CRYSTALLINE COHOMOLOGY, DIEUDONNÉ MODULES, AND JACOBI SUMS

By NICHOLAS M. KATZ

TABLE OF CONTENTS

Introduction. Hasse [20] and Hasse-Davenport [21] were the first to realize the connection between exponential sums over finite fields and the theory of zeta and L-functions of algebraic varieties over finite fields. This connection was exploited by Weil; one of the very first applications that Weil gave of the then newly proven "Riemann Hypothesis" for curves over finite fields was the estimation of the absolute value of Kloosterman sums (cf[46]). The basic idea (cf[20]) is that by using the theory of L-functions, one can express the negative of such an exponential sum as the sum of certain of the reciprocal zeroes of the zeta function itself; because the magnitude of these zeroes is given by the ''Riemann Hypothesis,'' one gets an estimate. In a fixed characteristic p, the estimate one gets in this way for all the finite fields $\mathbf{F}_{p^n}$ is best possible. On the other hand, very little is known about the variation with p of the absolute values, even for Kloosterman sums, though in this case there is a conjecture, of Sato-Tate type, which seems inaccessible at present.

One case in which the problem of unknown variation with p does not arise is when the expression of the exponential sum as a sum of reciprocal roots of zeta reduces to a sum consisting of a *single* reciprocal root; then the Riemann Hypothesis tells us the exact magnitude of the exponential sum. Conversely, an elementary argument shows that in a certain sense, this is the only case in which such exact knowledge of the magnitude of exponential sums can arise, and it shows further that a theorem of Hasse-Davenport type always results from such exact knowledge. Examples of exponential sums of this sort are Gauss sums and Jacobi sums.

Honda was the first to suggest that the identification of say, Jacobi sums, with reciprocal zeroes of zeta functions could also lead to significant non-archimedean information about Jacobi sums. A few years before his untimely death, Honda conjectured a p-adic limit formula for Jacobi sums in terms of ratios of binomial coefficients ([23]). I gave an overcomplicated proof (in a letter to Honda of Nov. 1971) which managed to shed no light whatever on the meaning of the formula. Recently, B.H. Gross and N. Koblitz [14] showed that Honda's limit formula was really an *exact* p-adic formula for Jacobi sums in terms of products of values of Morita's p-adic Γ-function; as such, it constituted the first improvement in this century over Stickelberger's formula which gave the

p-adic valuation and the *first* non-vanishing p-adic digit in the p-adic expansion of a Jacobi sum!

In this paper, I will discuss the cohomological genesis of formulas of the sort discovered by Honda. The basic idea is that the reciprocal zeroes of zeta are the eigenvalues of the Frobenius endomorphism of a suitable cohomology group; if this group, together with the action of Frobenius upon it, can be made sufficiently explicit, one obtains the desired "explicit formulas"

There are two approaches to the question, which differ more in style than in substance. The first and longer is based on Honda's explicit construction of the Dieudonné module of a formal group in terms of "formal de Rham cohomology". The second, less elementary but more efficient, is grounded in crystalline cohomology, particularly in the theory of the de Rham-Witt complex. I hope the reader will share my belief that there is something to be gained from each of the approaches, and pardon my decision to discuss both of them.

I would like to thank B. Dwork for many helpful discussions concerning the original proof of Honda's conjecture. Whatever I know of the Grothendieck-Mazur-Messing approach to Dieudonné theory through exotic Ext's, I was taught by Bill Messing. I would also like to thank Spencer Bloch for his encouragement when I was trying to understand Honda's explicit Dieudonné theory, and Luc Illusie for gently correcting some extravagent assertions I made at the Colloquium.

Finally, I would like to dedicate this paper to the memory of T. Honda.

I. Elementary Axiomatics, and the Hasse-Davenport Theorem.

Consider a projective, smooth and geometrically connected variety X, say of dimension d, over a finite field $\mathbf{F}_q$. For each integer $n \geq 1$, we denote by $X(\mathbf{F}_{q^n})$ the finite set of points of X with values in $\mathbf{F}_{q^n}$, and by $\# X(\mathbf{F}_{q^n})$ the cardinality of this set. The zeta function $Z(X/\mathbf{F}_q, T)$ of X over $\mathbf{F}_q$ is the formal power series in T with $\mathbf{Q}$-coefficients defined as

$$Z(X/\mathbf{F}_q, T) = \exp\Big(\sum_{n \geq 1} \frac{T^n}{n} \# X(\mathbf{F}_{q^n}) \Big).$$

Thanks to Deligne [6], we know that this zeta function has a unique expression as a finite alternating product of polynomials $P_i(T) \in \mathbf{Z}[T]$, $i = 0, \ldots, 2d$:

$$Z(X/\mathbf{F}_q, T) = \prod_{i=0}^{2d} P_i(T)^{(-1)^{i+1}} = \frac{P_1P_3\ldots P_{2d-1}}{P_0P_2\ldots P_{2d}}$$

in which each polynomial $P_i(T) \in \mathbf{Z}[T]$ is of the form

$$P_i(T) = \prod_{j=1}^{\deg P_i} (1 - \alpha_{i,j} T)$$

with $\alpha_{i,j}$ algebraic integers such that

$$|\alpha_{i,j}| = \sqrt{q}^{\,i}$$

for *any* archimedean absolute value $|\ \ |$ on the field $\bar{\mathrm{Q}}$ of all algebraic numbers. The extreme polynomials P_0, P_{2d} are given explicitly:

$$P_0(T) = (1-T) \quad , P_{2d}(T) = (1 - q^d \cdot T)$$

Despite this apparently "elementary" characterization of the polynomials $P_i(T)$, their true genesis is cohomological. Let us recall this briefly.

For each prime number l different from the characteristic p of $\mathbf{F}_q$, let us denote by $H_l^i(X)$ the finitely generated $\mathbf{Z}_l$-module defined as

$$H_l^i(X) = \varprojlim_n H^i_{\text{etale}}(X \otimes \bar{\mathbf{F}}_q, \mathbf{Z}/l^n\mathbf{Z}).$$

Corresponding to the prime p itself, we denote by $W(\mathbf{F}_q)$ the ring of p-Witt vectors of $\mathbf{F}_q$, and by $H^i_{\text{cris}}(X)$ the finitely generated $W(\mathbf{F}_q)$—module defined as

$$H^i_{\text{cris}}(X) = \varprojlim_n H^i_{\text{cris}}(X/W_n(\mathbf{F}_q)).$$

The Frobenius endomorphism F of X relative to $\mathbf{F}_q$ acts, by functoriality, on these various cohomology groups $H_l^i(X)$ for $l \neq p$, and $H^i_{\text{cris}}(X)$; and F induces automorphisms of the corresponding vector spaces $H_l^i(X) \underset{Z_l}{\otimes} Q_l$, $H^i_{\text{cris}}(X) \underset{W(F_q)}{\otimes} K$ (K denoting the fraction field of $W(\mathbf{F}_q)$). The polynomial $P_i(T) \in \mathbf{Z}[T]$ which occurs in the factorization of the zeta function is then given cohomologically by the formulas

$$P_i(T) = \det(1 - TF|H_l^i(X) \otimes \mathbf{Q}_l) \text{ for } l \neq p$$

$$P_i(T) = \det(1 - TF|H^i_{\text{cris}}(X) \otimes K).$$

The resulting formula for zeta as the alternating product of characteristic polynomials of F on the H^i , in each of the cohomology theories $H_l^i(X) \otimes Q_l$ for $l \neq p$, $H^i_{\text{cris}}(X) \otimes K$, is equivalent, via logarithmic differentiation, to the identities in those theories

$$\# X(\mathbf{F}_{q^n}) = \sum (-1)^i \operatorname{trace}(F^n|H^i). \text{ for all } n \geq 1.$$

By viewing the set $X(\mathbf{F}_{q^n})$ as the set of fixed points of F^n acting on $X(\bar{\mathbf{F}}_q)$, this identity becomes a Lefschetz trace formula

$$\# \operatorname{Fix}(F^n) = \sum (-1)^i \operatorname{trace}(F^n|H^i) \text{ all } n \geq 1$$

for F and its iterates in each of our cohomology theories. If we take as *given* these Lefschetz trace formulas, then the identification of P_i with $\det(1 - FT|H^i)$ is equivalent to the assertion:

> On any of the groups $H_l^i(X) \otimes Q_l$ with $l \neq p$, $H^i_{\text{cris}}(X) \otimes K$, the eigenvalues of F are algebraic integers all of whose archimedean absolute values are $\sqrt{q}^{\,i}$.

In fact, there is not a great deal more that is known about the action of F on the $H_l^i(X) \otimes Q_l$ for $l \neq p$, and on $H^i_{\text{cris}}(X) \otimes K$. It is still *not* known, for example, whether the action of F on these cohomology groups is always semi-simple when $i > 1$. (That it is when $i = 1$ results from the theory of abelian varieties).

Suppose that a finite group G operates on X by $\mathbf{F}_q$—automorphisms. Let us choose a number field E big enough that all complex representations of G are realizable over E, and whose residue fields at all p-adic places contain $\mathbf{F}_q$. (For example, the field $Q(\zeta_{q-1}, \zeta_N)$, where N is the *l*.c.m. of the orders of elements of G, is such an E). We denote by λ an l-adic place of E, $l \neq p$, and by P a p-adic place of E. Thus E_λ is a finite extension of Q_l, and E_P is a finite extension of K.

Let M be a finite dimensional E-vector space given with an action of G, say $\rho: G \to \operatorname{Aut}_E(M)$. The associated L-function $L(X/\mathbf{F}_q, \rho, T)$ is the formal power series with E-coefficients defined as

$$L(X/\mathbf{F}_q, \rho, T) = \exp\left(\sum_{n\geq 1} \frac{T^n}{n} \cdot \frac{1}{\#G} \sum_{g\in G} \mathrm{tr}(\rho(g^{-1})) \# \mathrm{Fix}(F^n g)\right)$$

where Fix $(F^n g)$ denotes the finite set of fixed points of $F^n g$ acting on $X(\overline{\mathbf{F}}_q)$. We recover the zeta function of $X/\mathbf{F}_q$ by taking for ρ the regular representation of G. The usual formalism of zeta and L-functions gives

$$Z(X/\mathbf{F}_q, T) = \prod_{\rho \text{ irred}} L(X/\mathbf{F}_q, \rho, T)^{\deg(\rho)}$$

It follows from Deligne's results that for any representation ρ, we have a unique expression for the corresponding L-function as an alternating product of polynomials $P_{i,\rho}(T) \in E[T]$,

$$L(X/\mathbf{F}_q, \rho, T) = \prod_{i=0}^{2d} P_{i,\rho}(T)^{(-1)^{i+1}},$$

which are of the form

$$P_{i,\rho}(T) = \prod_{j=1}^{\deg P_{i,\rho}} (1 - \alpha_{i,j,\rho} T)$$

with algebraic integers $\alpha_{i,j,\rho}$ such that

$$|\alpha_{i,j,\rho}| = \sqrt{q}^{\,i}$$

for any archimedean absolute value $|\ |$ on the field $\overline{Q}$ of all algebraic numbers.

The cohomological expression of these $P_{i,\rho}$ is straighforward (cf[18]). Because the action of G is "defined over $\mathbf{F}_q$", it commutes with F, and therefore the induced action of G on the cohomology commutes with the action of F. Therefore G, acting by composition, induces automorphisms of the E_λ-vector spaces, $l \neq \rho$,

$$\mathrm{Hom}_{E_\lambda[G]}(M \underset{E}{\otimes} E_\lambda, H^i_l(X) \underset{\mathbf{Z}_l}{\otimes} E_\lambda).$$

and of the E_p-vector spaces

$$\mathrm{Hom}_{E_p[G]}(M \underset{E}{\otimes} E_p, H^i_{\mathrm{cris}}(X) \underset{W(\mathbf{F}_q)}{\otimes} E_p).$$

The polynomials $P_{i,\rho}(T) \in E[T]$ are given by the formulas

$$P_{i,\rho}(T) = \det(1 - TF | \mathrm{Hom}_{E_\lambda[G]}(M \underset{E}{\otimes} E_\lambda, H^i_l(X) \underset{\mathbf{Z}_l}{\otimes} E_\lambda)) \text{ for } l \neq \rho$$

$$P_{i,\rho}(T) = \det(1 - TF | \mathrm{Hom}_{E_p[G]}(M \underset{E}{\otimes} E_p, H^i_{\mathrm{cris}}(X) \underset{W(\mathbf{F}_q)}{\otimes} E_p)).$$

Let us recall the derivation of these formulas. We first observe that the characteristic polynomial of F on $\mathrm{Hom}_G(M, H^i) \simeq (\check{M} \otimes H^i)^G \subset \check{M} \otimes H^i$ *divides* $\det(1 - FT | H^i)^{\dim(\check{M})}$, and hence the eigenvalues of F on $\mathrm{Hom}_G(M, H^i)$ are algebraic integers, all of whose archimedean absolute values are $\sqrt{q}^{\,i}$. So it remains only to verify that the alternating product of those characteristic polynomials is indeed the L-function, i.e. that

$$L(X/\mathbf{F}_q, \rho, T) = \prod \det(1 - FT | (\check{M} \otimes H^i)^G)^{(-1)^{i+1}},$$

Equivalently, we must check that

$$\frac{1}{\#G} \sum \mathrm{trace}\, \rho(g^{-1}) \# \mathrm{Fix}(F^n g)$$

$$= \sum (-1)^i \mathrm{trace}(1 \otimes F^n | (\check{M} \otimes H^i)^G)$$

$$= \sum (-1)^i \frac{1}{\#G} \sum_{g\in G} \mathrm{trace}(g \otimes F^n g | \check{M} \otimes H^i)$$

$$= \sum (-1)^i \frac{1}{\#G} \sum_{g\in G} \mathrm{trace}\, \check{\rho}(g) \cdot \mathrm{trace}(F^n g | H^i)$$

$$= \frac{1}{\#G} \sum_{g\in G} \mathrm{trace}\, \rho(g^{-1}) \sum (-1)^i \mathrm{trace}(F^n g | H^i).$$

To check this last equality, we would like to invoke the Lefschetz trace formula, not for F^n, but for $F^n g$, with g an automorphism of *finite order* which commutes with F; this amounts to invoking the Lefschetz trace formula for Fg on X and on all its "extensions of scalars" $X \otimes \mathbf{F}_{q^n}$. But an elementary descent argument shows that given an automorphism g of finite order which commutes with F, there is *another* variety $X'/\mathbf{F}_q$ together with an isomorphism $X \otimes \overline{\mathbf{F}}_q \simeq X' \otimes \overline{\mathbf{F}}_q$ under which $Fg \otimes 1$ corresponds to $F \otimes 1$. Because this isomorphism also induces isomorphisms of cohomology groups

$$H^i_l(X) \overset{\mathrm{dfn}}{=} H^i_{\mathrm{et}}(X' \otimes \overline{\mathbf{F}}_q, \mathbf{Z}_l) \simeq H^i(X \otimes \overline{\mathbf{F}}_q, \mathbf{Z}_l) \overset{\mathrm{dfn}}{=} H^i_l(X),$$

$$H^i_{\mathrm{cris}}(X') \otimes W(\overline{\mathbf{F}}_q) \simeq H^i_{\mathrm{cris}}(X' \otimes \overline{\mathbf{F}}_q) \simeq H^i_{\mathrm{cris}}(X \otimes \overline{\mathbf{F}}_q) \simeq$$

$$\simeq H^i_{\mathrm{cris}}(X) \otimes W(\overline{\mathbf{F}}_q),$$

the truth of the Lefschetz formula for Fg on X results from its truth for F on X′.

