of lemmas is based to some extent upon $\beta^{p^2}=\beta$. This could be avoided and $\beta=\beta^{p^2}$ deduced from this last lemma and equation (7.10) which shows that the singularities of χ are restricted to the set

$$\lambda^{p^2}-\lambda\equiv 0 \bmod \mathfrak{P}.$$

Lemma **(8.8)**. — *Specializing* λ *to* β, *the matrix* A_λ *becomes*

$$A_\beta = \begin{pmatrix} \gamma_1 & \gamma_2 \\ \gamma_3 & \gamma_4 \end{pmatrix}.$$

(i) *This matrix has coefficients in* K_ν, *the unramified extension of* $K_1 = \mathbf{Q}_p(\pi)$ *of degree* $\nu (= 1, 2)$. *For* $p \geq 5$ *we have*

$$\operatorname{ord} \gamma_2 = 0, \quad \operatorname{ord} \gamma_1 \geq 1/\nu$$
$$\operatorname{ord} \gamma_3 = 1, \quad \operatorname{ord} \gamma_4 \geq 1.$$

(ii) *For* $\nu = 2$, *let* σ *be the automorphism of* K_2 *over* K_1 *and let*

$$A_\beta A_\beta^\sigma = \begin{pmatrix} \gamma_1' & \gamma_2' \\ \gamma_3' & \gamma_4' \end{pmatrix}.$$

Then

$$\operatorname{ord} \gamma_1' \geq 1, \quad \operatorname{ord} \gamma_2' \geq \frac{1}{2}$$
$$\operatorname{ord} \gamma_4' \geq 1, \quad \operatorname{ord} \gamma_3' \geq \frac{3}{2}$$

while if $\operatorname{ord} \gamma_1 = \frac{1}{2}$ *then*

$$\operatorname{ord} \gamma_2' = \frac{1}{2}, \quad \operatorname{ord} \gamma_3' \geq \frac{3}{2}.$$

If $A_\beta A_\beta^\sigma$ *is semisimple then* $\operatorname{ord} \gamma_1 = \operatorname{ord} \gamma_4 \geq 1$.

Proof. — These results are based on the methods of ([4], § 7). Certain modifications in notation are present.

a) The matrices of ([4], § 7) have an extraneous factor p, which as noted in § 6 *i)* is dropped here.

b) For the present application (e.g. equation (8.3) of [4]) the useful basis is represented by $\{\pi X_0 X_1 X_2 X_3, (\pi X_0 X_1 X_2 X_3)^2\}$ while in the reference the π-factors are missing.

c) The matrix of [4] is replaced by its transpose.

d) Aside from these minor changes we explain that the estimates of [4] are based on the splitting function indexed by $s = \infty$ ([2], § 4) while the present article is based on the $s = 1$ splitting function. The relations between the matrices $A_\beta^{(1)}$, $A_\beta^{(\infty)}$ are given by equation (3.19) [4] so that for the bases as indicated in item *b)* above,

$$A_\beta^{(1)} = (I + T_{\beta^p}) A_\beta^{(\infty)} (I + T_{\beta^p})^{-1}$$

where I is the multiplicative identity and T_β is a two by two matrix whose coefficients have ordinals not less than $t_p = \frac{p-1}{p} - \frac{1}{p-1}$. The statement and proof of the present

lemma are indeed valid only for $A_\beta^{(\infty)}$. However the purpose of the present lemma is to prove Lemma (8.9) below which involves stability properties under the mapping

$$(x, y) \to (x, y)A_\beta^{(1)}$$

of vectors satisfying the condition $\operatorname{ord} x/y = -\frac{1}{2}$. The proof of that lemma is based upon $A_\beta^{(\infty)}$ but we observe that the condition $\operatorname{ord}(x/y) = -1/2$ is not affected when (x, y) is replaced by $(x, y)(I+T)$ if the coefficients of T have ordinal greater than $1/2$. Since $t_p > 1/2$ for $p > 3$, we need make no further distinction between $A_\beta^{(1)}$ and $A_\beta^{(\infty)}$.

Making the modification in ([4], § 7) indicated by *a), b), c)* above we find

(8.24)
$$\operatorname{ord}\gamma_1 \geq 0, \quad \operatorname{ord}\gamma_2 \geq 0$$
$$\operatorname{ord}\gamma_4 \geq 1, \quad \operatorname{ord}\gamma_3 \geq 1.$$

For $\nu = 1$ we use $\gamma_1 + \gamma_4 = 0$ and hence $\operatorname{ord}\gamma_1 = \operatorname{ord}\gamma_4 \geq 1$, while $p = \det A_\beta$ which shows that $\operatorname{ord}(\gamma_1\gamma_4 - \gamma_2\gamma_3) = 1$. Thus $\operatorname{ord}(\gamma_2\gamma_3) = 1$, which together with the lower bounds of (8.24) gives the precise values of $\operatorname{ord}\gamma_2$ and $\operatorname{ord}\gamma_3$.

For $\nu = 2$ we use $\operatorname{Tr} A_\beta A_\beta^\sigma = \pm 2p$ and hence the explicit formula for the trace together with (8.24) show that $\operatorname{ord}\gamma_1 \geq 1/2$. Thus $\operatorname{ord}\gamma_1\gamma_4 \geq 3/2 > 1$ and the precise values of $\operatorname{ord}\gamma_2$, $\operatorname{ord}\gamma_3$ may be obtained as in the case $\nu = 1$ from the fact that $\operatorname{ord}\det A_\beta = 1$.

The estimates for $\operatorname{ord}\gamma_i'$ $(i = 1, 2, 3, 4)$ follow from the explicit formulae for the γ_i' in terms of the γ_i. If $A_\beta A_\beta^\sigma$ is semisimple then $0 = \gamma_2' = \gamma_1\gamma_2^\sigma + \gamma_2\gamma_4^\sigma$ so that $\operatorname{ord}\gamma_1 = \operatorname{ord}\gamma_4 \geq 1$ as asserted. This completes the proof of the lemma.

We recall that if v is a solution of (4.2) at β^p then the solution u at β given by $\rho(v, v') = (u, u')$ has initial conditions related to those of v by

(8.25)
$$(u(\beta), u'(\beta)) = (v(\beta^p), v'(\beta^p))A_\beta.$$

Let R_v (resp. R_u) $= v'(\beta^p)/v(\beta^p)$ (resp. $u'(\beta)/u(\beta)$). We shall say that v is *special* if

(8.26)
$$\operatorname{ord} R_v = -\frac{1}{2}$$

and the same holds for the images of (v, v') under powers of ρ. Two special solutions v_1, v_2 will be said to be a *polarized pair* if in addition

(8.27)
$$\operatorname{ord}(R_{v_1} - R_{v_2}) = \frac{-1}{2}$$

and the same holds for images under powers of ρ.

Lemma **(8.9).** — (i) *A polarized pair of special solutions exists in all cases.*

(ii) *If* $\nu = 1$ *then the eigenvectors of* ρ *form such a pair.*

(iii) *If* $\nu = 2$ *and* $A_\beta A_\beta^\sigma$ *is semisimple then of course the polarized pair of* (i) *consists of eigenvectors of* ρ^2 *while if* $A_\beta A_\beta^\sigma$ *is not semisimple then the unique eigenvector of* ρ^2 *is one element of a polarized pair of special solutions.*

Proof. — The discussion may be simplified by setting $B=\frac{1}{\sqrt{-p}}D^{-1}A_\beta D$ where $D=\begin{pmatrix}1 & 0\\ 0 & \sqrt{-p}\end{pmatrix}$.