Let us now consider in greater detail the case of an irreducible ρ. Then $P_{i,\rho}$ is a polynomial whose degree is the common *multiplicity* of ρ in any of the $H^i_l(X) \otimes E_\lambda$, $l \neq \rho$, or in $H^i_{\text{cris}}(X) \otimes E_p$. Decomposing the regular representation leads to the factorization

$$P_i(T) = \prod_{\rho \text{ irred}} P_{i,\rho}(T)^{\deg(\rho)}$$

The coarser factorization

$$P_i(T) = \prod_{\rho \text{ irred}} (P_{i,\rho}(T)^{\deg(\rho)})$$

corresponds to the decomposition of $H^i_l(X) \otimes E_\lambda$, resp $H^i_{\text{cris}}(X) \otimes E_p$, into ρ-isotypical components

$$H^i_l(X) \otimes E_\lambda \simeq \bigoplus_{\text{irred } \rho} (H^i_l(X) \otimes E_\lambda)^\rho$$
$$H^i_{\text{cris}}(X) \otimes E_p \simeq \bigoplus_{\text{irred } \rho} (H^i_{\text{cris}}(X) \otimes E_p)^\rho$$

Indeed the corresponding identities, for ρ irreducible, are

$$P_{i,\rho}(T)^{\deg(\rho)} = \det(1 - TF|(H^i_l(X) \otimes E_\lambda)^\rho) \quad l \neq p$$
$$P_{i,\rho}(T)^{\deg(\rho)} = \det(1 - TF|(H^i_{\text{cris}}(X) \otimes E_p)^\rho).$$

Let us denote by $S(X/\mathbf{F}_q, \rho, n)$ the exponential sums used to define the L-function:

$$S(X/\mathbf{F}_q, \rho, n) = \frac{1}{\# G} \sum_{g \in G} \operatorname{tr}(\rho(g)) \# \operatorname{Fix}(F^n g^{-1}).$$

The following lemma gives the cohomological meaning of theorems of Hasse-Davenport type (cf [20]).

LEMMA 1.1. *Let $X/\mathbf{F}_q$ be projective and smooth. Let a finite group G operate on X by $\mathbf{F}_q$-automorphisms, and let ρ be an irreducible complex representation of G. Fix an integer i_o, and denote by H^{i_o} any one of the cohomology groups $H^{i_o}_l(X) \underset{\mathbf{Z}_l}{\otimes} E_\lambda$ with $l \neq p$, or $H^{i_o}_{\text{cris}}(X) \underset{W(\mathbf{F}_q)}{\otimes} E_p$. Let $|\ \ |$ be any archimedean absolute value on the field $\overline{Q}$ of all algebraic numbers. The following conditions are equivalent:*

(1) *The multiplicity of ρ in H^{i_o} is one, and the multiplicity of ρ in H^i is zero if $i \neq i_o$.*

(2) *For all $n \geq 1$, we have*

$$(-1)^{i_o} S(X/\mathbf{F}_q, \rho, n) = ((-1)^{i_o} S(X/\mathbf{F}_q, \rho, 1))^n,$$

and $$|S(X/\mathbf{F}_q, \rho, 1)| = \sqrt{q}^{\,i_o}$$

(3) *For all $n \geq 1$, we have*

$$|S(X/\mathbf{F}_q, \rho, n)| = \sqrt{q}^{\,i_o n}$$

(4) *For all $n \geq 1$, we have*

$$|S(X/\mathbf{F}_q, \rho, n)| = |S(X/\mathbf{F}_q, \rho, 1)|^n$$

and $$\sqrt{q}^{\,i_o} \leq |S(X/\mathbf{F}_q, \rho, 1)| < \sqrt{q}^{\,1+i_o}$$

(5) *The polynomial $P_{i_o,\rho}(T)$ is given by*

$$P_{i_o,\rho}(T) = 1 - (-1)^{i_o} S(X/\mathbf{F}_q, \rho, 1)T$$

and for $i \neq i_o$, we have $P_{i,\rho}(T) = 1$.

(6) *The ρ-isotypical component $(H^i)^\rho = 0$ for $i \neq i_o$, $(H^{i_o})^\rho$ has dimension $=$ $\deg(\rho)$, and F operates on $(H^{i_o})^\rho$ as the scalar $(-1)^{i_o} S(X/\mathbf{F}_q, \rho, 1)$.*

Proof. This is an easy exercise, using the basic identities:

$$\begin{cases} \exp\left(\sum \frac{T^n}{n} S(X/\mathbf{F}_q, \rho, n)\right) = L(X/\mathbf{F}_q, \rho, T) = \prod_i P_{i,\rho}(T)^{(-1)^{i+1}} \\ P_{i,\rho}(T) = \prod_j (1 - \alpha_{i,j,\rho} T), \ |\alpha_{i,j,\rho}| = \sqrt{q}^{\,i} \\ \deg P_{i,\rho} = \text{multiplicity of } \rho \text{ in } H^i = \frac{1}{\deg(\rho)} \cdot \dim((H^i)^\rho). \end{cases}$$

Suppose, first, that (1) holds, or equivalently that for $i \neq i_o$, $P_{i,\rho}(T) = 1$, while $P_{i_o,\rho}$ is a linear polynomial $P_{i_o,\rho}(T) = (1 - AT)$ with $|A| = \sqrt{q}^{\,i_o}$. The cohomological expression for L then becomes

$$\exp\left(\sum \frac{T^n}{n} S(X/\mathbf{F}_q, \rho, n)\right) = \left(\frac{1}{1 - AT}\right)^{(-1)^{i_o}}.$$

Taking logarithms and equating coefficients, we find

$$(-1)^{i_o} S(X/\mathbf{F}_q, \rho, n) = A^n \qquad \text{for all } n \geq 1.$$

In particular (2) and (5) hold.

The implications (5) ⇒ (1), (6) ⇒ (1) are obvious. Also (5) ⇒ (6), for if $P_{i_o,\rho}$ is linear, then ρ has multiplicity one in H^{i_o}, so that $(H^{i_o})^\rho$ is G-irreducible, and hence F must operate on $(H^{i_o})^\rho$ as a *scalar*, which we compute by the formula

$$P_{i_o,\rho}(T)^{\deg(\rho)} = \det(1 - TF|(H^{i_o})^\rho).$$

Clearly we have (2) ⇒ (3) ⇒ (4). We must show that if (4) holds, then exactly *one* of the $P_{i,\rho}$ is $\neq 1$, and that one is linear. Logarithmically differentiating the cohomological formula for L, we find

$$S(X/\mathbf{F}_q, \rho, n) = \sum_i (-1)^i \sum_{j=1}^{\deg P_{i,\rho}} (\alpha_{i,j,\rho})^n, \qquad |\alpha_{i,j,\rho}| = \sqrt{q}^{\,i}.$$

We must show that if (4) holds, then the double sum has only a single term in it. Separating the $\alpha_{i,j,\rho}$ according to the *parity* of i, we get two disjoint sets of non-zero complex numbers (disjoint because their absolute values are disjoint), to which we apply the following lemma.

Lemma 1.2. *Let $N \geq 0$ and $M \geq 0$ be non-negative integers. Let $\{A_i\}$ be a family of N not-necessarily distinct elements of C^x, and $\{B_i\}$ a family of M not-necessarily distinct elements of C^x. Suppose that for all i, j, $A_i \neq B_j$. If, for some real number $R > 0$, we have*

$$|\sum A_i^n - \sum B_j^n| = R^n \qquad \textit{for all } n \geq 1,$$

then $N + M = 1$, i.e. either there is just one A and no B's, or just one B and no A's.

Proof. Suppose first that either N = 0 or M = 0, say M = 0. Then we have

$$|\sum A_i^n| = R^n.$$

Squaring, we get

$$\sum_{i,j} (A_i \bar{A}_j)^n = (R^2)^n \qquad \text{for } n \geq 1$$

whence

$$\prod_{i,j} (1 - A_i \bar{A}_j T) = (1 - R^2 T),$$

and hence N = 1.

In case both N ≥ 1 and M ≥ 1, squaring leads to

$$\sum (A_i \bar{A}_k)^n + \sum (B_j \bar{B}_l)^n = (R^2)^n + \sum (A_i \bar{B}_j)^n + \sum (\bar{A}_i B_j)^n$$

or equivalently,

$$\frac{1}{(1 - R^2 T)} = \frac{\prod (1 - A_i \bar{B}_j T) \prod (1 - \bar{A}_i B_j T)}{\prod (1 - A_i \bar{A}_k T) \prod (1 - B_j \bar{B}_l T)}$$

Let $R_{\max}$ be $\max(|A_i|, |B_j|)$, and consider the order of pole at $T = R_{\max}^{-2}$. The numerator's factors $1 - A_i \bar{B}_j T$, $1 - \bar{A}_i B_j T$ are all non-zero there (for if $A_i \bar{B}_j = R^2_{\max}$, by maximality we must have $A_i = B_j = R_{\max}$, in which case we see, using polar coordinates, that $A_i = B_j$, which is forbidden). In the denominator, each of the terms $(1 - |A_i|^2 T)$, $(1 - |B_j|^2 T)$ with $|A_i| = R_{\max}$ and $|B_j| = R_{\max}$ vanishes at $T = R_{\max}^{-2}$. Therefore we may conclude that in fact $R = R_{\max}$, and that precisely *one* among all the A_i and B_j has this absolute value. A similar argument shows that $R_{\min} = R$. QED

In a similar but lighter vein, we have the following variant, whose proof is left to the reader.

Lemma 1.3. *Let $X/\mathbf{F}_q$ be projective and smooth. Let a finite group G operate on X by $\mathbf{F}_q$-automorphisms, and let ρ be an irreducible complex representation of G. Denote by H^i any of the cohomology groups $H^i_l(X) \underset{Z_l}{\otimes} E_\lambda$ with $l \neq p$, or $H^i_{\mathrm{cris}}(X) \underset{W}{\otimes} E_p$. The following conditions are equivalent.*

(1) *For all i, ρ does not occur in H^i, i.e. we have $(H^i)^\rho = 0$.*

(2) *For all $n \geq 1$, we have*

$$S(X/\mathbf{F}_q, \rho, n) = 0.$$

II. Gauss and Jacobi Sums as exponential sums, and as eigenvalues of Frobenius

We begin by discussing Gauss sums. Let us fix an integer $N \geq 2$ prime to p, and a number field E containing the Np'th roots of unity. Given an additive character ψ of $\mathbf{F}_p$, i.e. a homomorphism

$$\psi : (\mathbf{F}_p, +) \longrightarrow E^{\times},$$

we define an additive character ψ_q of each finite extension $\mathbf{F}_q$ by composing ψ with the trace map:

$$\begin{tikzcd} \mathbf{F}_q \arrow[r, "\mathrm{trace}_{\mathbf{F}_q/\mathbf{F}_p}"] \arrow[rr, bend right, "\psi_q"'] & \mathbf{F}_p \arrow[r, "\psi"] & E^{\times} \end{tikzcd}$$

Given a character of $\boldsymbol{\mu}_N$, i.e. a homomorphism

$$\chi : \boldsymbol{\mu}_N(E) \longrightarrow E^{\times},$$

a p-adic place P of E , with residue field $\mathbf{F}_{N(P)}$, and a finite extension $\mathbf{F}_q$ of this residue field, the map "reduction mod P" induces an isomorphism

$$\boldsymbol{\mu}_N(E) \xrightarrow{\sim} \boldsymbol{\mu}_N(\mathbf{F}_{N(P)}) = \boldsymbol{\mu}_N(\mathbf{F}_q)$$

Because $\mathbf{F}_q^{\times}$ is cyclic, we know that $q \equiv 1 \bmod N$, and that the map $x \longrightarrow x^{\frac{q-1}{N}}$ defines a surjection

$$\mathbf{F}_q^{\times} \twoheadrightarrow \boldsymbol{\mu}_N(\mathbf{F}_q) = \boldsymbol{\mu}_N(\mathbf{F}_{N(P)}) \simeq \boldsymbol{\mu}_N(E)$$

We define the character χ_q of $\mathbf{F}_q^{\times}$ as the composite

$$\begin{tikzcd} \mathbf{F}_q^{\times} \arrow[r, two heads] \arrow[rr, bend right, "\chi_q"'] & \boldsymbol{\mu}_N(\mathbf{F}_q) = \boldsymbol{\mu}_N(\mathbf{F}_{N(P)}) \simeq \boldsymbol{\mu}_N(E) \arrow[r, "\chi"] & E^{\times}. \end{tikzcd}$$

The Gauss sum $g_q(\psi, \chi, P)$ attached to this situation is defined by the formula

$$g_q(\psi, \chi, P) = \sum_{x \in \mathbf{F}_q^{\times}} \psi_q(x)\, \chi_q(x)$$

An elementary computation shows that

$$g_q(\psi, \chi, P) = \begin{cases} q-1 & \text{if } \psi, \chi \text{ both trivial} \\ 0 & \text{if } \psi \text{ trivial, } \chi \text{ non-trivial} \\ -1 & \text{if } \psi \text{ non-trivial, } \chi \text{ trivial} \end{cases}$$

while

$$|\, g_q(\psi, \chi, P)| = \sqrt{q} \quad \text{if } \psi, \chi \text{ both non-trivial}$$

for any archimedean absolute value on E (cf[47]).

Now consider the Artin-Schreier curve $X/\mathbf{F}_q$, defined to be the complete non-singular model of the affine smooth geometrically connected curve over $\mathbf{F}_q$ with equation

$$T^p - T = X^N.$$

Set theoretically, X consists of this affine curve plus a single rational point at ∞ . The group $\mathbf{F}_p \times \boldsymbol{\mu}_N(\mathbf{F}_q)$ operates on $X/\mathbf{F}_q$ curve by the affine formulas

$$(a, \zeta) : (T, X) \longrightarrow (T + a, \zeta X),$$

fixing the point at ∞ . Via the "reduction mod P" isomorphism

$$\boldsymbol{\mu}_N(E) \xrightarrow{\sim} \boldsymbol{\mu}_N(\mathbf{F}_{N(P)}) = \boldsymbol{\mu}_N(\mathbf{F}_q),$$

we may view (ψ, χ) as a character of the group $\mathbf{F}_p \times \boldsymbol{\mu}_N(\mathbf{F}_q)$:

$$(\psi, \chi)(a, \zeta) = \psi(a)\, \chi(\zeta).$$

Thus we may speak of the sums

$$S(X/\mathbf{F}_q, (\psi, \chi), n) = \frac{1}{pN} \sum_{(a,\zeta) \in \mathbf{F}_p \times \boldsymbol{\mu}_N} \psi(a)\, \chi(\zeta)\, \# \mathrm{Fix}(F^n \cdot (a, \zeta)^{-1})$$

attached to this situation.

LEMMA 2.1. *If χ is non-trivial and ψ is arbitrary, then we have*

(2.1.1) $$S(X/F_q, (\psi, \chi), n) = g_{q^n}(\psi, \chi, P).$$

Proof. It suffices to treat the case n = 1, for we have

$$S(X/\mathbf{F}_{q^n}, (\psi, \chi), 1) = S(X/\mathbf{F}_q, (\psi, \chi), n).$$

We can rewrite $S(X/\mathbf{F}_q, (\psi, \chi), 1)$ as

$$\sum_{x \in X(\overline{F}q)} \frac{1}{pN} \sum_{\substack{(a,\zeta) \text{s.t.} \\ F(x) = (a,\zeta)(x)}} \psi(a)\chi(\zeta)$$

Given any point $x \in X(\overline{\mathbf{F}}_q)$, the set of $(a,\zeta) \in \mathbf{F}_p \times \mu_N$ which satisfy $F(x) = (a,\zeta)(x)$ is either empty or principal homogeneous under the inertia *subgroup* I_x of $\mathbf{F}_p \times \mu_N$ which *fixes* x; therefore if the restriction of (ψ, χ) to this subgroup is *non-trivial*, the inner sum above *vanishes*. Because χ is assumed *non-trivial*, this vanishing applies to the point at ∞ (for which I_x is all of $\mathbf{F}_p \times \mu_N$) and to any finite point (T,0) whose X-coordinate is zero (then $I_{(T,0)} = \{0\} \times \mu_N$).

Given a point (T,X) with $X \neq 0$, we have

$$F(T,X) = (T^q, X^q)$$

and the inertia subgroup $I_{(T,X)}$ is trival. If there is an element $(a, \zeta) \in \mathbf{F}_p \times \mu_N$ satisfying $F(T,X) = (T + a, \zeta X)$, then it is given by the formulas

$$a = T^q - T, \zeta = X^{q-1}$$

Since the point (T,X) is subject to the defining equation

$$T^P - T = X^N$$

we see that

$$(X^N)^{q-1} = (X^{q-1})^N = \zeta^N = 1, \text{ hence } X^N \in \mathbf{F}_q^\times, \zeta = (X^N)^{\frac{q-1}{N}}$$

$$T^P - T = X^N \in \mathbf{F}_q^\times,$$

$$a = T^q - T = \text{trace}_{F_q/F_p}(T^p - T) = \text{trace}_{F_q/F_p}(X^N).$$

For each $u \in \mathbf{F}_q^\times$, the equations $(T^P - T = u, X^N = u)$ have pN solutions (T,X) over $\overline{\mathbf{F}}_q$, all of which satisfy

$$F(T,X) = (a,\zeta)(T,X)$$

with the *same* (a,ζ), namely $(\text{trace}_{F_q/F_p}(u), u^{\frac{q-1}{N}})$, and *every* point (T,X) which contributes to our sum lies over some $u \in \mathbf{F}_q^\times$. Thus our sum becomes

$$\sum_{u \in Fq^\times} \psi(\text{trace}_{F_q/F_p}(u))\chi(u^{\frac{q-1}{N}})^{\text{dfn}} \; g_q(\psi, \chi, P) \cdot \text{QED}$$

Corollary 2.2. *Let H^i denote any of the cohomology groups $H^i_l(X) \otimes E_\lambda$ with $l \neq p$, or $H^i_{\text{cris}}(X) \underset{W}{\otimes} E_p$ of the Artin-Schreier curve X/F_q.*

(1) If ψ and χ are both non-trivial, then the eigenspace $(H^1)^{\psi \cdot \chi}$ is one-dimensional, and we have a direct sum decomposition

$$H^i = \oplus (H^1)^{\psi \cdot \chi}$$

indexed by the $(p-1\,(N-1)$ pairs (ψ, χ) of non-trivial characters.

(2) The eigenvalue of F on $(H^1)^{\psi \cdot \chi}$ is $-g_q(\psi, \chi, P)$, and for each $n \geq 1$ we have the Hasse-Davenport formula

$$-g_{q^n}(\psi, \chi, P) = (-g_q(\psi, \chi, P))^n.$$

(3) The group $F_q \times \mu_N$ acts trivially on both H^0 and H^2.

Proof. That the group acts trivially on both H^0 and H^2 follows from the fact that these are one-dimensional spaces on which F always acts as 1 and q respectively. The descent argument shows that for any automorphism of *finite order* g which commutes with F, Fg also acts as 1 and q on H^0 and H^2 respectively, and hence that g itself acts trivially on H^0 and H^2.

That the multiplicity of (ψ, χ) in H^1 is *one* when both ψ and χ are non-trivial follows from the lemma of the previous section, given the identity (2.1.1) and the known absolute value of gauss sums; and assertion (2) above is just a repetition of part of that lemma in this particular case. To see that no other characters occur in H^1, we recall that the dimension of H^1 is known to be 2g, g = genus of X, and so it suffices to verify that $2g = (p-1)\,(N-1)$. This formula, whose elementary verification we leave to the reader, is in fact valid in any characteristic prime to $N(p-1)$. (Hint: view $T^P - T = X^N$ as an N-fold covering of the T-line!)

QED

We now turn to the consideration of Jacobi sums. We fix an integer $N \geq 2$ prime to p, and a number field E containing the N'th roots of unity. Given a p-adic place P of E, a character χ of μ_N

$$\chi : \mu_N(E) \longrightarrow E^{\times}$$

and a finite extension $\mathbf{F}_q$ of the residue field $\mathbf{F}_{N(P)}$ at P, we obtain the character χ_q

$$\chi_q : \mathbf{F}_q^{\times} \longrightarrow E^{\times}$$

in the manner explained above. Given two characters χ, χ' of μ_N, the Jacobi sum $J_q(\chi,\chi',P)$ is defined by the formula

$$J_q(\chi,\chi',P) \overset{\text{dfn}}{=} \sum_{\substack{x \in Fq \\ x \neq 0,1}} \chi_q(x)\chi'_q(1-x).$$

An elementary computation (cf [14]) shows that if the *product* $\chi\chi'$ is non-trivial, then for any non-trivial additive character ψ of $\mathbf{F}_p$, we have the formula

$$g_q(\psi,\chi,P)g_q(\psi,\chi',P) = J_q(\chi,\chi',P)g_q(\psi,\chi\chi',\ P)$$

In particular, from the known absolute values of Gauss sums we obtain

$$|\, J_q(\chi,\chi',p) \,| = \sqrt{q}$$

for all archimedean absolute values of E, provided that χ,χ', and $\chi\chi'$ are *all* non-trivial.

Now consider the Fermat curve $Y/\mathbf{F}_q$, defined by the homogeneous equation

$$X^N + Y^N = Z^N$$

The group $\mu_N \times \mu_N$ operates on this curve by the formula

$$(\zeta_1,\zeta_2):(X,Y,Z) \longrightarrow (\zeta_1 X, \zeta_2 Y, Z).$$

Viewing (χ,χ') as a character of this group

$$(\chi,\chi')(\zeta_1,\zeta_2) \overset{\text{dfn}}{=} \chi(\zeta_1)\chi'(\zeta_2),$$

we may speak of the sums $S(Y/\mathbf{F}_q, (\chi,\chi'),n)$ attached to this situation.

In complete analogy with the situation for the Artin-Schreier curve, we have the following lemma and corollary, whose analogous proofs are left to the reader.

LEMMA 2.3. *If χ and χ' are non-trivial characters of μ_N such that $\chi\chi'$ is also non-trivial, then we have, for all $n \geq 1$,*

$$(2.3.1) \qquad S(Y/F_q,(\chi,\chi'),n) = J_{q^n}(\chi,\chi',p).$$

COROLLARY 2.4. *Let H^i denote any of the cohomology groups $H^i_l(Y) \otimes E_\lambda$ with $l \neq p$, or $H^i_{\text{cris}}(X) \underset{W}{\otimes} E_P$ of the Fermat curve Y/F_q.*

(1) If χ, χ' and $\chi\chi'$ are all non-trivial, then the eigenspace $(H^1)^{(\chi,\chi')}$ is one-dimensional, and we have a direct sum decomposition

$$H^1 = \oplus (H^1)^{(\chi,\chi')}$$

indexed by the $(N-1)\ (N-2)$ pairs (χ,χ') of non-trivial characters of μ_N whose product $\chi\chi'$ is also non-trivial.

(2) The eigenvalue of F on $(H^1)^{(\chi,\chi')}$ is $-J_q\ (\chi,\chi',P)$, and for each integer $n \geq 1$ we have the Hasse-Davenport formula

$$-J_{q^n}(\chi,\chi',P) = (-J_q(\chi,\chi',P))^n.$$

(3) The group $\mu_N \times \mu_N$ operates trivally on both H^0 and H^2.

III. The problem of "explicitly" computing Frobenius. We return now to the general setting of a projective, smooth, and geometrically connected variety $X/\mathbf{F}_q$ of dimension d. A tantalizing feature of all the cohomology theories that we have been discussing is that when the variety X "lifts" to characteristic zero, then the corresponding cohomology groups $H^i(X)$ have an "elementary" description in terms of standard algebro-geometric and topological invariants of the lifting.

More precisely, suppose we are given a projective smooth scheme **X** over $W(\mathbf{F}_q)$, together with an $\mathbf{F}_q$-isomorphism of its special fibre with X. (This is a rather strong notion of what a "lifting" of X should mean, but it is adequate for our purposes, and it avoids certain technical problems related to ramification). Then there is a canonical isomorphism

$$H^i_{\text{cris}}(X) \longrightarrow H^i_{DR}(\mathbf{X}/W(\mathbf{F}_q))$$

of H^i_{cris} with the algebraic de Rham cohomology of the lifting (cf[19], [27]).

To discuss $H^i_l(X)$, we must in addition choose (!) a complex embedding

$$W(F_q) \hookrightarrow C.$$

By means of such an embedding, we may "extend scalars" to obtain from X/W a projective smooth complex variety X_C, and an associated complex manifold X_C^{an}. For each prime number $l \neq p$, there is a canonical isomorphism

$$H^i_l(X) \longrightarrow H^i_{\text{top}}(X_C^{an}, Z) \otimes_Z Z_l,$$

where H^i_{top} denotes the usual "topological" cohomology.

To emphasize the similarity between these two sorts of isomorphisms, we have a recall that by GAGA and the holomorphic Poincaré lemma, we have a canonical isomorphism

$$\begin{tikzcd}
H^i_{DR}(X/W) \otimes_W C \arrow[r, "\sim"] & H^i_{DR}(X/C) \arrow[r, "\sim"] & H^i_{\text{top}}(X_C^{an}, C) \\
 & & H^i_{\text{top}}(X^{an}, Z) \otimes_Z C \arrow[u, "\wr"]
\end{tikzcd}$$

Unfortunately, these rather concrete descriptions of the various cohomology *groups* $H^i(X)$ shed little light on their *functoriality*. In the rather unusual case of an F_q-endomorphism $f : X \longrightarrow X$ which happens to admit a lifting to a W-endomorphism

$$f : X \longrightarrow X,$$

we have the simple formulas

$$\begin{cases} f^* \text{ on } H^i_{\text{cris}}(X) = f^* \text{ on } H^i_{DR}(X/W) \\ f^* \text{ on } H^i_l(X) = (f_C^{an})^* \otimes 1 \text{ on } H^i_{\text{top}}(X_C^{an}, Z) \otimes_Z Z_l,\ l \neq p \end{cases}$$

But for those f which do not lift, we are left somewhat in the dark as to an explicit description of the map f^* on cohomology.

Suppose for example that a finite group G operates on X by F_q-automorphisms, and that this action can be lifted to an action of G on X by W-automorphisms. Then our canonical isomorphisms

$$\begin{cases} H^i_{\text{cris}}(X) \xrightarrow{\sim} H^i_{DR}(X/W) \\ H^i_l(X) \xrightarrow{\sim} H^i_{\text{top}}(X_C^{an}, Z) \otimes Z_l \text{ for } l \neq p \end{cases}$$

are G-equivariant. In particular, we can "explicitly compute" the multiplicities of the various complex irreducible representations ρ of G in the cohomology of X, and we can "explicitly compute" the various isotypical components of the cohomology. If it turns out that a given irreducible representation ρ occurs in a given H^i with multiplicity *one*, then we know a priori that F must operate on the corresponding isotypical component $(H^i)^\rho$ as a *scalar*, and we know this even when F itself does not lift.

For example, we could recover the isotypical decomposition of H^1 of the Fermat curve Y under the action of $\mu_N \times \mu_N$ by lifting the curve and the group action (use the "same" equations) and making an explicit algebro-geometric or topological calculation of the corresponding isotypical decomposition in characteristic zero. In terms of, say, the crystalline cohomology, we obtain an F-stable decomposition

$$H^1_{\text{cris}}(Y) \xrightarrow{\sim} H^1_{DR}(Y/W) = \oplus H^1_{DR}(Y/W)^{(\chi,\chi')};$$

in a basis of $H^1_{DR}(Y/W)$ adapted to this decomposition, the matrix of F is the diagonal matrix

$$\begin{pmatrix} \ddots & & O \\ & -J_q(\chi,\chi',P) & \\ O & & \ddots \end{pmatrix}$$

However, it must be borne in mind that the Fermat curve is atypically susceptible to this sort of analysis; it is unusual for a group action, even on a curve, to be liftable to characteristic zero. For example, the action of F_p on an Artin-Schreier covering of A^1 doesn't lift to characteristic zero. To get around this non-liftability, we will be led to consider the Washnitzer-Monsky cohomology as well, in Chapter VII.

IV. H^1 and abelian varieties; preliminaries. Consider an abelian variety A/F_q, say of dimension g. We denote by End(A) the ring of all F_q-endomorphisms of A, and by $\text{End}(A)^0$ the opposite ring. As Z-modules, they are free and finitely generated. For each prime $l \neq p$, the cohomology group $H^1_l(A)$ is a free $\mathbf{Z}_l$-module of rank 2g, and is an $\mathrm{End}\,(A)^0$ -module. (It is also the case that $H^1_{\mathrm{cris}}(A)$ is a free W-module of rank 2g, and is an $\mathrm{End}(A)^0$-module, but we will not make use of this fact for the moment).

Lemma *4.1. If E is a number field, and λ is a place of E lying over a prime $l \neq p$, the natural maps*

$$\begin{tikzcd} End(A)^0 \underset{\mathbf{Z}}{\otimes} E \arrow[r] & End(A)^0 \underset{\mathbf{Z}}{\otimes} E_\lambda \arrow[r] & End_{\mathbf{Z}_l}(H^1_l(A)) \underset{\mathbf{Z}_l}{\otimes} E_\lambda \\ & & End_{E_\lambda}(H^1_l(A) \underset{\mathbf{Z}_l}{\otimes} E_\lambda) \arrow[u, "\wr"'] \end{tikzcd}$$

are all injective.

Proof. The first map is injective simply because $E \subset E_\lambda$, and because $\mathrm{End}\,(A)^0$ is flat over $\mathbf{Z}$. The second map is obtained from the map

$$\mathrm{End}(A)^0 \underset{\mathbf{Z}}{\otimes} \mathbf{Z}_l \longrightarrow \mathrm{End}_{\mathbf{Z}_l}(H^1_l(A))$$

by tensoring over $\mathbf{Z}_l$ with the flat $\mathbf{Z}_l$-module E_λ. In fact this flatness is irrelevant, for the above map is injective and has $\mathbf{Z}_l$-flat cokernel. To see this, recall that (by the Kummer sequence in etale cohomology) we have a canonical isomorphism

$$H^1_l(A) \simeq T_l(\mathrm{Pic}^0(A))\,(-1) \simeq \mathrm{Hom}(T_l(A), \mathbf{Z}_l),$$

under which the map considered above is the "opposite" of the map

$$\mathrm{End}(A) \underset{\mathbf{Z}}{\otimes} \mathbf{Z}_l \longrightarrow \mathrm{End}_{\mathbf{Z}_l}(T_l(A))$$

Our assertion of its injectivity with $\mathbf{Z}_l$-flat cokernel is equivalent to the injectivity of (any one of) the maps

$$\mathrm{End}(A)/l^n\mathrm{End}(A) \longrightarrow \mathrm{End}(A_{l^n}),$$

and this injectivity follows from the exactness of the sequence

$$0 \longrightarrow A_{l^n} \longrightarrow A \xrightarrow{l^n} A \longrightarrow 0$$

in the etale topology. QED

Now consider a projective, smooth and geometrically connected variety $X/\mathbf{F}_q$. Its Albanese variety Alb(X) is an abelian variety over $\mathbf{F}_q$ which for our purposes is best viewed as the *dual* of the Picard variety variety Pic(X), itself defined in terms of the Picard scheme $\mathrm{Pic}_{X/\mathbf{F}_q}$ as $(\mathrm{Pic}^0{}_{X/\mathbf{F}_q})^{\mathrm{red}}$. The Kummer sequence in etale cohomology together with the duality of abelian varieties gives isomorphisms for each $l \neq p$

$$H^1_l(X) \xrightarrow{\sim} T_l(\mathrm{Pic}(X))\,(-1) \tag{4.1.1}$$

$$H^1(\mathrm{Alb}(X)) \xrightarrow{\sim} T_l(\mathrm{Pic}(\mathrm{Alb}(X))\ )(-1) = T_l(\mathrm{Pic}(X))(-1) \tag{4.1.2}$$

which combine to give a canonical isomorphism

$$H^1_l(X) \simeq H^1_l(\mathrm{Alb}(X)) \qquad \text{for } l \neq p \tag{4.1.3}$$

Suppose now that a finite group G operates on X by $\mathbf{F}_q$ -automorphisms. Let ρ be an absolutely irreducible representation of G defined over a number field E, which occurs in $H^1(X)$ with multiplicity r. Denote by

$$P_{1,\rho}(T) = 1 + a_1(\rho)T + \ldots. + a_r(\rho)T^r \in \mathcal{O}_E\,[T]$$

the reversed characteristic polynomial of F acting on the space $\mathrm{Hom}_G(\rho, H^1(X))$ of occurrences of ρ in H^1;

$$P_{1,\rho}(T) = \det(1 - TF|\mathrm{Hom}_G(\rho, H^1(X)).$$

Let us denote by $\mathrm{Proj}(\rho) \in \mathcal{O}_E\ [1/\#G]\,[G]$ the projector

$$\mathrm{Proj}(\rho) = \frac{\deg(\rho)}{\#G} \sum_{g \in G} \mathrm{tr}(\rho(q^{-1}))\cdot[g]\,\cdot$$

By functoriality, G also operates on Alb(X) by $\mathbf{F}_q$ -automorphisms, so we may view $\mathrm{Proj}(\rho)$, or indeed any element of the $\mathcal{O}_E\ [1/\#G]$ – group ring of G, as defining an element of $\mathrm{End}\,(\mathrm{Alb}(X)) \otimes \mathcal{O}_E\ [1/\#G]$.