If we write $B=\begin{pmatrix}b_1 & b_2\\ b_3 & b_4\end{pmatrix}$

then by an elementary computation, ord $b_1\geq 0$, ord $b_2=0=$ ord b_3, ord $b_4\geq\frac{1}{2}$. Furthermore the eigenvalues of B (resp. BB^σ) are $+1$, -1 (resp. both equal to $+1$ or -1) if $\nu=1$ (resp. $\nu=2$) obtained from the roots of the zeta function of the reduced elliptic curve by dividing by $\sqrt{-p}$ (resp. $-p$). With this change in matrix, special solutions correspond to units, x, such that if B and B^σ are viewed as fractional linear transformations

$$B:\ x\mapsto\frac{b_2+b_4x}{b_1+b_3x} \tag{8.28}$$

(similarly for B^σ) then Bx, $B^\sigma Bx$, $BB^\sigma Bx$, etc., are all units. Likewise a polarized pair of special solutions correspond to a pair of units x, y which satisfy this condition and also the further condition that the differences between corresponding images of x and y are also units.

We first consider the case in which ord $\gamma_1>\frac{1}{2}$ (i.e. ord $b_1>0$). If x is a unit then $Bx\equiv b_2/(b_3x) \bmod \pi$ so that both B and B^σ map units onto units. Furthermore if x and y lie in distinct residue classes mod π then the same holds for Bx (resp. $B^\sigma x$) and By (resp. $B^\sigma y$). Thus the existence of polarized pairs is clear if the residue class field has at least two distinct non-zero elements.

If ord $\gamma_1=\frac{1}{2}$ (i.e. b_1 is a unit) then $\nu=2$ and $A_\beta A_\beta^\sigma$ is not semisimple. We defer the proof of (i) for this case until we consider (iii).

To prove (ii) we recall that ord $\gamma_1>\frac{1}{2}$ so that b_1 is a non-unit while an eigenvector $(1, x_i)$ of B with eigenvalue e_i is given by $x_i=-(b_1-e_i)/b_3$. Thus $x_1-x_2=(e_1-e_2)/b_3=\pm 2/b_3$ and the assertion is clear.

We now consider part (iii) and hence we suppose that $\nu=2$, $A_\beta A_\beta^\sigma$ is not semisimple. If $(1, x)$ is the eigenvector of BB^σ of eigenvalue $e(=\pm 1)$ then both $(1, x)B$ and $(1, x^\sigma)$ are eigenvectors of $B^\sigma B$. Since $B^\sigma B$ is also not semisimple, we have

$$x^\sigma=\frac{b_2+b_4x}{b_1+b_3x}. \tag{8.29}$$

Thus $b_3xx^\sigma+b_1x^\sigma=b_4x+b_2$. Since b_2 is a unit, ord $x>0$ is impossible, while if ord $x<0$ then the b_3xx^σ term is the unique maximal one, which is impossible. Thus x is a unit, showing that the eigenvector of ρ^2 is special. To find y such that $(1, x)$ and $(1, y)$

correspond to a polarized pair, we may assume that $\operatorname{ord}\gamma_1=\frac{1}{2}$. Let t be an element of $\mathbf{K}_2$ to be chosen and let $(1,y)$ be the vector defined by

$$(1,y)BB^{\sigma}=e(1,y)+t(1,x).$$

Thus
$$(1,y)(BB^{\sigma})^m=e^m(1,y)+me^{m-1}t(1,x)$$

and letting
$$b_3'=b_3b_1^{\sigma}$$
$$y_m=(ey+mtx)/(e+mt),$$

it is easy to verify that $(1,y)$ and the eigenvector $(1,x)$ correspond to a polarized pair of special solutions if t is chosen such that y_m, By_m, y_m-x and By_m-Bx are units for all integers $m\geq 0$. This reduces to the condition that the residue classes of t, $\frac{1}{t}+\frac{1}{xb_3'}$, $\frac{1}{t}+\frac{b_3}{b_3'}\frac{1}{b_1+b_3x}$ be non-rational (i.e. not in $\mathbf{Z}$ mod p). For $p>3$, the residue class field of $\mathbf{K}_2$ has enough elements for t to be chosen so as to satisfy this condition. This completes the proof of the lemma.

If u_1, u_2 are independent solutions of (4.2) holomorphic in $\beta+\mathfrak{P}$ then we may consider $\tau=u_2/u_1$, a function meromorphic in $\beta+\mathfrak{P}$.

Lemma **(8.10)**. — *If u_1 and u_2 satisfy* (8.26) *then τ is holomorphic in* $\mathbf{C}\left(\frac{1}{2}+\frac{1}{p-1}\right)$ *and is a one to one map onto*

$$\mathrm{S}_{\tau}=\left\{z\,|\,\operatorname{ord}\left(\frac{z}{\tau(\beta)}-1\right)>\frac{1}{2}+\frac{1}{p-1}+\operatorname{ord}(\mathrm{R}_{u_1}-\mathrm{R}_{u_2})\right\}.$$

The inverse map is also holomorphic.

Proof. — We first note that since u_1 and u_2 satisfy (8.26) neither vanish at β. The main point in the proof is that since τ is a ratio of solutions of (4.2), it satisfies the Schwarzian equation (cf. E. Poole, *Introduction to the Theory of Linear Differential Equations*, Oxford, 1936, p. 121)

$$\frac{\tau'''}{\tau'}-\frac{3}{2}\left(\frac{\tau''}{\tau'}\right)^2=2\mathrm{I}$$

where
$$\mathrm{I}=\frac{1}{4}\left(\frac{1}{\lambda^2}+\frac{1}{\lambda(1-\lambda)}+\frac{1}{(1-\lambda)^2}\right).$$

We write this equation in the form

(8.30)
$$\frac{d}{d\lambda}(z_1,z_2)=(g(z_1,z_2),k(z_1,z_2))$$

where $z_1=\tau'$, $z_2=\tau''$, $g(z_1,z_2)=z_2$, $k(z_1,z_2)=2\mathrm{I}z_1+\frac{3}{2}(z_2^2/z_1)$.

Since $\beta \neq 0, 1$, ord $I \geq 0$ everywhere in $\beta + \mathfrak{P}$. The initial data is

$$\delta_1 = z_1(\beta) = \tau(\beta)\left(\frac{u_2'}{u_2}(\beta) - \frac{u_1'}{u_1}(\beta)\right)$$

(8.31)

$$\delta_2 = \frac{z_2}{z_1}(\beta) = -2\frac{u_1'}{u_1}(\beta) - \frac{1}{\beta} + \frac{1}{1-\beta}$$

(to compute δ_2 use the fact that $u_1^2\tau'$ is the Wronskian of (4.2)).

Since u_1 and u_2 are independent, $\delta_1 \neq 0$ and since u_1 satisfies (8.26), it is clear that $|\delta_2| > 1$.

Precisely as in the calculus of limits (cf. [20], § 2):

$$\frac{d^n z_1}{d\lambda^n} = \left(g\frac{\partial}{\partial z_1} + k\frac{\partial}{\partial z_2}\right)^{n-1} g \tag{8.32}$$

and hence for $|z_1 - \delta_1| \leq b_1$, $|z_2 - \delta_1\delta_2| \leq b_2$, (where b_1, b_2 are positive real numbers to be chosen subsequently), $|\lambda| \leq 1$, we obtain the estimates

$$\left|\frac{d^n z_1}{d\lambda^n}\right| \leq M_1\left(\mathrm{Max}\left(\frac{M_1}{b_1}, \frac{M_2}{b_2}\right)\right)^{n-1}, \tag{8.33}$$

where $M_1 = \mathrm{Sup}\, g$, $M_2 = \mathrm{Sup}\, k$, the sup to be computed in the indicated region. Clearly

$$M_1 \leq \mathrm{Max}(|\delta_1\delta_2|, b_2).$$

Since $\delta_1 \neq 0$, we may choose $b_1 < |\delta_1|$ so that in the indicated region

$$|z_1| = |\delta_1|,$$

and hence

$$M_2 \leq \mathrm{Max}(|\delta_1|, M_1^2/|\delta_1|).$$

We choose $b_2 = |\delta_1\delta_2|$ and thus $M_1 \leq |\delta_1\delta_2|$, $M_2 \leq |\delta_1||\delta_2|^2$. Thus $M_2/b_2 \leq |\delta_2|$, $M_1/b_1 \leq |\delta_2|e$ where

$$e = |\delta_1|/b_1 > 1.$$

However e may be made as close to 1 as desired. Equation (8.33) now takes the form

$$\left|\frac{d^n z_1}{d\lambda^n}\right| \leq M_1(e|\delta_2|)^{n-1}$$

and hence for λ close to β:

$$\tau'(\lambda) = \delta_1 + \delta_1\delta_2(\lambda - \beta) + \sum_{n=2}^{\infty} \frac{B_n}{n!}(\lambda - \beta)^n$$

where $|B_n| \leq M_1(e|\delta_2|)^{n-1}$ for $n \geq 2$. Since this inequality holds for all $e > 1$, we may let $e \to 1$ and deduce for $n \geq 2$:

$$|B_n| \leq M_1|\delta_2|^{n-1}. \tag{8.34}$$

It is now easy to conclude that

$$\textbf{(8.35)} \qquad \frac{\tau(\lambda)}{\tau(\beta)} - 1 = \frac{\delta_1}{\tau(\beta)}(\lambda-\beta)\left(1+\sum_{n=1}^{\infty}\frac{C_n}{(n+1)!}(\delta_2(\lambda-\beta))^n\right)$$

where $C_n \in \mathfrak{O}$ for $n \geq 1$. The lemma now follows from the fact that ord $\delta_2 = -\frac{1}{2}$ and $\delta_1/\tau(\beta) = R_{u_2} - R_{u_1}$.

We may now state one of our main conclusions.

Theorem **(8.2)**. — (We assume $p \geq 5$.)

In equation (8.21) ord $A_1 = 1$.

Proof. — Let v_1, v_2 be a polarized pair of special solutions of (4.2) in $\beta^p + \mathfrak{P}$ and let (u_i, u_i') be the image of (v_i, v_i') under ρ $(i = 1, 2)$. Thus if we set $\tau_0(\lambda) = \frac{v_2}{v_1}(\lambda)$, $\tau_1(\lambda) = \frac{u_2}{u_1}(\lambda)$, then by Theorem (8.1), for $\lambda \in \mathfrak{A}\left(0, \frac{p}{p+1}\right)$

$$\textbf{(8.36)} \qquad \tau_1(\lambda) = \tau_0(\lambda').$$

Now suppose ord $A_1 > 1$; then, restricting our attention to the annulus $\mathfrak{A}\left(\frac{1}{2} + \frac{1}{p-1}, \frac{p}{p+1}\right)$, we have by Lemma (8.3):

$$\text{ord}(\lambda' - \beta^p) \geq 1 > \text{ord}(\lambda - \beta)$$

so that the previous lemma, in particular equation (8.35), may be applied to both sides of (8.36), showing the existence (for each λ in the annulus) of x, y in $\mathfrak{P}$ such that

$$\tau_0(\beta^p)(1 + (R_{v_2} - R_{v_1})(\lambda' - \beta^p)(1+x)) = \tau_1(\beta)(1 + (R_{u_2} - R_{u_1})(\lambda - \beta)(1+y)).$$

It follows from equation (8.27) that $\tau_0(\beta^p)/\tau_1(\beta)$ is a unit B, and hence of the three quantities, ord$(B-1)$, $-\frac{1}{2} + \text{ord}(\lambda' - \beta^p)$, $-\frac{1}{2} + \text{ord}(\lambda - \beta)$, the two minimal ones must be equal. But as noted above ord$(\lambda' - \beta^p) > \text{ord}(\lambda - \beta)$ which shows that $-\frac{1}{2} + \text{ord}(\lambda - \beta) = \text{ord}(B-1)$, a constant, which is impossible. This proves the theorem.

We note that we have excluded one of the possibilities in Lemma (8.3) and hence for $\lambda \in \mathfrak{A}\left(\frac{1}{p+1}, \frac{p}{p+1}\right)$:

$$\textbf{(8.37)} \qquad \text{ord}(\chi(\lambda) - \beta^p) = 1 - \text{ord}(\lambda - \beta).$$

We shall refer to this annulus as the *critical annulus* (about β) and we shall refer to the " closed " disk

$$\left\{\lambda \mid \text{ord}(\lambda - \beta) \geq \frac{p}{p+1}\right\}$$

as the *inner disk* (about β).

Lemma **(8.11).** — (i) *For each positive integer s, the s-fold composition of χ with itself is holomorphic in the critical annulus.*

(ii) $\chi\circ\chi$ *may be extended from the critical annulus to a holomorphic function of support* $\mathrm{C}\left(\frac{1}{p+1}\right)$.

(iii) *Let u_1 be a solution of* (4.2) *of support $\beta+\mathfrak{P}$ which is an eigenvector of ρ^ν and let u_2 be an independent eigenvector of ρ^ν* (resp. *an independent solution of the same support*) *if ρ^ν is semi-simple* (resp. *not semisimple*). *Let $\tau=u_2/u_1$. If $\nu=1$ then*

$$\tau(\lambda')=-\tau(\lambda) \quad \textit{for} \quad \lambda\in\mathfrak{A}\left(0,\frac{p}{p+1}\right)$$

and for all ν

$$\tau(\lambda'')=\tau(\lambda) \qquad (\text{resp. } \tau(\lambda)+t)$$

for $\lambda\in\mathfrak{A}\left(0,\frac{1}{p+1}\right)\cup\mathrm{C}\left(\frac{1}{p+1}\right)$, *$t$ being non-zero in the non semi-simple case.*

(iv) $\lambda''=\lambda$ *for all* $\lambda\in\mathrm{C}\left(\frac{1}{p+1}\right)$ *if and only if ρ^ν is semisimple.*

Proof. — The first assertion follows directly from equation (8.37). For the second assertion we note that by Lemma (8.9) we may suppose that u_1, u_2 form a polarized pair of special solutions of support $\beta+\mathfrak{P}$. For each integer s, let $u_{i,s}$ be the image of u_i under ρ^s $(i=1,2)$. Thus putting $\tau_s=u_{2,s}/u_{1,s}$ $(\tau_0=\tau)$, which is meromorphic in $\beta^{p^s}+\mathfrak{P}$, it follows that for $s\geq 1$:

(8.38) $$\tau_s(\lambda)=\tau_{s-1}(\chi(\lambda))$$

for $\lambda\in\mathfrak{A}\left(0,\frac{p}{p+1}\right)$, the center being at β (resp. β^p) if s is even (resp. odd). In particular for $s=2$, this gives (for λ in the critical annulus)

$$\tau_2(\lambda)=\tau(\lambda'').$$

However Lemma (8.10) shows that $\lambda\mapsto\tau^{-1}\tau_2(\lambda)$ is holomorphic in $\mathrm{C}\left(\frac{1}{2}+\frac{1}{p-1}\right)$. If we denote this function by H then for $\lambda\in\mathfrak{A}\left(\frac{1}{2}+\frac{1}{p-1},\frac{p}{p+1}\right)$, both $\mathrm{H}(\lambda)$ and λ'' lie in $\mathrm{C}\left(\frac{1}{2}+\frac{1}{p-1}\right)$ while

$$\tau(\mathrm{H}(\lambda))=\tau(\lambda'')$$

and hence $\lambda''=\mathrm{H}(\lambda)$ for all λ in the last mentioned annulus. The function H thus extends $\chi^{(2)}$ to the asserted region, which completes the proof of (ii).