Proposition *4.2. In the above situation, we have the formula*

$$(F^r + a_1(\rho)F^{r-1} + \ldots. + a_r(\rho))\cdot \mathrm{Proj}(\rho) = 0$$

$$\mathrm{Proj}(\rho)\cdot(F^r + a_1(\rho)F^{r-1} + \ldots. + a_r(\rho)) = 0$$

in $End(Alb(X)) \otimes \mathcal{O}_E\ [1/\#G]$. (N.B. since F and G commute, these formulas are equivalent).

Proof. Since $\mathrm{End}(\mathrm{Alb}(X)) \otimes \mathcal{O}_E\ [1/\#G]$ is contained in $\mathrm{End}(\mathrm{Alb}(X)) \otimes E$, which is in turn contained in $\mathrm{End}(H^1_l(\mathrm{Alb}(X)) \underset{\mathbf{Z}}{\otimes} E_\lambda)$

for any $l \neq p$, it suffices to verify that $F^r + a_1(\rho)F^{r-1} + \ldots + a_r(\rho)$ annihilates $(H^1(Alb(X))^\rho$. But this space is isomorphic to $(H^1(X))^\rho$, which is in turn isomorphic to $\rho \otimes Hom_G(\rho, H^1(X))$, with F acting through the second factor, so we need the above polynomial in F to annihilate $Hom_G(\rho, H^1(X))$. This follows from the Cayley-Hamilton theorem. QED

COROLLARY 4.3. *Let D be any contravariant additive functor from the category of abelian varieties over F_q to the category of $\mathcal{O}_E$ [1/# G]-modules. For any element $m \in (D(Alb(X)))^\rho$, we have*

$$F^r(m) + a_1(\rho)F^{r-1}(m) + \ldots + a_r(\rho) \cdot m = 0$$

in $D(Alb(X))$.

We will apply this to the functor "Dieudonne module of the formal group of A," constructed a la Honda.

V. Explicit Dieudonné Theory à la Honda; generalities

5.1. BASIC CONSTRUCTIONS. We begin by recalling the notions of formal Lie variety and formal Lie groups. Over any ring R, an n-dimensional formal Lie variety V is a set-valued functor on the category of adic R-algebras which is isomorphic to the functor.

$$R' \longrightarrow \text{n-tuples of topologically nilpotent elements of } R'.$$

A system of coordinates $X_1, \ldots, X_n$ for V is the choice of such an isomorphism. The coordinate ring A(V) is the R-algebra of all maps of set-functors from V to the "identical functor" $R' \longmapsto R'$; in coordinates, A(V) is just the power series ring $R[[X_1, \ldots, X_n]]$. Although the ideal $(X_1, \ldots, X_n)$ in A(V) is *not* intrinsic, the adic topology it defines on A(V) is intrinsic, and A(V), viewed as an adic R-algebra, represents the functor V.

The de Rham cohomology groups $H^i_{DR}(V/R)$ are the R-modules obtained by taking the cohomology groups of the formal de Rham complex $\Omega^\bullet_{V/R}$ (the separated completion of the "literal" de Rham complex of A(V) as R-algebra); in terms of coordinates $X_1, \ldots, X_n$ for V, $\Omega^\bullet_{V/R}$ is the exterior algebra over A(V) on $dX_1, \ldots, dX_n$, with exterior differentiation $d: \Omega^i \longrightarrow \Omega^{i+1}$ given by the customary formulas.

A pointed formal Lie variety (V,0) over R is a formal Lie variety V over R together with a marked point "0" $\in$ V(R). A formal Lie group G over R is a "group-object" in the category of formal Lie varieties over R.

We denote by CFG(R) the additive category of commutative formal Lie groups over R. The "sum" map

$$\text{sum}: G \times G \longrightarrow G$$

as well as the two projections

$$pr_1, pr_2 : G \times G \longrightarrow G$$

are morphisms in this category. For $G \in CFG(R)$, we define $\mathbf{D}(G/R)$ to be the R-submodule of $H^1_{DR}(G/R)$ consisting of the primitive elements, i.e. the elements $a \in H^1_{DR}(G/R)$ such that

$$\text{sum}^*(a) = pr_1^*(a) + pr_2^*(a) \text{ in } H^1_{DR}((G \times G)/R).$$

LEMMA 5.1.1. *Over any ring R, the construction $G \longrightarrow \mathbf{D}(G/R)$ defines a (contravariant) additive functor from CFG(R) to R-modules.*

Proof. This is a completely "categorical" result. To begin, let $G, G' \in CFG(R)$, and let $f: G' \longrightarrow G$ be a homomorphism. Then the diagram

$$\begin{tikzcd} G' \times G' \arrow[r, "\text{sum}"] \arrow[d, "f \times f"] & G' \arrow[d, "f"] \\ G \times G \arrow[r, "\text{sum}"] & G \end{tikzcd}$$

commutes, as do the analogous diagrams with "sum" replaced by pr_1 or pr_2. Therefore given any element $a \in H^1_{DR}(G/R)$, we have

$$\text{sum}^*(f^*(a)) - pr_1^*(f^*(a)) - pr_2(f^*(a)) =$$

$$(f \times f)^*(\text{sum}^*(a) - pr_1^*(a) - pr_2^*(a)).$$

In particular, if $a \in \mathbf{D}(G/R)$ then $f^*(a) \in \mathbf{D}(G'/R)$.

Given f_1, f_2 homomorphisms $G' \longrightarrow G$, let f_3 be their sum. Then we have a commutative diagram

$$\begin{tikzcd} G' \arrow[r, "f_1 \times f_2"] \arrow[rr, bend right, "f_3"'] & G \times G \arrow[r, "\mathrm{sum}"] & G \end{tikzcd}$$

as well as a commutative diagram

$$\begin{tikzcd} G' \arrow[r, "f_1 \times f_2"] \arrow[rr, bend left=60, "f_1"] \arrow[rr, bend right=60, "f_2"'] & G \times G \arrow[r, shift left, "\mathrm{pr}_1"] \arrow[r, shift right, "\mathrm{pr}_2"'] & G \end{tikzcd}$$

Therefore for any a $\in H^1_{DR}(G/\mathbf{R})$, we have

$$f_3^*(a) - f_1^*(a) - f_2^*(a) = (f_1 \times f_2)^*(\mathrm{sum}^*(a) - \mathrm{pr}_1^*(a) - \mathrm{pr}_2^*(a)).$$

In particular, if a $\in \mathbf{D}(G/R)$, then $f_3^*(a) = f_1^*(a) + f_2^*(a)$. QED

For the remainder of this section, we will consider a ring R which is flat over **Z**, and an ideal I $\subset$ R which has divided powers. The flatness means that if we denote by K the **Q**-algebra R $\otimes$ **Q**, then R $\subset$ K. That the ideal I $\subset$ R has divided powers means that for any integer n $\geq$ 1, and any element i $\in$ I, the element $i^n/n!$ of K actually lies in I.

Given a formal Lie variety V over R, we denote by V $\otimes$ K the formal Lie variety over K obtained by extension of scalars. In terms of coordinates $X_1, \dots, X_n$ for V, A(V $\otimes$ K) is the power-series ring $K[[X_1, \dots, X_n]]$. We say that an element of A (V $\otimes$ K) is *integral* if it lies in the subring A(V); similarly, an element of the de Rham complex $\Omega_{V \otimes K/K}$ is said to be *integral* if it lies in the subcomplex $\Omega_{V/R}$.

LEMMA 5.1.2. *Let (V,0) be a pointed Lie variety over a* **Z***-flat ring R. Then exterior differentiation induces an isomorphism of R-modules*

$$\frac{\{f \in A(V \otimes K) | f(0) = 0, df \text{ integral}\}}{\{f \in A(V) | f(0) = 0\}} \xrightarrow{\sim} H^1_{DR}(V/R)$$

which is compatible with morphisms of pointed Lie varieties.

Proof. Because K is a **Q**-algebra, the formal Poincare lemma gives $H^0_{DR}(V \otimes K/K) = K$, $H^i_{DR}(V \otimes K/K) = 0$ for $i \geq 1$. Therefore any closed one-form on V/R can be written as df with f $\in$ A(V $\otimes$ K), and this f is unique up to a constant. If we normalize f by the condition f(0) = 0, we get the asserted isomorphism. QED

KEY LEMMA 5.1.3. *Let (V,0) and (V′,0) be pointed formal Lie varieties over a* **Z***-flat ring R, and let I $\subset$ R be an ideal with divided powers. If f_1, f_2 are two pointed morphisms V′ ⟶ V such that $f_1 = f_2$ mod I, then the induced maps*

$$f_1^*, f_2^* : H^1_{DR}(V/R) \longrightarrow H^1_{DR}(V'/R)$$

are equal.

Proof. Let φ_1, φ_2 denote the algebra homomorphisms A(V) → A(V′) corresponding to f_1 and f_2. By the previous lemma, we must show that for every element f $\in$ A(V $\otimes$ K) with f(0) = 0 and df integral, the difference $\varphi_1(f) - \varphi_2(f)$ lies in A(V′), i.e. is itself integral. (Because f_1 and f_2 were assumed pointed, this difference automatically has constant term zero).

In terms of pointed coordinates $X_1, \dots, X_n$ for V′ and $Y_1, \dots, Y_m$ for V, the maps φ_1 and φ_2 are given by substitutions

$$\varphi_1(f(Y)) = f(\varphi_1(X))$$

$$\varphi_2(f(Y)) = f(\varphi_2(X))$$

where $\varphi_1(X)$, $\varphi_2(X)$ are m-tuples of series in $X = (X_1, \dots, X_n)$ without constant term. The hypothesis $f_1 = f_2$ mod I means that the component-by-component difference $\Delta = \varphi_2(X) - \varphi_1(X)$ satisfies

$$\Delta(0) = 0, \Delta \text{ has all coefficients in I.}$$

We now compute using Taylor's formula, and usual multi-index notation :

$$\begin{aligned} \varphi_2(f) - \varphi_1(f) &= f(\varphi_2(X)) - f(\varphi_1(X)) \\ &= f(\varphi_1(X) + \Delta) - f(\varphi_1(X)) \\ &= \sum_{|\underline{n}| \geq 1} \frac{\Delta^{\underline{n}}}{(\underline{n})!} \left(\frac{\partial^{\underline{n}}}{\partial Y^{\underline{n}}} f\right)(\varphi_1(X)). \end{aligned}$$

This last sum is X-adically convergent (because Δ has no constant term), and its individual terms are integral (because Δ has coefficients in the divided power ideal I, the terms $\Delta^{\underline{n}}/(\underline{n})!$ all have coefficients in I, and hence in R; because df is integral, all the first partials $\partial f/\partial Y_i$ are integral, and a fortiori all the higher partials are integral). QED

THEOREM 5.1.4. *Let R be a $\mathbf{Z}$–flat ring, and $I \subset R$ a divided power ideal. Let G, G' be commutative formal Lie groups over R, and denote by G_0, G'_0 the commutative formal Lie groups over $R_0 = R/I$ obtained by reduction mod I.*

1) If $f: G' \to G$ is any morphism of pointed formal Lie varieties whose reduction mod I, $f_0: G'_0 \to G_0$, is a group homomorphism, then the induced map $f^*: H^1_{DR}(G/R) \to H^1_{DR}(G'/R)$ maps $\mathbf{D}(G/R)$ to $\mathbf{D}(G'/R)$.
(2) If f_1, f_2, f_3 are three maps $G' \longrightarrow G$ of pointed formal Lie varieties whose reductions mod I are group homomorphisms which satisfy $(f_3)_0 = (f_1)_0 + (f_2)_0$ in $Hom(G'_0, G_0)$, then for any element $a \in \mathbf{D}(G/R)$ we have

$$f_1^*(a) + f_2^*(a) = f_3^*(a).$$

Proof. If $f: G' \longrightarrow G$ is a pointed map which reduces mod I to a group homomorphism, the diagram

$$\begin{tikzcd}
G' \times G' \arrow[r, "\mathrm{sum}"] \arrow[d, "f \times f"] & G' \arrow[d, "f"] \\
G \times G \arrow[r, "\mathrm{sum}"] & G
\end{tikzcd}$$

commutes mod I, i.e.

$$\mathrm{sum} \cdot (f \times f) \equiv f \cdot \mathrm{sum} \qquad \mathrm{mod}\, I.$$

and hence for any $a \in H^1_{DR}(G/R)$ we have, by the previous lemma,

$$(f \times f)^*(\mathrm{sum}^*(a)) = \mathrm{sum}^*(f^*(a))$$

The analogous diagrams with "sum" replaced by pr_1 or pr_2 commute, hence

$$(f \times f)^*(pr_i^*(a)) = pr_i^*(f^*(a)) \quad \text{for } i = 1,2.$$

Combining these, we find

$$(f \times f)^*(\mathrm{sum}^*(a) - pr_1^*(a) - pr_2^*(a)) =$$
$$\mathrm{sum}^*(f^*(a)) - pr_1^*(f^*(a)) - pr_2^*(f^*(a)).$$

In particular, if $a \in \mathbf{D}(G/R)$ then $f^*(a) \in \mathbf{D}(G'/R)$.

Similarly, if f_1, f_2 and f_3 are as in the assertion of the theorem, the diagram

$$\begin{tikzcd}
G' \arrow[r, "f_1 \times f_2"] \arrow[rr, bend right, "f_3"'] & G \times G \arrow[r, "\mathrm{sum}"] & G
\end{tikzcd}$$

commutes mod I, and the diagram

$$\begin{tikzcd}
G' \arrow[r, "f_1 \times f_2"] \arrow[rr, bend left, "f_1"] \arrow[rr, bend right, "f_2"'] & G \times G \arrow[r, shift left, "pr_1"] \arrow[r, shift right, "pr_2"'] & G
\end{tikzcd}$$

commutes. So again using the preceding lemma, we see that for any $a \in H^1_{DR}(G/R)$, we have

$$f_3^*(a) - f_1^*(a) - f_2^*(a) = (f_1 \times f_2)^*(\mathrm{Sum}^*a) - pr_1^*(a) - pr_2^*(a)).$$

In particular, for $a \in \mathbf{D}(G/R)$, we obtain the asserted formula

$$f_3^*(a) = f_1^*(a) + f_2^*(a).$$

QED

Let $CFG(R;R_0)$ denote the additive category whose *objects* are the commutative formal Lie groups over R, but in which the morphisms are the homomorphisms between their reductions mod I:

$$\mathrm{Hom}_{CFG(R,R_0)}(G', G) = \mathrm{Hom}(G'_0, G_0).$$

Given a homomorphism $f_0 : G'_0 \longrightarrow G_0$, it always lifts to a pointed morphism $f : G' \longrightarrow G$ of formal Lie varieties (just lift its power-series coefficients one-by-one, and keep the constant terms zero). According to the theorem, the induced map

$$f^* : \mathbf{D}(G/R) \longrightarrow \mathbf{D}(G'/R)$$

is *independent* of the choice of pointed lifting f of f_0. So it makes sense to denote the induced map

$$(f_0)^* : \mathbf{D}(G/R) \longrightarrow \mathbf{D}(G'/R).$$

THEOREM 5.1.5. *Let R be a Z-flat ring, and I ⊂ R a divided power ideal. Then the construction G* $\longmapsto$ *D(G/R),* $f_0 \longmapsto (f_0)^* =$ *(any pointed lifting)** *defines a contravariant additive functor from the category CFG(R;*R_0*) to the category of R-modules.*

Proof. This is just a restatement of the previous theorem. QED

REMARKS (1) Thanks to Lazard [33], we know that every commutative formal Lie group G_0 over R_0 lifts to a commutative formal Lie group G over R. If G′ is another lifting of G_0, then the identity endomorphism of G_0 is an isomorphism of G′ with G in the category CFG(R; R_0). Formation of the induced isomorphism $\mathbf{D}(G/R) \xrightarrow{\sim} \mathbf{D}(G'/R)$ provides a transitive system of identifications between the **D**'s of all possible liftings. In this way, it is possible to view the construction

$$G_0 \longmapsto \mathbf{D}(G/R), \text{ where G is some lifting of } G_0$$

as providing a contravariant additive functor from CFG(R_0) to the category of R-modules. We will not pursue that point of view here.

(2) Even without appealing to Lazard, one can proceed in an elementary fashion by observing that any commutative formal Lie group G_0 over R_0 can certainly be lifted to a formal Lie "monoid with unit" M over **R** (simply lift the individual coefficients of the group law, and always lift 0 to 0). For a monoid, one can still define **D**(M/R) as the primitive elements of H^1_{DR} (M/R), and one can still show exactly as before that the construction

$$G_0 \longrightarrow \mathbf{D}(M/R), \quad M \text{ any monoid lifting of } G_0$$

defines a contravariant additive functor from CFG(R_0) to R-modules.