Part (iii) follows from (8.38) since for $\nu=1$, $\tau_1(\lambda)=\frac{\sqrt{-pu_1}}{-\sqrt{-pu_2}}(\lambda)=-\tau(\lambda)$, while for $\nu=2$, $\tau_2=\tau$ if ρ^ν is semisimple, and $\tau_2=\tau+t$ $(t\neq 0)$ if ρ^ν is not semisimple.

For part (iv) we note that if ρ^{ν} is not semisimple then $\lambda \mapsto \lambda''$ has no fixed points except at the zeros of u_1, while if ρ^{ν} is semisimple then for $\nu = 1, 2$, $\tau(\lambda'') = \tau(\lambda)$ and hence for $\lambda \in C\left(\frac{1}{2} + \frac{1}{p-1}\right)$, Lemma (8.10) shows that $\lambda = \lambda'$. This equality is extended in this case to $C\left(\frac{1}{p+1}\right)$ by part (ii).

The following lemma is of interest only in connection with the eventual proof that ρ^{ν} is semisimple.

Lemma **(8.12)**. — *If ρ^{ν} is not semisimple, then the eigenvector u_1 of ρ^{ν} of support $\beta + \mathfrak{P}$ cannot have a unique zero in the critical annulus.*

Proof. — Suppose otherwise and let z be the unique zero. Lemma (8.11) shows that $z'' = \chi^{(2)}(z)$ is also a zero of u_1. Since z'' also lies in the annulus, the hypothesis of uniqueness shows that $z'' = z$. Let $z' = \chi(z)$ and consider λ'' and λ as algebraic functions of λ' in a neighborhood of z'. We know (equation (7.10)) that (λ'', λ') and (λ, λ') are zeros of G_p and since λ and λ'' take the same value when $\lambda' = z'$, we may conclude that λ and λ'' coincide locally provided the root $t = z$ of the polynomial $G_p(t, z')$ is not a multiple root. Thus it is enough to show that (z, z') is not a zero of $\frac{\partial}{\partial X} G_p(X, Y)$. However

$$\frac{\partial}{\partial X} G_p(X, Y) \equiv X^p - Y \mod p\mathfrak{O}[X, Y]$$

while both z and z' lie in $\mathfrak{O}$ and $|z^p - z'| \equiv \left|\frac{A_1}{z-\beta}\right| > |p|$. We conclude that the partial derivative does not vanish. This shows that λ'' coincides locally with λ, which contradicts part (iii) of the preceding lemma.

We now give a more precise form of Lemma (8.5).

Lemma **(8.13)**. — *For $\lambda \in \mathfrak{A}\left(0, \frac{p}{p+1}\right)$ we have*

$$\operatorname{ord} \frac{d\lambda'}{d\lambda} = 1 - 2 \operatorname{ord}(\lambda - \beta)$$

$$\operatorname{ord} f_1(\lambda) = \operatorname{ord}(\lambda - \beta)$$

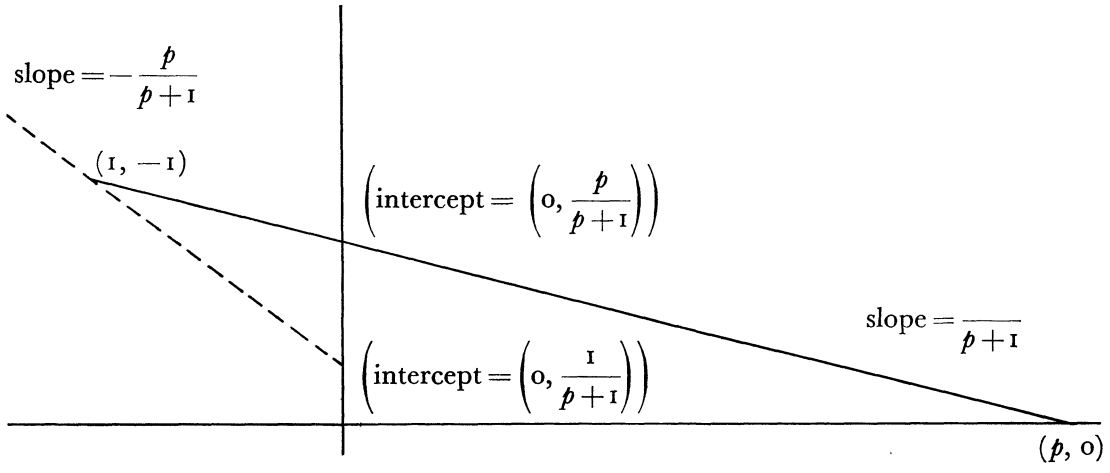
and hence if $\operatorname{ord}(\lambda_s - \beta) = \frac{1}{p^{s\nu}} \operatorname{ord}(\lambda - \beta)$, $\chi^{(s\nu)}(\lambda_s) = \lambda$, *then*

$$\operatorname{ord} u(\lambda_s) = \operatorname{ord} u(\lambda) - \frac{\nu s}{2} + \frac{1 - p^{-s\nu}}{p-1} \operatorname{ord}(\lambda - \beta)$$

if u is an eigenvector of ρ^{ν} of support $\beta + \mathfrak{P}$.

Proof. — The proofs of Lemmas (8.5), (8.6) show that it is enough to obtain the precise value of ord $\frac{d\lambda'}{d\lambda}$. This in turn may be reduced to the assertion that ord $h'(\lambda) = 1 - 2 \operatorname{ord}(\lambda - \beta)$ and this follows from equation (8.21) and Theorem (8.2). This completes the proof of the lemma.

Before turning to a closer examination of the zeros of the eigenvectors, we observe that the Newton polygon of $\chi(\lambda) - \beta^p$ as Laurent series in $(\lambda - \beta)$ is partially determined by Theorem (8.2). The side of slope $-\frac{1}{p+1}$ and the line of support [1] of slope $-\frac{p}{p+1}$ are as indicated in the diagram:



This diagram shows that if $\lambda' \in \beta^p + \mathfrak{P}$ then the equation

$$\chi(\lambda) = \lambda'$$

has either $p+1$ or p roots in $\mathfrak{A}\left(0, \frac{p}{p+1}\right)$. The former occurs if λ' lies either in the inner disk of center β^p $\left(\text{in which case the } p+1 \text{ roots lie on the circumference of } C\left(\frac{1}{p+1}\right)\right)$ or in the critical annulus of center β^p (in which case one root lies in the critical annulus and p roots lie on the circumference of $C\left(\frac{1}{p} \operatorname{ord}(\lambda' - \beta^p)\right)$. The second case occurs if λ' does not lie in the disk $C\left(\frac{1}{p+1}\right)$ of center β^p and in this case the p roots lie in the circumference of $C\left(\frac{1}{p} \operatorname{ord}(\lambda' - \beta^p)\right)\Big)$. (The roots are distinct by Lemma (8.16), (iii).)

[1] This line of support is indeed a side of infinite length (cf. § 8 *d)* below).

We now partition the points of $(\beta+\mathfrak{P})\cup(\beta^p+\mathfrak{P})$ into equivalence classes, two elements x, y being said to be equivalent if there exist non-negative integers m, n such that both

a) $\chi^{(m)}(x)=\chi^{(n)}(y)$;

b) none of the elements in either the sequence $\{\chi^{(i)}(x)\}_{i=0,1,\dots,m}$ or the sequence $\{\chi^{(j)}(y)\}_{j=0,1,\dots,n}$, except possibly for $\chi^{(m)}(x)=\chi^{(n)}(y)$, lie in the union of the disk $\mathbf{C}\left(\frac{1}{p+1}\right)$ with the corresponding disk of center β^p.

Each class has a unique " minimal " representative z in the union of these two disks. We partition the classes into 4 types depending upon the location of z.

I. z lies in the critical annulus of center β.
II. z lies in the critical annulus of center β^p.
III. z lies in the inner disk of center β.
IV. z lies in the inner disk of center β^p.

Of course if $\nu=1$ then $\beta=\beta^p$ and then there is no distinction between types I and II and no distinction between types III and IV.

We are interested in the intersection of each equivalence class with $\beta+\mathfrak{P}$. We classify the elements of each intersection according to their distances from β. The elements of a given intersection are now arranged by rings, the s-th ring having N_s elements λ having a common value D_s for $\operatorname{ord}(\lambda-\beta)$. In the following table, z refers to the minimal representative of the class. The element z itself is not counted in the table except for the class of type I.

Type	I = II	III = IV	I	II	III	IV
ν	1	1	2	2	2	2
D_s	$p^{-s}\operatorname{ord}(z-\beta)$	$p^{-s+1}/(p+1)$	$p^{-2s}\operatorname{ord}(z-\beta)$	$p^{-2s-1}\operatorname{ord}(z-\beta^p)$	$p^{-2s+1}/(p+1)$	$p^{-2s}/(p+1)$
N_s	p^s	$p^{s-1}(p+1)$	p^{2s}	p^{2s+1}	$p^{2s-1}(p+1)$	$p^{2s}(p+1)$
$s\geq$	0	1	0	0	1	0

Lemma **(8.14)**. — *Let u be an eigenvector of ρ^ν of support $\beta+\mathfrak{P}$. The zero set of u consists of the intersection of $\beta+\mathfrak{P}$ with either one or two classes. If $\nu=1$ then the zero set is a single class of type* I *whose minimal representative is a fixed point of χ. If two classes are involved then one class if of type* I *and the other is of type* II. *In particular this is the case for $\nu=2$ if u is a special solution. Furthermore ρ^2 is semisimple.*

Proof. — Let c_1 be the eigenvalue of ρ^ν for u. Let v be the image of u under ρ (so the support of v is $\beta^p+\mathfrak{P}$). The proof is based on

$$\text{(8.39)}\qquad \begin{aligned} v(\lambda')f_1(\lambda)&=c_1^{2/\nu}u(\lambda) \quad \text{if } \lambda\in\mathfrak{A}\left(0,\frac{p}{p+1}\right)\\ u(\lambda')f_1(\lambda)&=v(\lambda) \quad \text{if } \lambda\in\mathfrak{A}_{\beta^p}\left(0,\frac{p}{p+1}\right).\end{aligned}$$

Since u is unbounded, its zero set is non-empty and the above equations show that this set is the union of the intersection with $\beta+\mathfrak{P}$ of one or more classes.

We observe that if $\nu=1$ then by Lemma (8.9) the eigenvectors of ρ constitute a polarized pair of special solutions and hence by Lemma (8.10) there are no zeros in $C\left(\frac{1}{2}+\frac{1}{p-1}\right)$. This shows that in this case only classes of type I can occur.

We choose a rational number r, close to but less than $p/(p+1)$, such that u (resp. v) has no zeros on the circumferences of $C_\beta(r)$ (resp. $C_{\beta^p}(r)$). In this case u has no zeros on the circumference of $C(r/p^{2s})$ for any $s\geq 0$. If M_s denotes Inf ord $u(\lambda)$ as λ runs over the circumference of this last disk then we know from Lemma (8.13) that as $s\to\infty$:

$$\mathbf{(8.40)} \qquad M_s=-s+O(1).$$

We now compute M_s in terms of the zero set of u. Let $\mathfrak{C}$ be the intersection of a class with $\beta+\mathfrak{P}$ and let $L_s(\mathfrak{C})$ be the polynomial

$$L_s(\mathfrak{C})(\lambda)=\Pi\left(1-\frac{\lambda}{t}\right),$$

the product being over all $t\in\mathfrak{C}\cap C(r/p^{2s})$ (excluding the minimal representative in the inner disk if the class is of type III). Finally let $M_s(\mathfrak{C})$ denote Inf $L_s(\mathfrak{C})(\lambda)$, the inf again being over all λ in the circumference of $C(r/p^{2s})$. Clearly

$$\mathbf{(8.41)} \qquad M_s=\Sigma M_s(\mathfrak{C})+O(1),$$

the sum being over $\mathfrak{C}$ contained by the zero set of u. It is easy to compute $M_s(\mathfrak{C})$; we list the asymptotic value according to type, recalling that for $\nu=1$ we need only consider type I. As in the previous table, z refers to the minimal representative of the class of $\mathfrak{C}$.

Type	I	I	II	III	IV
ν	1	2	2	2	2
$M_s(\mathfrak{C})+O(1)$	$-2s$ ord$(z-\beta)$	$-s$ ord$(z-\beta)$	$-s$ ord$(z-\beta^p)$	$-s$	$-s$

If $\mathfrak{C}$ is of type I or II and lies in the zero set of u and has minimal representative z, then the class of $z'=\chi(z)$ must also meet the zero set. Thus if $\nu=1$ and $z\neq z'$ then by equation (8.41), $M_s+O(1)\leq -2s(\text{ord}(z-\beta)+\text{ord}(z'-\beta))=-2s$ which contradicts (8.40). Thus z must be a fixed point of χ and hence by (8.37), $\text{ord}(z-\beta)=\frac{1}{2}$. Thus $M_s(\mathfrak{C})=-s$ and no other class can occur.

We now suppose $\nu=2$. It is clear from the table that if a class of type III (resp. IV) meets the zero set of u then no other class can do so. If $\mathfrak{C}$ is of type I with representative z and $\mathfrak{C}'$ is the intersection of $\beta+\mathfrak{P}$ with the class of $z'=\chi(x)$ then

$M_s(\mathfrak{C})+M_s(\mathfrak{C}')=-s(\mathrm{ord}(z-\beta)+\mathrm{ord}(z'-\beta^p))+O(1)=-s+O(1)$. This shows that in this case no other class can occur.

We now consider the case in which u is special. We have already considered the case $\nu=1$ and hence may suppose $\nu=2$. From Lemma (8.9) we know that u is one element of a pair of special solutions (if ρ^2 is not semisimple this has been explicitly noted, while if ρ^2 is semisimple then by Lemma (8.8), $\mathrm{ord}\,\gamma_1\geq 1$ and the assertion follows from the proof of Lemma (8.9)) and from Lemma (8.10) we conclude that u has no zero in $\mathrm{C}\left(\frac{1}{2}+\frac{1}{p-1}\right)$. Equation (8.39) shows that u has no zero in the inverse image under χ of $\mathrm{C}_{\beta^p}\left(\frac{1}{2}+\frac{1}{p-1}\right)$. This shows that the zero set of u is neither of type III nor of type IV and hence is the union of the intersection of $\beta+\mathfrak{P}$ with one class of type I and the associated class of type II.