A variant. The reader cannot have failed to notice the purely formal nature of most of our arguments. We might as well have begun with *any* contravariant functor **H** from formal Lie varieties over a **Z**-flat ring R to R-modules for which the key lemma (5.1.3) holds. One such **H**, which we will denote H^1_{DR} (V/R; I), is defined as H^1 of the *subcomplex* of the de Rham complex of V/R

$$\text{“IA(V)”} \longrightarrow \Omega^1_{V/R} \longrightarrow \Omega^2_{V/R} \longrightarrow \cdots$$

where "IA(V)" denotes the kernel of reduction mod I:

$$\text{“IA(V)”} = \text{Ker}(A(V) \twoheadrightarrow A(V_0)).$$

In terms of coordinates for V, "IA(V)" is the ideal consisting of those series all of whose coefficients lie in I. The analogue of lemma (5.1.2) becomes

$$\frac{\{f \in A(V \otimes K) \mid f(0) = 0, \text{df integral}\}}{\{f \in \text{“IA(V)”} \mid f(0) = 0\}} \xrightarrow[\sim]{d} H^1_{DR}(V/R; I).$$

This much makes sense for *any* ideal I ⊂ R. If I has divided powers, then the proof of the key lemma (5.1.3) is almost word-for-word the same. (It works because the terms $\boldsymbol{\Delta}^{\underline{n}}/(\underline{n})!$ all have coefficients in I.)

The corresponding theory, "primitive elements in H^1_{DR} (G/R; I)," is denoted $\mathbf{D}_I$(G/R). In terms of coordinates $X = (X_1, \ldots, X_n)$ for G, we have the explicit description

$$\mathbf{D}_I(G/R) = \\ = \frac{\{f \in K[[X]] \mid f(0) = 0, \text{dfintegral}, f(X \underset{G}{+} Y) - f(X) - f(Y) \in I[[X,Y]]\}}{\{f \in I[[X]] \mid f(0) = 0\}}$$

as compared with the explicit description

$$\mathbf{D}(G/R) = \\ = \frac{\{f \in K[[X]] \mid f(0) = 0, \text{ df integral}, f(X \underset{G}{+} Y) - f(X) - f(Y) \text{ integral}\}}{\{f \in R[[X]] \mid f(0) = 0\}}$$

For ease of later reference we summarize the above discussion in a theorem.

THEOREM 5.1.6. *Let R be a **Z**-flat ring, and $I \subset R$ a divided power ideal. The key lemma (5.1.3) holds for $H^1_{DR}(V/R;\, I)$, and theorems (5.1.4) and (5.1.5) hold for $\mathbf{D}_I(G/R)$.*

The natural map $\mathbf{D}_I \longrightarrow \mathbf{D}$ is not an isomorphism, but its kernel and cokernel are visibly killed by I. In the work of Honda and Fontaine, it is $\mathbf{D}_I$ rather than $\mathbf{D}$ which occurs; in the work of Grothendieck and Mazur-Messing ([17], [35]), it is $\mathbf{D}$ which arises more naturally.

Let us denote by $\underline{\boldsymbol{\omega}}_{G/R}$ the R-module of translation-invariant, or what is the same, primitive, one-forms on G/R. Because G is commutative, every element $w \in \underline{\boldsymbol{\omega}}_{G/R}$ is a closed form, so we have natural maps

$$\begin{tikzcd}
\underline{\boldsymbol{\omega}}_{G/R} \arrow[r] & \mathbf{D}_I(G/R) \arrow[d] \\
 & \mathbf{D}(G/R)
\end{tikzcd}$$

(Notice that in the extreme case $I = (0)$, the map $\underline{\boldsymbol{\omega}} \longrightarrow \mathbf{D}_I$ is an isomorphism!)

LEMMA 5.1.7. *Suppose R flat over **Z**, and $I \subset R$ an ideal. We have exact sequences*

$$0 \longrightarrow Hom_{\text{R-groups}}(G, \mathbf{G}_a) \xrightarrow{\ d\ } \underline{\boldsymbol{\omega}}_{G/R} \longrightarrow \boldsymbol{D}(G/R)$$

$$0 \longrightarrow Hom_{\text{R/I-groups}}\big(G \underset{R}{\otimes} (R/I), (\mathbf{G}_a)_{R/I}\big) \longrightarrow \boldsymbol{D}_I(G/R) \longrightarrow \boldsymbol{D}(G/R)$$

Proof. The first is the special case $\mathbf{I} = 0$ of the second; the second is clear from the explicit description of $\mathbf{D}_I$ and $\mathbf{D}$ given above. QED

COROLLARY 5.1.8. *If $Hom_{\text{R-groups}}(G, \mathbf{G}_a) = 0$, then the natural maps*

$$\underline{\boldsymbol{\omega}}_G \longrightarrow \boldsymbol{D}_I(G/R) \qquad \textit{and} \qquad \underline{\boldsymbol{\omega}}_G \longrightarrow \boldsymbol{D}(G/R)$$

are injective.

The reader interested in obtaining the limit formula for Jacobi sums

conjectured by Honda may skip the rest of this chapter! Others may also be tempted.

5.2. INTERPRETATION VIA EXT A LA MAZUR-MESSING.

We denote by Ext(G, $\mathbf{G}_a$) the group of isomorphism classes of extensions of G by $\mathbf{G}_a$, i.e. of short exact sequences

$$0 \longrightarrow \mathbf{G}_a \longrightarrow E \longrightarrow G \longrightarrow 0$$

of abelian f.p.p.f. sheaves on (Schemes/R). We denote by $\mathrm{Ext}^{\mathrm{rigid}}(G, \mathbf{G}_a)$ the group of isomorphism classes of "rigidified extensions," i.e. pairs consisting of an extension of G by $\mathbf{G}_a$ together with a *splitting* of the corresponding extension of Lie algebras:

$$\begin{tikzcd}
0 \arrow[r] & R = \mathrm{Lie}(\mathbf{G}_a) \arrow[r] & \mathrm{Lie}(E) \arrow[r] & \mathrm{Lie}(G) \arrow[r] \arrow[l, bend right] & 0
\end{tikzcd}$$

Because Lie(G) is a free R-module of rank n = dim(G), any extension of G by $\mathbf{G}_a$ admits such a rigidification, which is indeterminate up to an element of Hom(Lie(G), Lie($\mathbf{G}_a$)) = $\underline{\boldsymbol{\omega}}_{G/R}$. Passing to isomorphism classes and remembering that the set of splittings of a trivial extension of G by $\mathbf{G}_a$ is itself principal homogeneous under Hom(G,$\mathbf{G}_a$), we obtain a four-term exact sequence (valid over *any* ring R)

$$\mathrm{Hom}(G, \mathbf{G}_a) \xrightarrow{\ d\ } \underline{\boldsymbol{\omega}}_G \longrightarrow \mathrm{Ext}^{\mathrm{rigid}}(G, \mathbf{G}_a) \longrightarrow \mathrm{Ext}(G, \mathbf{G}_a) \longrightarrow 0$$

THEOREM 5.2.1. *If R is flat over **Z**, there is a natural isomorphism*

$$\boldsymbol{D}(G/R) \xleftarrow{\ \sim\ } Ext^{\mathrm{rigid}}(G, \mathbf{G}_I)$$

in terms of which the resulting four term exact sequence

$$0 \longrightarrow Hom(G, \mathbf{G}_a) \longrightarrow \underline{\boldsymbol{\omega}}_G \longrightarrow \boldsymbol{D}(G/R) \longrightarrow Ext(G, \mathbf{G}_a) \longrightarrow 0$$

is the concatenation of the three-term sequence of (5.1.3) and the map

$$\boldsymbol{D}(G/R) \longrightarrow Ext(G, \mathbf{G}_a) \textit{ defined by}$$

$$f \longrightarrow \textit{the class of the symmetric 2-cocycle}$$

$$\partial f = f(X \underset{G}{+} Y) - f(X) - f(Y)$$

Proof. We begin by constructing the isomorphism. Given a rigidified extension

$$\begin{tikzcd}0 \arrow[r] & \mathbf{G}_a \arrow[r] & E \arrow[r] & G \arrow[r] & 0\end{tikzcd}$$

$$\begin{tikzcd}0 \arrow[r] & \mathrm{Lie}(\mathbf{G}_a) \arrow[r] & \mathrm{Lie}(E) \arrow[r] & \mathrm{Lie}(G) \arrow[r] \arrow[l, bend right, "s"'] & 0,\end{tikzcd}$$

extend scalars from R to $K = R \otimes \mathbf{Q}$. Because K is a **Q**-algebra, the Lie functor defines an equivalence of categories between commutative formal Lie groups over K and free finitely generated K-modules.

Therefore there is a unique splitting as K-groups

$$\begin{tikzcd}0 \arrow[r] & \mathbf{G}_a \underset{R}{\otimes} K \arrow[r] & E \underset{R}{\otimes} K \arrow[r] & G \underset{R}{\otimes} K \arrow[r] \arrow[l, bend right, "\exp(s)"'] & 0\end{tikzcd}$$

whose differential is the given splitting S on Lie algebras.

At the same time, we may choose a cross section S in the category of *pointed* f.p.p.f. sheaves over R

$$\begin{tikzcd}0 \arrow[r] & \mathbf{G}_a \arrow[r] & E \arrow[r] & G \arrow[r] \arrow[l, bend right, "S"'] & 0.\end{tikzcd}$$

The difference $f = S - \exp(s)$ is a pointed map from $G \otimes K$ to $(\mathbf{G}_a) \otimes K$, i.e. an element $f \in A(G \otimes K)$, and it satisfies $f(0) = 0$. We have $df = dS - s$, so df is integral, and the formula

$$f(X \underset{G}{+} Y) - f(X) - f(Y) = S(X \underset{G}{+} Y) - S(X) - s(Y),$$

valid because exp(s) is a homomorphism, shows that $f(X \underset{G}{+} Y) - f(X) - f(Y)$ is integral.

Because the initial choice of S is indeterminate up to addition of a pointed map from G to $\mathbf{G}_a$, the class of $f = S\text{-}\exp(s)$ in $\mathbf{D}(G/R)$ is well-defined independently of the choice of S, and it vanishes if and only if exp(s) is itself integral, i.e. if and only if the original rigidified extension is trivial as a rigidified extension. Thus we obtain an injective map

$$\mathrm{Ext}^{\mathrm{rigid}}(G, \mathbf{G}_a) \longrightarrow \mathbf{D}(G/R).$$

To see that it is an isomorphism, note that in any case the map $\mathbf{D}(G/R) \longrightarrow \mathrm{Ext}(G, G_a)$ defined by $f \longrightarrow$ the class of ∂f sits in an exact sequence

$$\begin{tikzcd}0 \arrow[r] & \mathrm{Hom}(G, \mathbf{G}_a) \arrow[r] & \underline{\omega}_G \arrow[r] & \mathbf{D}(G/R) \arrow[r] & \mathrm{Ext}(G, \mathbf{G}_a),\end{tikzcd}$$

which receives the $\mathrm{Ext}^{\mathrm{rigid}}$ exact sequence:

$$\begin{tikzcd}0 \arrow[r] & \mathrm{Hom}(G, \mathbf{G}_a) \arrow[r] \arrow[d, equal] & \underline{\omega}_G \arrow[r] \arrow[d, equal] & \mathbf{D}(G/R) \arrow[r] & \mathrm{Ext}(G, \mathbf{G}_a) \arrow[d, equal] \\ 0 \arrow[r] & \mathrm{Hom}(G, \mathbf{G}_a) \arrow[r] & \underline{\omega}_G \arrow[r] & \mathrm{Ext}^{\mathrm{rigid}}(G, \mathbf{G}_a) \arrow[r] \arrow[u, hook] & \mathrm{Ext}(G, \mathbf{G}_a) \arrow[r] & 0\end{tikzcd}$$

The result is now visible. QED

Given an ideal $I \subset R$, we denote by $\mathrm{Ext}(G, \mathbf{G}_a; I)$ the group of isomorphism classes of pairs consisting of an extension of G by $\mathbf{G}_a$ together with a splitting of its reduction modulo I. We denote by $\mathrm{Ext}^{\mathrm{rigid}}(G, \mathbf{G}_a; I)$ the group of isomorphism classes of pairs consisting of a rigidified extension and a splitting of the reduction mod I of the underlying extension. Analogously to the previous theorem, we have

THEOREM 5.2.2. *If R is flat over* $\mathbf{Z}$, *and* $I \subset R$ *an ideal, there is a natural isomorphism*

$$Ext^{\mathrm{rigid}}(G, \mathbf{G}_a; I) \xrightarrow{\sim} \mathbf{D}_1(G/R)$$

and a four-term exact sequence

$$0 \longrightarrow Hom(G, \mathbf{G}_a) \longrightarrow \underline{\omega}_G \longrightarrow \mathbf{D}_1(G/R) \xrightarrow{\partial} Ext(G, \mathbf{G}_a; I) \longrightarrow 0$$

in which the map ∂, *given by*

$$f \longrightarrow \textit{the class of the symmetric 2-cocycle}$$

$$\partial f = f(X \underset{G}{+} Y) - f(X) - f(Y),$$

corresponds to the map "forget the rigidification" on Ext's.

5.3 THE CASE OF P-DIVISIBLE FORMAL GROUPS. Let p be a prime number. A ring R is said to be p-adic if it is complete and separated in its p-adic topology, i.e., if

$$R \xrightarrow{\sim} \varprojlim R/p^n R.$$

A commutative formal Lie group G over a p-adic ring R is said to be p-divisible of height h if the map "multiplication by p" makes A(G) into a finite locally free module over itself of rank p^h.

If we denote by G^v the dual of G in the sense of p-divisible groups, it makes sense to speak of the tangent space of G^v at the origin, noted $\underline{t}_{G^v}$; it is known that $\underline{t}_{G^v}$ is a locally free R-module of rank h − dim (G), and that there is a canonical isomorphism

5.3.1 $$\mathrm{Ext}\,(G,\mathbf{G}_a) \xrightarrow{\sim} \underline{t}_{G^v}\,.$$

Because G is p-divisible and R is p-adic, $\mathrm{Hom}(G,G_a) = 0$, and the four-term exact sequence becomes a Hodge-like exact sequence

5.3.2 $$0 \longrightarrow \underline{\boldsymbol{\omega}}_G \longrightarrow \mathbf{D}(G/R) \longrightarrow \underline{t}_{G^v} \longrightarrow 0$$

Thus we find

THEOREM 5.3.3. *1) If R is a p-adic ring which is flat over* $\mathbf{Z}$*, then for a p-divisible commutative formal Lie group G over R, the R-module* $\mathbf{D}(G/R)$ *is locally free of rank h = height (G), and its formation commutes with arbitrary extension of scalars of* $\mathbf{Z}$*-flat p-adic rings.*

If in addition $I \subset R$ is an ideal which is closed in the p-adic topology, then R/I is again a p-adic ring, $G \otimes (R/I)$ is still p-divisible, and therefore admits no non-trivial homomorphisms to $\mathbf{G}_a$ over R/I. It follows that

(5.3.4) $$\begin{cases} \mathbf{D}_I(G/R) \subset \mathbf{D}(G/R) \\ \mathrm{Ext}(G,\mathbf{G}_a;I) \xrightarrow{\sim} \mathbf{I}\cdot\mathrm{Ext}(G,\mathbf{G}_a) \simeq I\cdot\underline{t}_{G^v} \end{cases}$$

and we have a short exact sequence

(5.3.5) $$0 \longrightarrow \underline{\boldsymbol{\omega}}_G \longrightarrow \mathbf{D}_I(G/R) \longrightarrow I\cdot\underline{t}_{G^v} \longrightarrow 0.$$

5.5 RELATION TO THE CLASSICAL THEORY. Let k be a perfect field of characteristic $p > 0$, and take $R = W(k)$, $I = (p)$. Let CW denote the k-group-functor "Witt covectors" (in the notations of Fontaine ([13]), with its structure of W(k)-module. According to Fontaine, for any formal Lie variety V over W(k), we obtain a W(k)-linear isomorphism

(5.5.1) $$w : CW(A(V \otimes k)) \xrightarrow{\sim} H^1_{DR}\,(V/W(k);(p))$$

by defining

(5.5.2) $$w(\ldots,a_{-n},\ldots,a_0) = d\left(\sum_{n\geq 0} \frac{(\tilde{a}_{-n})^{p^n}}{p^n}\right)$$

where $\tilde{a}_{-n}$ denotes an arbitrary lifting to A(V) of $a_{-n} \in A(V\otimes k)$. Similarly, we can define, following Grothendieck, Mazur-Messing ([35]), a $\boldsymbol{\sigma}$-linear isomorphism

(5.5.3) $$\psi : CW(A(V\otimes k)) \xrightarrow{\sim} H^1_{DR}\,(V/W(k))$$

by the formula

(5.5.4) $$\psi(\ldots,a_{-n},\ldots,a_0) = d\left(\sum_{n\geq 0} \frac{(\tilde{a}_{-n})^{p^{n+1}}}{p^{n+1}}\right).$$

These isomorphisms sit in a commutative diagram

(5.5.5)) $$\begin{tikzcd} & H^1_{DR}\,(V/W(k);(p)) \arrow[dd, "\frac{1}{p}F", "\wr"'] \\ CW(A(V\otimes k)) \arrow[ur, "\sim", "w"'] \arrow[dr, "\sim", "\psi"'] & \\ & H^1_{DR}\,(V/W(k)). \end{tikzcd}$$

When G is a commutative formal Lie group over W(k) which is *p-divisible*, the "classical" Dieudonné module of $G_0 = G\otimes k$ is *defined* as

(5.5.6) $$\begin{aligned} \mathbf{M}(G_0) \overset{\mathrm{dfn}}{=\!=} \mathrm{Hom}_{k-gp}&(G_0,CW) \\ &\| \\ \text{the primitive elements in } &CW\,(A(G_0)). \end{aligned}$$

Combining this definition with the previous isomorphisms, we find a commutative diagram of isomorphisms

(5.5.7) $$\begin{tikzcd} & \mathbf{D}_p\,(G/W(k)) \arrow[dd, "\frac{1}{p}F", "\wr"'] \\ \mathbf{M}(G_0) \arrow[ur, "\sim", "w"'] \arrow[dr, "\sim", "\psi"'] & \\ & \mathbf{D}(G/W(k)). \end{tikzcd}$$

5.6. Relation with abelian schemes and with the general theory. In this section, we recall without proofs some of the main results and compatibilities of the general **D**-theory of Grothendieck and Mazur-Messing.