We now show that ρ^ν is semisimple. We may again assume $\nu=2$, that ρ^ν is not semisimple and that u is the unique eigenvector which, as we recall, is special. We have just seen that the zero set of u involves a class of type I and a class of type II and hence u has just one zero in the critical annulus. This contradicts Lemma (8.12), which completes the proof.

Lemma **(8.15)**. — (i) *If* $\nu=1$ *then the zeros of the eigenvectors are algebraic numbers. In this case* χ *has just two fixed points in* $\mathfrak{A}\left(0,\frac{p}{p+1}\right)$ *and the class of each fixed point is the zero set of one eigenvector.*

(ii) *If* $\nu=2$ *and* u *is a special solution of* (4.2) *then* u *has a unique zero in* $\mathrm{C}\left(\frac{1}{p+1}\right)$ *which lies on the circumference of the disk* $\mathrm{C}\left(\frac{1}{2}\right)$.

Proof. — If one element of a class is an algebraic number then all the elements are algebraic numbers. If $\nu=1$ the Newton polygon of χ shows that χ has just two fixed points in $\mathfrak{A}\left(0,\frac{p}{p+1}\right)$. The assertion for $\nu=1$ now follows from Lemma (8.14).

For $\nu=2$, since ρ^ν is semisimple, $u(=u_1)$ is one element of a polarized pair of special solutions $\{u_1,u_2\}$ which are both eigenvectors. Lemma (8.14) shows that $u_i\,(i=1,2)$ has a unique zero z_i in the critical annulus of center β. If we put $a=\mathrm{Max}(\mathrm{ord}(z_1-\beta),\mathrm{ord}(z_2-\beta))$ (resp. $a'=\mathrm{Min}(\mathrm{ord}(z_1-\beta),\mathrm{ord}(z_2-\beta))$) then for $\lambda\in\mathrm{C}(a)$ we have (normalizing u_i so that $u_i(\beta)=1$)

$$u_i(\lambda)\in\frac{\lambda-z_i}{\beta-z_i}(1+(\lambda-\beta)(p^{-b})) \tag{8.42}$$

where $b=(1-a')/p$. (Equation (8.42) follows from the Newton polygon of $u_i(\lambda)/(\lambda-z_i)$ (as power series in $(\lambda-\beta)$), which may be determined from the known distribution of the zeros of u_i.)

For $\tau = u_2/u_1$, we have (for λ in the above disk)

$$\tau(\beta) = 1$$

$$\tau(\lambda) \in 1 + \frac{(\lambda-\beta)(z_2-z_1)}{\left(1-\frac{\lambda-\beta}{z_1-\beta}\right)(z_2-\beta)(z_1-\beta)} + (\lambda-\beta)(p^{-b}). \tag{8.43}$$

If we compare this with equation (8.35), we conclude that for $\lambda \in C(a)$, $(R_{u_2} - R_{u_1})(1+\mathfrak{P})$ meets $\frac{z_2-z_1}{(z_2-\beta)(z_1-\beta)} + (p^{-b})$. Since $\operatorname{ord}(R_{u_1} - R_{u_2}) = -\frac{1}{2} < -b$ it follows that

$$\frac{1}{2} = \operatorname{ord}(z_2-\beta) + \operatorname{ord}(z_1-\beta) - \operatorname{ord}(z_2-z_1). \tag{8.44}$$

Likewise

$$\frac{1}{2} = \operatorname{ord}(z_2'-\beta^p) + \operatorname{ord}(z_1'-\beta^p) - \operatorname{ord}(z_2'-z_1'). \tag{8.45}$$

We assert $\operatorname{ord}(z_2-\beta) = \operatorname{ord}(z_1-\beta)$. Suppose otherwise, say $\operatorname{ord}(z_2-\beta) > \operatorname{ord}(z_1-\beta)$ then $\operatorname{ord}(z_2-z_1) = \operatorname{ord}(z_1-\beta)$, which shows that $\operatorname{ord}(z_2-\beta) = \frac{1}{2}$. On the other hand the same inequality implies that $\operatorname{ord}(z_1'-\beta^p) > \operatorname{ord}(z_2'-\beta^p)$ and hence by the same argument, using (8.45), $\operatorname{ord}(z_1'-\beta^p) = \frac{1}{2}$ which implies that $\operatorname{ord}(z_1-\beta) = \frac{1}{2}$, contradicting the presumed inequality.

Thus $\operatorname{ord}(z_2-\beta) = a = \operatorname{ord}(z_1-\beta)$, $\operatorname{ord}(z_2-z_1) \geq a$ and hence by equation (8.44), $a \geq \frac{1}{2}$. Hence by the same argument, using (8.45) (since

$$1 - a = \operatorname{ord}(z_1'-\beta^p) = \operatorname{ord}(z_2'-\beta^p))$$

we know that $1-a \geq \frac{1}{2}$. This shows that $a = \frac{1}{2}$ as asserted. This completes the proof of the lemma.

We note that for a pair of eigenvectors of ρ^ν which are also a polarized pair of special solutions (this hypothesis must be stated for $\nu = 2$), the zeros z_1, z_2 are as far apart as possible, i.e. $\operatorname{ord}(z_2-z_1) = \frac{1}{2}$. This is also true for $\nu = 1$ but in that case the modular equation may be used to show that $\operatorname{ord}(z_1+z_2) \geq 1$.

Lemmas (8.2) and (8.15) show that the eigenvectors of ρ^ν have an arithmetic significance provided the roots of the zeta function of the reduced curve are unequal. It seems natural to ask whether in the excluded case it is possible to choose particular solutions of (4.2) in an intrinsic fashion. We observe that certain solutions may be of particular interest. In the following we suppose $\nu = 2$, the roots are equal.

a) There exists a solution defined uniquely up to a constant factor over K_2 by the condition $u(\beta) = 0$. This solution has by Lemma (8.14) a solution set consisting

of the intersection with $\beta+\mathfrak{P}$ of a class of type III, the minimal representative being β itself. A second solution is obtained by noting that u^σ is a solution of support $\beta^p+\mathfrak{P}$ and that ρu^σ has support $\beta+\mathfrak{P}$ and its zero set involves a class of type IV whose minimal representative is β^p. Clearly both zero sets consist of algebraic numbers and one zero set is mapped into the other by an automorphism over K_1 which extends σ.

b) It is not difficult to show the existence of a solution u of (4.2) which is defined over K_2 and has the property that $\rho u/u^\sigma$ is a constant. In the notation of the proof of Lemma (8.9), this is equivalent to the choice of x in K_2 which satisfies equation (8.29). However we now know that BB^σ is semisimple and therefore a routine computation shows that $b_2/b_3=a\in K_1$, $b_1=-b_4^\sigma b_3^{1-\sigma}$, and that equation (8.29) is equivalent to the condition, for $x\in K_2$,

(8.46) $$N_{K_2/K_1}(b_1+b_3x)=e$$

where $-ep$ is the value of the two equal roots of zeta function of the reduced elliptic curve. If x is chosen in this way then x is a unit and the corresponding solution u of (4.2) with support $\beta+\mathfrak{P}$ has the property that

(8.47) $$\rho u=k\sqrt{-p}\,u^\sigma$$

where k is an element of K_2 such that $N_{K_2/K_1}k=e$. This condition does not specify k uniquely but any other choice is of the form $kt^{\sigma-1}$ where $t\in K_2^*$. Replacing u by tu, we may in equation (8.47) replace $kt^{\sigma-1}$ by k. The solutions of (4.2) of support $\beta+\mathfrak{P}$ and initial data defined over K_2 form a two dimensional K_2-space which may be viewed as a four dimension K_1-space. Equation (8.47) (with k fixed) defines a K_1-linear subspace of dimension two. Each non-trivial element of this subspace has unique zero z in $\mathfrak{A}\left(\frac{1}{p+1},\frac{p}{p+1}\right)$ which lies in K_2 and is invariant under $\sigma\circ\chi$. Conversely such a fixed point z defines uniquely (up to a constant multiple in K_2) a solution of (4.2) defined over K_2 and it is clear that by suitable choice of the constant multiple, we obtain a solution which satisfies (8.47).

Alternately for each $t\in K_2^*$, let z_t be the minimal representative of the zero set of the solution, u, of (4.2) which satisfies the initial condition

(8.48) $$u'(\beta)/u(\beta)=(kt^{\sigma-1}-b_1)/(b_3\sqrt{-p}).$$

Then $t\mapsto z_t$ is a one to one correspondence between K_2^*/K_1^* and the elements of $K_2\cap(\beta+\mathfrak{P})$ which are fixed under $\sigma\circ\chi$. Thus there exists an infinite set of fixed points on the circumference of $C\left(\frac{1}{2}\right)$. A closer examination of this set of fixed points may be of interest. Finally we note that since -1 has norm 1, we may choose a second solution v of (4.2) of support $\beta+\mathfrak{P}$ such that

$$\rho v=-k\sqrt{-p}\,v^\sigma.$$

With such a pair of solutions, we obtain $\frac{v}{u}(\lambda) = -\left(\frac{v}{u}\right)^{\sigma}(\lambda')$ for all $\lambda \in \mathfrak{A}\left(0, \frac{p}{p+1}\right)$, which generalizes the relation between λ, λ' and the ratio of eigenvectors in the case $\nu = 1$ (cf. Lemma (8.11), (iii)).

d) Non-extension of χ.

We recall that our treatment of the supersingular case was based on

(L) The eigenvalues of ρ^2 are equal,

a result for which, as noted previously, we are indebted to Lubin. We sketch a proof of this fact which is based on a property of χ which is of independent interest. This treatment gives another proof of the semisimplicity of ρ^{ν}, and hence eliminates the need of Lemma (8.12).

We use the fact that part (i) of Lemma (8.9) may be proven without the use of (L). From this we may deduce the validity of parts (i), (ii) of Lemma (8.11), while part (iii) of that lemma must be replaced by

$$\tau(\lambda'') = c\tau(\lambda) \quad \text{(resp. } \tau(\lambda) + t\text{)}$$

if ρ^{ν} is semisimple (resp. not semisimple), t being non-zero in the non-semisimple case and c being the ratio of the eigenvalues of ρ^{ν}. If we can show that $\lambda'' = \lambda$ for all λ in $C\left(\frac{1}{p+1}\right)$ then certainly ρ^2 is simply a multiplication by a constant.

To show this let $\mathfrak{N}_0$ be the ring of all elements of $\mathbf{Q}_p(\beta)[[\lambda - \beta]]$ which converge in $C\left(\frac{1}{p+1}\right)$ and let $\mathfrak{N}$ be the field of quotients of $\mathfrak{N}_0$. The field $\mathfrak{N}$ has an obvious imbedding in the field of functions meromorphic on $\mathfrak{A}\left(\frac{1}{p+1}, \frac{p}{p+1}\right)$ and the restriction of χ to this annulus is an element of this second field. Using λ' to denote this restriction, we may consider the field generated by λ' over $\mathfrak{N}$. We assert that

(8.50) $$\deg \mathfrak{N}(\lambda')/\mathfrak{N} = p + 1.$$

We have noted that for x fixed in the inner disk (about β^p) the equation $\chi(Y) = x$ has $p+1$ distinct roots, each lying in the circumference of $C\left(\frac{1}{p+1}\right)$. This implies that for x fixed in the inner disk (about β), the equation (cf. (7.10)) $G_p(x, Y) = 0$ has $p+1$ roots for Y each lying in the circumference of $C_{\beta^p}\left(\frac{1}{p+1}\right)$. Let $b = \deg \mathfrak{N}(\lambda')/\mathfrak{N}$ and let

$$H(\lambda, Y) = \sum_{i=0}^{b} h_i(\lambda) \cdot (Y - \beta^p)^i \in \mathfrak{N}_0[Y]$$

be an irreducible polynomial over $\mathfrak{N}$ satisfied by λ'. Certainly $1 \leq b \leq p+1$. If λ is specialized to any element z of the inner disk (about β) which is not a zero of $h_0 . h_b$ then

by the above remarks, $H(z, Y)$, as polynomial in $Y-\beta^p$, must have Newton polygon with only one side and that side has slope $\frac{1}{p+1}$. Thus with this choice of z:

$$\text{ord}(h_0(z)/h_b(z))=\frac{b}{p+1}. \tag{8.51}$$

However the intersection of $\mathbf{Q}_p(\beta)$ with the inner disk about β is an infinite set and hence z may be chosen in $\mathbf{Q}_p(\beta)$. With z so chosen, we may conclude that $h_0(z)/h_b(z)$ lies in $\mathbf{Q}_p(\beta)$. This shows that the left side of (8.51) is a rational integer and hence $b=p+1$ as asserted.

We now observe that $\lambda'-\beta^p$ as holomorphic function on $\mathfrak{A}\left(\frac{1}{p+1}, \frac{p}{p+1}\right)$ may be represented by a Laurent series in $\lambda-\beta$ with coefficients in $\mathbf{Q}_p(\beta)$ and hence the same holds for $\lambda''-\beta$. It follows from Lemma (8.11) (ii) that $\lambda''\in\mathfrak{N}_0$. However $G_p(\lambda, \lambda')=0=G_p(\lambda', \lambda'')$. The symmetry of G_p shows that λ' is a zero of both $G_p(\lambda, Y)$ and $G_p(\lambda'', Y)$, two monic polynomials in $\mathfrak{N}[Y]$ of degree $p+1$. It follows from equation (8.50) that the two polynomials must be identical and in particular by equating the coefficients of Y, we obtain by equation (7.10):

$$-\lambda+p\sum_{\mu=1}^{p} c_{\mu,1}\lambda^{\mu}=-\lambda''+p\sum_{\mu=1}^{p} c_{\mu,1}\lambda''^{\nu}.$$

Since λ and λ'' assume values in $\mathfrak{O}$, it is clear that $\lambda''=\lambda$ for all $\lambda\in C\left(\frac{1}{p+1}\right)$. This completes our treatment of statement (L) (which is of course weaker than the quoted result of Lubin).

We deduce an interesting consequence. Given $\varepsilon>0$, we may choose a field E, of finite degree over $\mathbf{Q}_p(\beta)$ with absolute ramification prime to $p+1$, such that the intersection of E with $\mathfrak{A}\left(\frac{p}{p+1}, \frac{p}{p+1}+\varepsilon\right)$ is infinite.

By choosing z in this intersection, the proof of equation (8.50) may be extended so that $\mathfrak{N}$ may be replaced by $\mathfrak{N}_\varepsilon$, the field of functions which are both meromorphic in $\mathfrak{A}\left(\frac{1}{p+1}, \frac{p}{p+1}+\varepsilon\right)$ and defined over $\mathbf{Q}_p(\beta)$. It follows that λ' cannot be meromorphic in this annulus for any $\varepsilon>0$. (An alternate proof of non-meromorphy follows from the fact that otherwise with the aid of Lemma (8.11) (ii) we would have $\chi^{(2)}$ meromorphic in $\beta+\mathfrak{P}$ and hence by part (iv) of that lemma would everywhere coincide with the identity mapping.)