Given an abelian scheme A over an arbitrary ring R, there are canonical isomorphisms

$$(5.6.1)\qquad \begin{cases} \mathrm{Ext}^{\mathrm{rigid}}(A,\mathbf{G}_a) \xrightarrow{\sim} H^1_{\mathrm{DR}}(A/R) \\ \mathrm{Ext}(A,\mathbf{G}_a) \xrightarrow{\sim} H^1(A,O_A) = \mathrm{Lie}(A^{\vee}) \end{cases}$$

in terms of which the $\mathrm{Ext}^{\mathrm{rigid}}$-exact sequence "becomes" the Hodge exact sequence:

(5.6.2)
$$\begin{tikzcd}
0 \arrow[r] & \underline{\omega}_A \arrow[r] \arrow[d, equal] & \mathrm{Ext}^{\mathrm{rigid}}(A,\mathbf{G}_a) \arrow[r] \arrow[d, "\wr"'] & \mathrm{Ext}(A,\mathbf{G}_a) \arrow[r] \arrow[d, "\wr"'] & 0 \\
0 \arrow[r] & \underline{\omega}_A \arrow[r] & H^1_{\mathrm{DR}}(A/R) \arrow[r] & H^1(A,O_A) \arrow[r] \arrow[d, equal] & 0 \\
& & & \mathrm{Lie}(A^{\vee}) &
\end{tikzcd}$$

Given a p-divisible (Barsotti-Tate) group $G = \varinjlim G_n$ over a ring R in which p is nilpotent, the exact sequence

$$(5.6.3)\qquad 0 \longrightarrow G_n \longrightarrow G \xrightarrow{p^n} G \longrightarrow 0$$

for any n sufficiently large that $p^n = 0$ in R, leads to a canonical isomorphism

$$(5.6.4)\qquad \mathrm{Lie}(G^{\vee}) = \mathrm{Lie}(G_n^{\vee}) = \mathrm{Hom}(G_n,\mathbf{G}_a) \xrightarrow{\sim} \mathrm{Ext}(G,\mathbf{G}_a).$$

The $\mathrm{Ext}^{\mathrm{rigid}}$-exact sequence can thus be written

$$(5.6.5)\qquad 0 \longrightarrow \underline{\omega}_G \longrightarrow \mathrm{Ext}^{\mathrm{rigid}}(G,\mathbf{G}_a) \longrightarrow \mathrm{Lie}(G^{\vee}) \longrightarrow 0,$$

where $\underline{\omega}_G$ is the R-linear dual of Lie(G).

Given an abelian scheme A over a ring R in which p is nilpotent, the exact sequence

$$(5.6.6)\qquad 0 \longrightarrow A_{p^n} \longrightarrow A \xrightarrow{p^n} A \longrightarrow 0$$

for any n sufficiently large that $p^n = 0$ in R leads to a canonical isomorphism

$$(5.6.7)\qquad \mathrm{Lie}(A^{\vee}) = \mathrm{Lie}(A_{p^n}^{\vee}) = \mathrm{Hom}(A_{p^n},\mathbf{G}_a) \xrightarrow{\sim} \mathrm{Ext}(A,\mathbf{G}_a).$$

Therefore the inclusion $A_{p^\infty} \hookrightarrow A$ induces an isomorphism

$$(5.6.8)\qquad \mathrm{Ext}(A,\mathbf{G}_a) \xrightarrow{\sim} \mathrm{Ext}(A_{p^\infty},\mathbf{G}_a)$$

(the identity on $\mathrm{Hom}(A_{p^n}, \mathbf{G}_a)$!), and consequently we obtain a commutative diagram of isomorphisms

(5.6 9)
$$\begin{tikzcd}
0 \arrow[r] & \underline{\omega}_A \arrow[r] \arrow[d, equal] & \mathrm{Ext}^{\mathrm{rigid}}(A,\mathbf{G}_a) \arrow[r] \arrow[d, "\wr"'] & \mathrm{Ext}(A,\mathbf{G}_a) \arrow[r] \arrow[d, "\wr"'] & 0 \\
0 \arrow[r] & \underline{\omega}_{A_{p^\infty}} \arrow[r] & \mathrm{Ext}^{\mathrm{rigid}}(A_{p^\infty},\mathbf{G}_a) \arrow[r] & \mathrm{Ext}(A_{p^\infty},\mathbf{G}_a) \arrow[r] & 0,
\end{tikzcd}$$

i.e., an isomorphism

$$(5.6.10)\qquad H^1_{\mathrm{DR}}(A/R) \xrightarrow{\sim} \mathbf{D}(A_{p^\infty}/R)$$

compatible with the Hodge filtration.

For variable B – T groups G over a fixed ring R in which p is nilpotent, the functors $\underline{\omega}_G$, $\mathrm{Lie}(G^{\vee})$, and consequently $\mathrm{Ext}^{\mathrm{rigid}}(G,\mathbf{G}_a)$, are exact functors whose values are locally free R-modules of finite rank; their formation commutes with arbitrary extension of scalars of rings in which p is nilpotent.

Following Grothendieck and Mazur-Messing we *define*

$$(5.6.11)\qquad \mathbf{D}(G/R) \overset{\mathrm{dfn}}{=\!=} \mathrm{Ext}^{\mathrm{rigid}}(G,\mathbf{G}_a)$$

when G is a B – T group over a ring R in which p is nilpotent.

When R is a p-adic ring, and G is a B – T group over R, we *define*

$$(5.6.12)\qquad \begin{cases} \mathbf{D}(G/R) = \varprojlim\limits_{n} \mathbf{D}(G\otimes(R/p^nR)/(R/p^nR)) \\ \mathrm{Lie}(G) = \varprojlim \mathrm{Lie}(G\otimes(R/p^nR)) \\ \underline{\omega}_G = \varprojlim \underline{\omega}_G \otimes (R/p^nR) \end{cases}$$

Thus for variable B – T groups G over a p-adic ring R, the fnctors $\underline{\omega}_G$, Lie($G^\vee$) and $\mathbf{D}(G/R)$ are all exact functors in locally free R-modules of finite rank, sitting in an exact sequence

$$(5.6.13) \qquad 0 \longrightarrow \underline{\omega}_G \longrightarrow \mathbf{D}(G/R) \longrightarrow \mathrm{Lie}(G^\vee) \longrightarrow 0$$

whose formation commutes with arbitrary extension of scalars of p-adic rings. When A is an abelian scheme over a p-adic ring R, we obtain an isomorphism

$$H^1_{DR}(A/R) \xrightarrow{\sim} \mathbf{D}(A(p^\infty)/R),$$

compatible with Hodge filtrations, by passage to the limit.

As we have seen in the previous section, this general $\mathrm{Ext}^{\mathrm{rigid}}$ notion of $\mathbf{D}(G/R)$ agrees with our more explicit one in the case that both are defined, namely when G is a p-divisible formal group over a $\mathbf{Z}$-flat p-adic ring R.

5.7. RELATION WITH COHOMOLOGY

THEOREM 5.7.1. *Let A be an abelian scheme over the Witt vectors W(k) of an algebraically closed field k of characteristic p > 0. There is a short exact sequence of W-modules*

$$0 \longrightarrow H^1_{et}(A\otimes k, Z_p)\otimes W \xrightarrow{\alpha} H^1_{cris}(A\otimes k/W) \xrightarrow{\beta} D(\hat{A}/W) \longrightarrow 0$$

which is functorial in $A\otimes k$.

Proof. We begin by defining the maps α and β. They will be defined by passage to the limit from maps α_n, β_n in an exact sequence

$$5.7.2 \quad 0 \longrightarrow H^1_{et}(A\otimes k, \mathbf{Z}/p^n\mathbf{Z})\otimes W_n \xrightarrow{\alpha_n} H^1_{cris}(A\otimes k/W_n)$$
$$\xrightarrow{\beta_n} \mathbf{D}(\hat{A}\otimes W_n/W_n) \longrightarrow 0.$$

of W_n-modules.

An element of $H^1(A\otimes k, \mathbf{Z}/p^n\mathbf{Z})$ is (the isomorphism class of) a $\mathbf{Z}/p^n\mathbf{Z}$-torsor over $A\otimes k$. An element of $H^1_{cris}(A\otimes k/W_n)$ is (the isomorphism class of) a rule which assigns to every test situation $Y \hookrightarrow Y_n$ consisting an $A\otimes k$ scheme Y and a divided-power thickening of Y to a W_n-scheme Y_n a $\mathbf{G}_a$-torsor on Y_n in a way which is compatible with inverse image whenever we have a morphism $(Y, Y_n) \longrightarrow (Y', Y'_n)$ of such test situations (cf. [35] for more details).

Given a $\mathbf{Z}/p^n\mathbf{Z}$-torsor T on $A\otimes k$, we must define for every test situation $Y \hookrightarrow Y_n$, a $\mathbf{G}$ -torsor $\alpha_n(T)_{(Y,Y_n)}$ on Y_n. Because Y is given as an $A\otimes k$ scheme, we can pull back T to obtain a $\mathbf{Z}/p^n\mathbf{Z}$-torsor T_Y on Y. Because Y_n is a W_n-scheme which is a divided-power thickening, its ideal of definition is necessarily a nil-ideal; therefore the etale Y-scheme T_Y extends uniquely to an etale Y_n-scheme $T_{(Y,Y_n)}$, and its structure of $\mathbf{Z}/p^n\mathbf{Z}$-torsor extends uniquely as well. Because Y_n is a W_n-scheme, the natural map

$$\mathbf{Z}/p^n\mathbf{Z} \longrightarrow W_n$$

gives rise to a morphism of algebraic groups on Y_n

$$(\mathbf{Z}/p^n\mathbf{Z})_{Y_n} \xrightarrow{\alpha_n} (\mathbf{G}_a)_{Y_n};$$

the required $\mathbf{G}_a$-torsor $\alpha_n(T)_{(Y,Y_n)}$ is obtained by "extension of structural group via α_n" from the $\mathbf{Z}/p^n$ $\mathbf{Z}$-torsor $T_{(Y,Y_n)}$.

To define β_n, we begin with an element Z of $H^1_{cris}(A\otimes k/W_n)$. We must define an element $\beta_n(Z)$ in $\mathrm{Ext}^{\mathrm{rigid}}(\hat{A}\otimes W_n, (G_a)\otimes W_n) = \mathbf{D}(\hat{A}\otimes W_n/W_n)$. Its value on the test object $A\otimes k \hookrightarrow A\otimes W_n$ is a $\mathbf{G}_a$-torsor on $A\otimes W_n$ which is endowed with an integrable connection (cf. [2], [3]), i.e., it is an element of $H^1_{DR}(A\otimes W_n/W_n)$. [This interpretation provides the canonical isomorphism

$$H^1_{cris}(A\otimes k/W_n) \xrightarrow{\sim} H^1_{DR}(A\otimes W_n/W_n).]$$

Composing with the isomorphism

$$H^1_{DR}(A\otimes W_n/W_n) \xrightarrow{\sim} \mathrm{Ext}^{\mathrm{rigid}}(A\otimes W_n, G_a\otimes W_n),$$

we obtain an element of $\mathrm{Ext}^{\mathrm{rigid}}(A\otimes W_n, G_a\otimes W_n)$, whose restriction to the formal group $\hat{A}\otimes W_n$ is the required element $\beta_n(Z)$.

To see that the map β obtained from these β_n by passage to the limit is in fact functorial in $A \otimes k$, we first note that it sits in the commutative diagram

(5.7.3)

$$\begin{tikzcd}
H^1_{\mathrm{cris}}(A \otimes k/W) \arrow[r, "\beta"] \arrow[d, "\wr"', "\text{canonical isom}"] & D(\hat{A}/W) \arrow[d, hook, "\begin{array}{l}\text{inclusion of}\\ \text{primitive}\\ \text{elements}\end{array}"] \\
H^1_{DR}(A/W) \arrow[r, "\text{natural map}", "\text{``restriction to } \hat{A}\text{''}"'] & H^1_{DR}(\hat{A}/W).
\end{tikzcd}$$

What must be shown is that if we are given a second abelian scheme B over W, and a homomorphism

$$f_0 : B \otimes k \longrightarrow A \otimes k$$

then the diagram

(5.7.)

$$\begin{tikzcd}
H^1_{\mathrm{cris}}(A \otimes k/W) \arrow[r, "\beta"] \arrow[d, "(f_0)^*"] & D(\hat{A}/W) \arrow[d, "\begin{array}{l}(\text{any pointed}\\ \text{lifting of } \hat{f}_0)^*\end{array}"] \\
H^1_{\mathrm{cris}}(B \otimes k/W) \arrow[r, "\beta"] & D(\hat{B}/W)
\end{tikzcd}$$

is *commutative*.

But in virtue of the commutativity of the previous diagram (5.7.3), it is enough to show the commutativity of the diagram

5.7.5

$$\begin{tikzcd}
H^1_{\mathrm{cris}}(A \otimes k/W) \simeq H^1_{DR}(A/W) \arrow[r, "\text{restriction}"] \arrow[d, "(f_0)^*"] & H^1_{DR}(\hat{A}/W) \arrow[d, "\begin{array}{l}(\text{any pointed}\\ \text{lifting of } \hat{f}_0)^*\end{array}"] \\
H^1_{\mathrm{cris}}(B \otimes k/W) \simeq H^1_{DR}(B/W) \arrow[r, "\text{restriction}"] & H^1_{DR}(\hat{B}/W).
\end{tikzcd}$$

This last commutativity has nothing to do with abelian schemes, nor does it require pointed liftings. It is an instance of the following general fact, whose proof we defer for a moment.

General Fact 5.7.6. *For any two pointed W-schemes A,B which are both proper and smooth, any pointed map $f_0 : B \otimes k \longrightarrow A \otimes k$, and any integer $i \geq 0$, we have a commutative diagram*

$$\begin{tikzcd}
H^i_{\mathrm{cris}}(A \otimes k/W) \simeq H^i_{DR}(A/W) \arrow[r, "\textit{restriction}"] \arrow[d, "(f_0)^*"] & H^i_{DR}(\hat{A}/W) \arrow[d, "\begin{array}{l}(\textit{any lifting}\\ \textit{of } \hat{f}_0)^*\end{array}"] \\
H^i_{\mathrm{cris}}(B \otimes k/W) \simeq H^i_{DR}(B/W) \arrow[r, "\textit{restriction}"] & H^i_{DR}(\hat{B}/W)
\end{tikzcd}$$

To conclude the proof of the theorem (!), it remains to see that our marvelously functorial maps α, β really do form an exact sequence. To do this, we will use the abelian scheme A over W. Its formal group $\hat{A}$ is p-divisible, and sits in an exact sequence of p-divisible groups over W,

$$0 \longrightarrow \hat{A}_{p^\infty} \longrightarrow A_{p^\infty} \longrightarrow E \longrightarrow 0,$$

in which $E = \varinjlim E_n$ denote the etale quotient of A_{p^∞}. Because k is algebraically closed, E is a *constant* p-divisible group, namely the abstract p-divisible group $\varinjlim A_{p^n}(k)$ of all p-power torsion points of $A(k)$.