Let V be the modular correspondence, i.e. the curve defined over $\mathbf{Q}$ by the equation

$$G_p(X, Y)=0.$$

We determine the singular locus of V and show that, contrary to what might be expected, the projections of that locus on the coordinate axes lie in the support of χ.

Lemma **(8.16).** — *Let* S *be the set of all points* $(\alpha_{can}, \alpha'_{can})$, *as* $\alpha \bmod \mathfrak{P}$ *runs through all elements of* $GF[p^2]$ *for which the Hasse invariant is not zero.*

(i) *The singular locus of* V *consists of the elements of* S *and the point at infinity.*

(ii) *Each element of* V *is of the form* (λ, λ') *or* (λ', λ).

(iii) *The zeros of* $d\lambda'/d\lambda$ *are at* $\lambda = 0, 1$.

(iv) *If one of the first derivatives of* G_p *vanishes at a point of* V *then the point lies in* S.

Proof. — It follows from equation (7.9) that we may restrict our attention to $\mathfrak{D}\times\mathfrak{D}$. Let us denote G_p by G and use G_i $(i = 1, 2)$ to denote the derivative of G with respect to the i-th variable. An elementary computation gives

$$\textbf{(8.52)} \qquad G_2(\lambda, \lambda')G_2(\lambda', \lambda'')d\lambda''/d\lambda = G_1(\lambda, \lambda')G_1(\lambda', \lambda'') = G_2(\lambda', \lambda)G_2(\lambda'', \lambda'),$$

the last equality being a consequence of the symmetry of G.

If $\alpha \bmod \mathfrak{P}$ lies in $GF[p^2]$ but is not a zero of the Hasse invariant then by equation (8.19) $d\lambda''/d\lambda$ assumes a non-unit value at $\lambda = \alpha_{can}$. Since $G_2(\alpha_{can}, \alpha'_{can})$ and $G_2(\alpha'_{can}, \alpha_{can})$ are conjugate over $\mathbf{Q}_p$ and $\alpha_{can} = \alpha''_{can}$, it follows from equation (8.52) that G_1 and G_2 vanish at each point of S, as asserted. The proof of (i) will be completed subsequently.

The proof of (iii) follows from Lemma (8.13) in the case of supersingular reduction and from equation (7.17) in the case of non-supersingular reduction if $\lambda \neq 0, 1$. The assertion for $\lambda = 0$ follows from equation (4.21) and for $\lambda = 1$ by the symmetry, $\lambda \mapsto 1 - \lambda$.

For fixed z we consider the equation

$$\textbf{(8.53)} \qquad \chi(Y) = z.$$

In all cases we know that this equation has at least p roots while if $\operatorname{ord}(z - \alpha) > 1/(p+1)$, $\alpha^{p^2} = \alpha$, $\alpha \bmod \mathfrak{P}$ supersingular, there are $p+1$ roots. It follows from (iii) that these roots are distinct. The roots of (8.53) are necessarily roots of

$$\textbf{(8.54)} \qquad G(z, Y) = 0$$

and in the case in which (8.53) has p roots we know that z' is also a root of (8.54). If z' is not a root of (8.53) then this gives $p+1$ distinct roots of (8.54) which verifies (ii) in that case and also shows that no singular point of V has z as first coordinate. In the supersingular case, if $\operatorname{ord}(z - \alpha) \leq 1/(p+1)$, we know that the p roots of (8.53) are further from α^p than is z' and hence (8.54) has $p+1$ distinct roots. In the non-supersingular case, if z' is a root of (8.53) then z must be the canonical lifting of an element of $GF[p^2]$. This shows that the singular locus of V in $\mathfrak{D}\times\mathfrak{D}$ lies in S and hence completes the proof of (i). If z is the first coordinate of an element of S then (8.54) has a multiple root and hence the p distinct roots of (8.53) give all the roots of (8.54). This completes the proof of (ii). Finally we note that (iv) follows from (ii), (iii), the symmetry of G and the relation:

$$0 = G_1(\lambda, \lambda') + G_2(\lambda, \lambda')d\lambda'/d\lambda.$$

This completes the proof of the lemma.

REFERENCES

[1] B. DWORK, Norm residue symbol in local number fields, *Abh. Math. Sem. Univ. Hamburg*, **22** (1958), pp. 180-190.

[2] —, On the zeta function of a hypersurface, *Publ. Math. I.H.E.S.*, **12** (1962), pp. 5-68.

[3] —, A deformation theory for the zeta function of a hypersurface, *Proc. Int. Cong. Math.*, Stockholm, 1962.

[4] —, On the zeta function of a hypersurface, II, *Annals of Math.*, **80** (1964), pp. 227-299.

[5] P. GRIFFITHS, *Periods of integrals of an algebraic manifold*, Notes, Univ. of Calif., Berkeley, 1966.

[6] —, On the period matrices and monodromy of homology in families of algebraic varieties, *Publ. Math. I.H.E.S.* (to appear).

[7] W. HODGE, *Theory and applications of harmonic integrals*, Cambridge, 1952.

[8] N. KATZ, On the differential equations satisfied by period matrices, *Publ. Math. I.H.E.S.*, **35** (1968), pp. 71-106.

[9] M. KRASNER, Prolongement analytique uniforme et multiforme dans les corps valués complets, *Colloque Int. C.N.R.S.*, n° 143, Paris, 1966.

[10] S. LANG and A. WEIL, Number of points of varieties in finite fields, *Amer. J. Math.*, **76** (1954), pp. 819-827.

[11] J. MANIN, The Hasse-Witt matrix of an algebraic curve, *Amer. Math. Soc. Translations*, ser. 2, **45** (1965).

[12] D. REICH, A p-adic fixed point formula, *Amer. J. Math.* (to appear).

[13] S. SHATZ, The cohomology of certain elliptic curves over local and quasi-local fields, *Ill. J. Math.*, **11** (1967).

[14] H. WEBER, *Lehrbuch der algebra*, vol. III, Chelsea Publ. Co., N. Y.

[15] A. GROTHENDIECK, Theorèmes de dualité pour les faisceaux algébriques cohérents, *Sem. Bourbaki*, n° 149 (1957).

[16] B. DWORK, On the rationality of the zeta function, *Amer. J. Math.*, **82** (1960), pp. 631-648.

[17] —, A deformation theory for singular hypersurfaces, *Proc. Int. Colloq. Alg. Geom.*, Tata Inst. Fund Res. Bombay, 1968.

[18] G. WASHNITZER, *Some properties of formal schemes*, Notes, Princeton Univ., 1963-1964.

[19] J.-P. SERRE, *Abelian l-adic representations and elliptic curves*, W. A. Benjamin, Inc., New York, 1968.

[20] D. N. CLARK, A note on the p-adic convergence of solutions of linear differential equations, *Proc. Amer. Math. Soc.*, **17** (1966), pp. 262-269.

[21] R. FRICKE, *Die Elliptischen Funktionen und ihre Anwendungen*, vol. II, Leipzig, 1922.

Manuscrit reçu le 9 avril 1969.

Correction. — In the statement of Lemma (7.3), the hypothesis (here paraphrased), " h is a biholomorphic map of $1+\mathfrak{P}$ onto itself " should be replaced by the weaker hypothesis, " h is a holomorphic map of $1+\mathfrak{P}$ into itself ".