We will identify the exact sequence of the proposition with the exact sequence

$$0 \longrightarrow \mathbf{D}(E/W) \xrightarrow{\alpha'} \mathbf{D}(A_{p^\infty}/W) \xrightarrow{\beta'} \mathbf{D}(\hat{A}/W) \longrightarrow 0,$$

and we will identify the (α_n, β_n)-sequence with the exact sequence

$$0 \longrightarrow \mathbf{D}(E \otimes W_n/W_n) \xrightarrow{\alpha'_n} \mathbf{D}(A_{p^\infty} \otimes W_n/W_n) \xrightarrow{\beta'_n} \mathbf{D}(\hat{A} \otimes W_n/W_n) \longrightarrow 0.$$

It is clear from the construction of β_n that we have a commutative diagram

$$\begin{tikzcd}
\mathbf{D}(A_{p^\infty}\otimes W_n/W_n) \arrow[rr, "\beta_n'"] \arrow[d, equal] & & \mathbf{D}(\hat{A}\otimes W_n/W_n) \arrow[d, equal, "\text{dfn}"] \\
\mathrm{Ext}^{\text{rigid}}(A_{p^\infty}\otimes W_n, \mathbf{G}_a) \arrow[rr, "\text{restriction}"] & & \mathrm{Ext}^{\text{rigid}}(\hat{\mathbf{A}}\otimes W_n, \mathbf{G}_a) \\
\mathrm{Ext}^{\text{rigid}}(A\otimes W_n, \mathbf{G}_a) \arrow[u, "\wr"] \arrow[d, "\wr"'] \arrow[urr, "\text{restriction}"] & & \\
H^1_{DR}(A\otimes W_n/W_n) & & \\
H^1_{\text{cris}}(A\otimes k/W_n). \arrow[u, "\wr"] \arrow[uuurr, "\beta_n"'] & &
\end{tikzcd}$$

To relate the map α_n to the $\mathbf{D}$-maps, use the exact sequence

$$0 \longrightarrow E_n\otimes W_n \longrightarrow E\otimes W_n \xrightarrow{p^n} E\otimes W_n \longrightarrow 0$$

to compute

$$\begin{tikzcd}
\mathbf{D}(E\otimes W_n/W_n) \arrow[r, "\sim"] & \mathrm{Ext}(E\otimes W_n, \mathbf{G}_a) \simeq & \mathrm{Hom}(E_n\otimes W_n, \mathbf{G}_a) \arrow[d, equal, "\wr"'] \\
& & \mathrm{Hom}(E_n(\mathbf{W}_n), \mathbf{G}_a(W_n)) \arrow[d, equal] \\
& & \mathrm{Hom}(E_n(\mathbf{k}), W_n) \arrow[d, equal] \\
& & \mathrm{Hom}(E_n(k), \mathbf{Z}/p^n\mathbf{Z})\otimes W_n\,.
\end{tikzcd}$$

(E_n is constant)

Next use the sequence

$$0 \longrightarrow A_{p^n}\otimes W_n \longrightarrow A\otimes W_n \xrightarrow{p^n} A\otimes W_n \longrightarrow 0$$

to compute

$$\begin{tikzcd}
\mathrm{Ext}(A\otimes W_n, \mathbf{Z}/p^n\mathbf{Z}) \simeq & \mathrm{Hom}(A_{p^n}\otimes W_n, \mathbf{Z}/p^n\mathbf{Z}) \\
& \mathrm{Hom}(E_n\otimes W_n, \mathbf{Z}/p^n\mathbf{Z}) \arrow[u, "\wr"] \arrow[d, "\wr"'] \\
H^1_{\text{et}}(A\otimes k, \mathbf{Z}/p^n\mathbf{Z}) & \mathrm{Hom}(E_n(k), \mathbf{Z}/p^n\mathbf{Z}). \arrow[l, "\sim"']
\end{tikzcd}$$

(E_n = etale quotient of A_{p^n})

Combining these isomorphisms, and remembering that $\mathrm{Ext} = \mathrm{Ext}^{\text{rigid}}$ when either of the arguments is etale, we find a commutative diagram

$$\begin{tikzcd}
\mathbf{D}(E\otimes W_n/W_n) \arrow[r, "\alpha_n'"] & \mathbf{D}(A_{p^\infty}\otimes W_n/W_n) \\
\mathrm{Hom}(E_n(k), \mathbf{Z}/p^n\mathbf{Z})\otimes W_n \arrow[u, "\wr"] \arrow[d, dash, "\wr"'] & \mathbf{D}(A\otimes W_n/W_n) \arrow[u, "\wr"'] \arrow[d, equal] \\
\mathrm{Ext}^{\text{rigid}}(A\otimes W_n, \mathbf{Z}/p^n\mathbf{Z})\otimes W_n \arrow[r, "***"] \arrow[d, dash, "\wr"'] & \mathrm{Ext}^{\text{rigid}}(A\otimes W_n, \mathbf{G}_a) \arrow[d, equal] \\
H^1_{\text{et}}(A\otimes k, \mathbf{Z}/p^n\mathbf{Z})\otimes W_n \arrow[r, "\alpha_n"] & H^1_{\text{cris}}(A\otimes k/W_n)
\end{tikzcd}$$

in which the arrow*** is "push-out" along the homomorphism

$$\mathbf{Z}/p^n\mathbf{Z} \longrightarrow W_n \longrightarrow (\mathbf{G}_a)_{W_n}\,.$$

QED

COROLLARY 5.7.7. *Let A be an abelian scheme over the Witt vectors $W(k)$ of a perfect field k of characteristic $p>0$. Then we have a short exact sequence of $W(k)$-modules*

$$0 \longrightarrow \Big((H^1_{\text{et}}(A\otimes\bar{k}, \mathbf{Z}_p)\otimes W(\bar{k}) \Big)^{\mathrm{Gal}(\bar{k}/k)} \longrightarrow H^1_{\text{cris}}(A\otimes k/W(k)) \longrightarrow \mathbf{D}(\hat{A}/W(k)) \longrightarrow 0,$$

in which $\bar{k}$ denotes an algebraic closure of k, and in which the galois group $Gal(\bar{k}/k)$ acts simultaneously on $H^1_{\text{et}}(A\otimes\bar{k}, \mathbf{Z}_p)$ and on $W(\bar{k})$ by "transport of structure."

Proof. One can obtain this sequence either by passing to $\mathrm{Gal}(\bar{k}/k)$-invariants in the already-established analogous sequence for $A \otimes W(\bar{k})$, or by repeating the *proof* given for the proposition. In the latter case, one finds, in the notations of the proof,

$$\begin{aligned} \mathbf{D}(E \otimes W_n(k)/W_n(k)) &\simeq \mathrm{Hom}(E_n \otimes W_n(k), (\mathbf{G}_a)_{W_n(k)}) \\ &\simeq \mathrm{Hom}(E_n(\bar{k}), W_n(\bar{k}))^{\mathrm{Gal}(\bar{k}/k)} \\ &\simeq \mathrm{Hom}(A_{p^n}(\bar{k}), W_n(\bar{k}))^{\mathrm{Gal}(\bar{k}/k)} \\ &= \left(H^1_{et}(A \otimes \bar{k}, \mathbf{Z}/p^n\,\mathbf{Z}) \otimes W_n(\bar{k}) \right)^{\mathrm{Gal}(\bar{k}/k)} \end{aligned}$$

and the rest of the proof remains unchanged. QED

COROLLARY 5.7.8. *Let A be an abelian scheme over the Witt vectors of a perfect field k of characteristic $p > 0$. The above exact sequence is the Newton-Hodge filtration*

$$0 \longrightarrow (\mathit{slope}\ 0) \longrightarrow H^1_{\mathrm{cris}}(A \otimes k/W) \longrightarrow (\mathit{slope} > 0) \longrightarrow 0$$

of $H^1_{\mathrm{cris}}(A \otimes k/W)$) as an F-crystal.

Proof. Since F induces a σ-linear automorphism of

$$\begin{aligned} &(H^1_{et}(A \otimes \bar{k}, \mathbf{Z}_p) \otimes W(\bar{k}))^{\mathrm{Gal}} \\ &\simeq \left(\mathrm{Hom}(T_p(A \otimes \bar{k}), W(\bar{k})) \right)^{\mathrm{Gal}(\bar{k}/k)}, \end{aligned}$$

it remains only to see that F is topologically nilpotent on $\mathbf{D}(\hat{A}/W(k))$, for its p-adic topology. Because $\mathbf{D}(\hat{A}/W(k))$ is a *finitely generated* $W(k)$ submodule of $H^1_{DR}(\hat{A}/W(k))$, the topology *induced* on $\mathbf{D}(\hat{A}/W(k))$ by the *inverse limit* topology on H^1_{DR} through the isomorphism (cf. lemma 5.8.1. ahead)

$$(5.7.9) \qquad H^1_{DR}(\hat{A}/W(k)) \xrightarrow{\sim} \varprojlim H^1_{DR}(\hat{A} \otimes W_n(k)/W_n(k))$$

must be *equivalent* to the p-adic topology in $\mathbf{D}(\hat{A}/W(k))$. So it suffices to remark that F^n annihilates $H^1_{DR}(\hat{A} \otimes W_n/W_n)$ (indeed F^n annihilates $\Omega^i_{\hat{A} \otimes W_n/W_n}$ for $i \geq 1$, since for any pointed lifting of $X \longmapsto X^p$, $F(dX) = d(F(X)) = d(X^p + pY) \in p\Omega^1$) to establish the required topological nilpotence of F on $\mathbf{D}(\hat{A}/W)$. QED

5.8. THE MISSING LEMMAS. It remains for us to establish the "general fact" (5.7.7), and to establish the isomorphism (5.7.9). In fact, the two questions are intimately related. We begin with the second.

LEMMA 5.8.1. *Let R be a* **Z**-*flat p-adic ring, and let $R_n = R/p^n R$. For any formal Lie variety V over R, we have isomorphisms*

$$H^i_{DR}(V/R) \xrightarrow{\sim} \varprojlim H^i_{DR}(V \otimes R_n/R_n).$$

Proof. Pick coordinates $X_1, \ldots, X_N$ for V. Over any ring R, we can define a $\mathbf{Z}^N$-grading of the de Rham complex of $R[[X_1, \ldots, X_N]]/R$, by attributing the weight $(a_1, \ldots, a_N) \in \mathbf{Z}^N$ to each "monomial"

$$(\Pi X_i^{a_i})\Big(\prod_{j \in S} \frac{dX_j}{X_j}\Big) \qquad S \text{ any subset of } \{1, \ldots, N\}.$$

Exterior differentiation is homogeneous of degree zero, and the de Rham complex is the *product* of all its homogeneous graded pieces

$$\Omega^\bullet = \Pi\, \Omega^\bullet(a_1, \ldots a_N).$$

Because both cohomology and inverse limits commute with products, we are reduced to proving the lemma homogeneous component by homogeneous component.

The individual complexes $\Omega^\bullet(a_1, \ldots a_N)$ are quite simple. They vanish except when all $a_i \geq 0$. The complex $\Omega^\bullet(0, \ldots, 0)$ is

$$R \longrightarrow 0 \longrightarrow 0 \longrightarrow \ldots\ .$$

If some $a_i \geq 1$, and all $a_i \geq 0$, the complex $\Omega^\bullet(a_1, \ldots a_N)$ is the tensor product complex

$$\bigotimes_{i \text{ with } a_i \geq 1} (R \xrightarrow{a_i} R).$$

What is important for us is that each of these complexes is obtained from a complex of free finitely generated **Z**-modules (!) by extension of scalars to R.

Thus let K denote any complex of free finitely-generated $\mathbf{Z}_p$-modules. We must show that for a **Z**-flat p-adic ring R we have

$$H^i(K^\bullet \otimes R) \xrightarrow{\sim} \varprojlim H^i(K^\bullet \otimes R_n).$$

The exact sequence of complexes

$$0 \longrightarrow K^\bullet \otimes R \xrightarrow{p^n} K^\bullet \otimes R \longrightarrow K^\bullet \otimes R_n \longrightarrow 0$$

gives a "universal coefficients" exact sequence

$$0 \to H^i(K^\bullet \otimes R) \otimes R_n \to H^i(K^\bullet \otimes R_n) \to p^n\text{-Torsion}(H^{i+1}(K^\bullet \otimes R)) \to 0.$$

Passing to the inverse limit over n leads to an exact sequence

$$0 \to \varprojlim H^i(K^\bullet \otimes R) \otimes R_n \to \varprojlim H^i(K^\bullet \otimes R^n) \to T_p(H^{i+1}(K^\bullet \otimes R)) \to 0.$$

To see that $T_p(H^{i+1}(K^\bullet \otimes R))$ vanishes, notice that an element of this T_p is represented by a system of elements $a_n \in K^{i+1} \otimes R$ with $d(a_n) = 0$, $p\ a_{n+1} = a_n - d(b_n), a_0 = 0$; because both $K^i \otimes R$ and $K^{i+1} \otimes R$ are p-adically complete and separated, we may infer

$$\begin{aligned} a_n &= pa_{n+1} + d(b_n) \\ &= p\Big(pa_{n+2} + d(b_{n+1})\Big) + d(b_n) \\ &= \ldots \\ &= d(\sum_{i \geq 0} p^i b_{n+i}). \end{aligned}$$

To see that the natural map

$$H^i(K^\bullet \otimes R) \longrightarrow \varprojlim H^i(K^\bullet \otimes R) \otimes R_n$$

is an isomorphism, use the **Z**-flatness of **R** and the **Z**-finite generation of the K^i to write

$$\begin{aligned} H^i(K^\bullet \otimes R) \xleftarrow{\sim} H^i(K^\bullet) \otimes R &= (\text{fin. gen. } \mathbf{Z}\text{-module}) \otimes R \\ &= (\mathbf{Z}^n \oplus (\oplus \mathbf{Z}/p^{n_i}) \oplus (\substack{\text{prime-to-p} \\ \text{torsion}})) \otimes R \\ &= R^n \oplus (\oplus R_{n_i}). \end{aligned}$$

QED

We now turn to the proof of the "general fact."

LEMMA 5.8.2. *Let k be a perfect field of characteristic $p > 0$, A and B two proper, smooth pointed $W(k)$-schemes, $f_0: B \otimes k \longrightarrow A \otimes k$ a pointed k-morphism and $\hat{f}: \hat{B} \longrightarrow \hat{A}$ a W-lifting of f_0 to the formal*

completions viewed as functors only on p-adic W-algebras. Then the diagram

$$\begin{tikzcd}
H^i_{\mathrm{cris}}(A \otimes k/W) \arrow[r, "\sim"] \arrow[d, "(f_0)^*"] & H^i_{\mathrm{DR}}(A/W) \arrow[r, "restriction"] & H^i_{\mathrm{DR}}(\hat{A}/W) \arrow[d, "(f)^*"] \\
H^i_{\mathrm{cris}}(B_0 \otimes k/W) \arrow[r, "\sim"] & H^i_{\mathrm{DR}}(B/W) \arrow[r, "restriction"] & H^i_{\mathrm{DR}}(\hat{B}/W)
\end{tikzcd}$$

is commutative.

Proof. If f_0 lifted, this would be obvious. But it does lift locally, which is enough for us. More precisely, let $U \subset A$ and $V \subset B$ be affine open neighborhoods of the marked W-valued points of A and B respectively such that f_0 maps $V \otimes k$ to $U \otimes k$. Because V is affine and U is smooth over W, we may successively construct a compatible system of W_n-maps $f_n: V \otimes W_n \longrightarrow U \otimes W_n$ with $f_{n+1} \equiv f_n \bmod p^n$. The f_n induce compatible maps $\hat{f}_n: \hat{B} \otimes W_n \longrightarrow \hat{A} \otimes W_n$ of formal completions, but these $\hat{f}_n$ need *not* be *pointed* morphisms.

We denote by $\hat{f}_\infty: \hat{B} \longrightarrow \hat{A}$ the limit of these $\hat{f}_n$. (Strictly speaking, $\hat{f}_\infty$ only makes sense as a map of functors when we *restrict* $\hat{B}$ and $\hat{A}$ to the category of p-adic W-algebras.)

For each n, we have a commutative diagram

$$\begin{tikzcd}
H^i_{\mathrm{DR}}(A \otimes W_n/W_n) \arrow[r, phantom, "\simeq"] \arrow[rrr, bend left, "restr."] & H^i_{\mathrm{cris}}(A \otimes k/W_n) \arrow[r, "restr."] \arrow[d] & H^i_{\mathrm{cris}}(U \otimes k/W_n) \arrow[r, phantom, "\simeq"] \arrow[d] & H^i_{\mathrm{DR}}(U \otimes W_n/W_n) \arrow[r, "restr."] \arrow[d] & H^i_{\mathrm{DR}}(\hat{A} \otimes W_n/W_n) \arrow[d] \\
H^i_{\mathrm{DR}}(B \otimes W_n/W_n) \arrow[r, phantom, "\simeq"] \arrow[rrr, bend right, "restr."'] & H^i_{\mathrm{cris}}(B \otimes k/W_n) \arrow[r, "restr."] & H^i_{\mathrm{cris}}(V \otimes k/W_n) \arrow[r, phantom, "\simeq"] & H^i_{\mathrm{DR}}(V \otimes W_n/W_n) \arrow[r, "restr."] & H^i_{\mathrm{DR}}(\hat{B} \otimes W_n/W_n)
\end{tikzcd}$$

Passing to the inverse limit over n, and using the previous lemma to identify the right-hand inverse limits, we obtain a commutative diagram

$$\begin{tikzcd}
H^i_{\mathrm{cris}}(A \otimes k/W) \arrow[r, phantom, "\simeq"] \arrow[d, "(f_0)^*"] & H^i_{\mathrm{DR}}(A/W) \arrow[r, "restriction"] & H^i_{\mathrm{DR}}(\hat{A}/W) \arrow[d, "(\hat{f}_\infty)^*"] \\
H^i_{\mathrm{cris}}(B \otimes k/W) \arrow[r, phantom, "\simeq"] & H^i_{\mathrm{DR}}(\hat{B}/W) \arrow[r, "restriction"] & H^i_{\mathrm{DR}}(\hat{B}/W).
\end{tikzcd}$$

To conclude the proof, we need to know that the induced map

$$(\hat{f}_\infty)^* : H^i_{DR}\ (\hat{A}/W) \longrightarrow H^i_{DR}\ (\hat{B}/W)$$

depends only on the underlying map $\hat{f}_0 : \hat{B} \otimes k \longrightarrow \hat{A} \otimes k$, and not on the particular choice of lifting. In fact this is true for the individual $\hat{f}_n$ as well!

Lemma 5.8.3. *Let R be a p-adic ring. Let V and V′ be formal Lie varieties over R, and let f_1 and f_2 be morphisms of functors $V' \longrightarrow V$ of the restrictions of V′, V to the category of p-adic R-algebras. If f_1 f_2 mod p, then for each i, the induced maps*

$$f_1^*, f_2^* : H^i_{DR}(V/R) \longrightarrow H^i_{DR}(V'/R)$$

are equal.

Proof. (compare Monsky [39]). In terms of coordinates $X_1, \ldots, X_n$ for V′, $Y_1, \ldots Y_m$ for V, the corresponding R-algebra homomorphisms

$$\varphi_1, \varphi_2 : R[[Y_1, \ldots, Y_m]] \longrightarrow R[[X_1, \ldots, X_n]]$$

are related by

$$\varphi_2(Y) = \varphi_1(Y) + p\,\Delta(Y).$$

Introduce a new variable T, and consider the map

$$\varphi : R[[Y_1, \ldots, Y_m]] \longrightarrow R[[X_1, \ldots, X_n, T]]$$

$$\varphi(Y) = \varphi_1(Y) + T \cdot \Delta(Y).$$

We have a commutative diagram of algebraic homomorphisms

$$\begin{tikzcd}
R[[Y]] \arrow[r, "\varphi"'] \arrow[rr, bend left=40, "\varphi_1"] \arrow[rr, bend right=40, "\varphi_2"'] & R[[X,T]] \arrow[r, shift left, "T\to 0"] \arrow[r, shift right, "T\to p"'] & R[[X]].
\end{tikzcd}$$

So it suffices to consider the situation

$$\begin{tikzcd}
R[[X,T]] \arrow[r, shift left, "T\to 0"] \arrow[r, shift right, "T\to p"'] & R[[X]]
\end{tikzcd}$$

and show that these two maps have the same effect on H_{DR}.

A form ω on R[[X,T]] may be written uniquely

$$\omega = \sum_{n\geq 0} a_n \cdot T^n + \sum_{n\geq 1} b_n T^n \frac{dT}{T}$$

with a_n, b_n's forms on R[[X]]. This form is *closed* if and only if

$$d(a_n) = 0 \quad \text{for } n \geq 0, \qquad n \cdot a_n + d(b_n) = 0 \quad \text{for } n \geq 1.$$

Its images under $T \longrightarrow 0$ and $T \longrightarrow p$ are

$$a_0 \quad , \quad \sum_{n\geq 0} a_n p^n$$

respectively. Their *difference*, if ω is closed, is exact, namely

$$\omega|_{T=0} - \omega|_{T=p} = \sum_{b\geq 1} a_n p^n = d(\sum_{n\geq 1} \frac{p^n}{n} \cdot b_n).$$

QED

It seems worthwile to point out that this last lemma can be considerably strengthened.

Lemma 5.8.4. *Let R be a p-adic ring, $I \subset R$ a divided power ideal, V and V′ two formal Lie varieties over R, and f_1, f_2 two morphisms of functors $V' \longrightarrow V$ of the restrictions of V, V′ to the category of p-adic R-algebras. If $f_1 \equiv f_2$ mod I, then for all i the induced maps*

$$f_1^*, f_2^* : H^i_{DR}\ (V/R) \longrightarrow H^i_{DR}\ (V'/R)$$

are equal.

Proof. If we had $f_1 \equiv f_2$ mod I′ with $I' \subset I$ a *finitely generated* ideal, then we could repeat the proof of the previous lemma, introducing several new variables T_i, one for each generator of I'. In particular, the lemma is true if f_1 and f_2 are *polynomial* maps in some coordinate system. But we easily reduce to this situation, for in terms of coordinates $X_1, \dots X_n$ for V', we have a $\mathbf{Z}^n$-graduation of its de Rham complex and a corresponding product decomposition

$$H^i_{DR}(V'/R) = \prod_{(a_1,\dots a_n)} H^i_{DR}(V'/R)\,(a_1, \dots a_n).$$

Therefore it suffices to show that the composite maps

$$\begin{tikzcd} H^i_{DR}\,(V/R) \arrow[r, shift left, "f_1^*"] \arrow[r, shift right, "f_2^*"'] & H^i_{DR}\,(V'/R) \arrow[r, "\text{projection}"] & H^i_{DR}\,(V'/R)(a_1, \dots, a_n) \end{tikzcd}$$

agree, for every $(a_1, \dots, a_n) \in \mathbf{Z}^n$. But for fixed $(a_1, \dots, a_n)$, these composites depend only on the terms of total degree $\leq \Sigma\, a_i$ in the power series formulas for the maps f_1, f_2. Thus we are reduced to the case when f_1 and f_2 are each *polynomial* maps. QED

REMARK 5.8.5. If the ideal I is closed, the proof gives the same invariance property for the groups $H^i_{DR}(V/R; I)$ defined as the cohomology of

$$\text{“}I\Omega^{i-1}_{V/R}\text{”} \xrightarrow{d} \Omega^i_{V/R} \xrightarrow{d} \Omega^{i+1}_{V/R}.$$

5.9. APPLICATION TO THE COHOMOLOGY OF CURVES. Throughout this section we work over a mixed-characteristic valuation ring R of residue characteristic p, which is complete for a rank-one (i.e., real-valued) valuation. Let C be a projective smooth curve over R, with geometrically connected fibres of genus g. Its Jacobian $J = \mathrm{Pic}^0(C/R)$ is a g-dimensional autodual abelian scheme over R. For each rational point $x \in C(R)$, we denote by φ_x the corresponding Albanese mapping

$$\varphi_x : C \longrightarrow J$$

given on S-valued points, S any R-scheme, by

$$\varphi_x(y) = \text{the class of the invertible sheaf } \; I(y)^{-1} \otimes I(x),$$

where I(y) denotes the invertible ideal sheaf of $y \in C(S)$ viewed as a Cartier divisor in $C \underset{R}{\times} S$. As is well-known (cf. [44], [45]), this morphism induces isomorphisms

5.9.1
$$\begin{cases} H^1(J, O_J) \xrightarrow{\sim} H^1(C, O_C) \\ H^0(J, \Omega^1_{J/R}) = \underline{\omega}_J \xrightarrow{\sim} H^0(C, \Omega^1_{C/R}) \\ H^1_{DR}(J/R) \xrightarrow{\sim} H^1_{DR}(C/R) \end{cases}$$

which are independent of the choice of the rational point x.

Let $\hat{C}_x$ denote the formal completion of C along x; it is a pointed formal Lie variety of dimension one over R. Because $\varphi_x(0) = 0$, φ_x induces a map of pointed formal Lie varieties

$$\hat{\varphi}_x : \hat{C}_x \longrightarrow \hat{J},$$

whence an induced map on cohomology

$$D(\hat{J}/R) \subset H^1_{DR}(\hat{J}/R) \xrightarrow{(\hat{\varphi}_x)^*} H^1_{DR}(\hat{C}_x/R).$$

THEOREM 5.9.2. *The composite map*

$$D(\hat{J}/R) \xrightarrow{(\hat{\varphi}_x)^*} H^1_{DR}\,(\hat{C}_x/R)$$

is injective.

COROLLARY 5.9.3. *The natural map*

$$H^0(C, \Omega^1_{C/R}) \longrightarrow H^1_{DR}(\hat{C}_x/R)$$

is injective, i.e., a non-zero differential of the first kind cannot be formally exact.

Proof. Because $\hat{J}$ is p-divisible, the natural map $\underline{\omega}_J \longrightarrow D(J/R)$ is injective.

The corollary then follows immediately from the theorem and the commutativity of the diagram

5.9.4
$$\begin{tikzcd} D(\hat{J}/R) \arrow[r, hook, "(\hat{\varphi}_x)^*"] & H^1(\hat{C}_x/R) \\ \underline{\omega}_J \arrow[u, phantom, "\cup"] \arrow[r, "\sim"] & H^0(C, \Omega^1_{C/R}). \arrow[u] \end{tikzcd}$$

To prove the theorem, we choose an integer $n \geq 2g-1$, and consider the mapping

$$\varphi_x^{(n)} : C^n \longrightarrow J$$

defined by

$$\varphi_x^{(n)}(y_1, \ldots, y_n) = \sum_{i=1}^{n} \varphi_x(y_i),$$

the summation taking place in J. Passing to formal completions, we obtain

$$\hat{\varphi}_x^{(n)} : (\hat{C}_x)^n \longrightarrow \hat{J}$$

defined by

$$\hat{\varphi}_x^{(n)}(y_1, \ldots, y_n) = \sum \varphi_x(y_i).$$

In terms of the projections

$$\hat{\mathrm{pr}}_i : (\hat{C}_x)^n \longrightarrow \hat{C}_x$$

onto the various factors, we can rewrite this as

$$\hat{\varphi}_x^{(n)} = \sum_{i=1}^{n} \hat{\varphi}_x \circ \hat{\mathrm{pr}}_i,$$

the summation taking place in the abelian group of pointed maps to $\hat{J}$. Because $\mathbf{D}(\hat{J}/R)$ is defined to consist precisely of the *primitive* elements in $H^1_{DR}(\hat{J}/R)$, we have, for any $a \in \mathbf{D}(\hat{J}/R)$,

$$(\hat{\varphi}_x^{(n)})^*(a) = \sum_{i=1}^{n} (\hat{\varphi}_x \circ \hat{\mathrm{pr}}_i)^*(a) = \sum_{i=1}^{n} (\hat{\mathrm{pr}}_i)^*(\hat{\varphi}_x)^*(a).$$

Therefore the theorem would follow from the injectivity of the map

$$(\hat{\varphi}_x^{(n)})^* : \mathbf{D}(\hat{J}/R) \longrightarrow H^1_{DR}((\hat{C}_x)^n/R).$$

Because $\mathbf{D}(\hat{J}/R)$ is a flat R-module contained in $H^1_{DR}(\hat{J}/R)$, it suffices to show that the kernel of the map

$$(\hat{\varphi}_x^{(n)})^* : H^1_{DR}(\hat{J}/R) \longrightarrow H^1_{DR}((\hat{C}_x)^n/R)$$

consists entirely of torsion elements. In fact, we will show that this kernel is annihilated by n!. To do this, we observe that the map

$$\hat{\varphi}_x^{(n)} : C^n \longrightarrow J$$

is obviously invariant under the action of the symmetric group $\mathfrak{S}_n$ on C^n

by permutation of the factors. Therefore we can factor it

$$\begin{tikzcd} C^n \arrow[r, "\pi"] \arrow[rr, bend right, "\varphi_x^{(n)}"'] & \mathrm{Symm}^n(C) \arrow[r, "\psi"] & J. \end{tikzcd}$$

Passing to formal completions, we get a factorization

$$\begin{tikzcd} (\hat{C}_x)^n \arrow[r, "\hat{\pi}"] \arrow[rr, bend right, "\hat{\varphi}_x^{(n)}"'] & \mathrm{Symm}^n(\hat{C}_x) \arrow[r, "\hat{\psi}"] & \hat{J} \end{tikzcd}$$

We will first show that $(\hat{\psi})^*$ is injective on H^1_{DR}, by showing that the map $\hat{\psi}$ has a cross-section. This in turn follows from the global fact that ψ is a $\mathbf{P}^{n-g}$-bundle over J which is locally trivial on J for the Zariski topology. To see this last point, take a Poincare line bundle $\mathscr{C}$ on $C \times J$. Because $n \geq 2g-1$, the Riemann-Roch theorem and standard base-changing results show that the sheaf on J given by $(\mathrm{pr}_2)_*(\mathscr{C} \otimes \mathrm{pr}_1^*(I^{-1}(x)^{\otimes n}))$ is locally free of rank $n+1-g$. The associated projective bundle is naturally isomorphic to ψ.

It remains only to show that the kernel of the map

$$(\hat{\pi})^* : H^1_{DR}(\mathrm{Symm}^n(\hat{C}_x)/R) \longrightarrow H^1_{DR}((\hat{C}_x)^n/R)$$

is annihilated by n!. But if a one-form ω on $\mathrm{Symm}^n(\hat{C}_x)$ becomes exact when pulled back to $(\hat{C}_x)^n$, say $\omega = df$ with $f \in A((\hat{C}_x)^n)$, then

$$n!\,\omega = \sum_{\sigma \in \mathfrak{S}_n} \sigma(\omega) = d\Big(\sum_{\sigma \in \mathfrak{S}_n} \sigma(f)\Big)$$

is exact on $\mathrm{Symm}^n(\hat{C}_x)$.

QED

REMARK. The fact that for n large the symmetric product $\mathrm{Symm}^n(C)$ is a projective bundle over J may be used to give a direct proof that C and J have isomorphic H^1's in any of the usual theories (e.g., coherent, Hodge, De Rham, etale, crystalline...).

THEOREM 5.9.5. *Let k be a perfect field of characteristic $p > 0$, $\bar{k}$ its algebraic closure, C a projective smooth curve over $W(k)$ with geometrically connected fibre, $J = \mathrm{Pic}^0(C/W(k))$ its Jacobian, $x \in C(W(k))$ a* *rational point of C, and $\varphi_x : C \longrightarrow J$ the corresponding Albanese mapping. There is an exact sequence of W-modules*

$$\begin{tikzcd}
0 \arrow[r] & (H^1_{et}(C \otimes \bar{k}, Z_p) \otimes W(\bar{k}))^{Gal(\bar{k}/k)} \arrow[r, "\alpha"] & H^1_{cris}(C \otimes k/W(k)) \arrow[r, "ß"] & H^1_{DR}(\hat{C}_x/W(k)),
\end{tikzcd}$$

the maps in which are functorial in $(C, x) \otimes k$ as pointed k-scheme.

Proof. The map α is defined exactly as was its abelian variety analogue (cf. 5.7.1); the map ß is defined as the composite

$$\begin{tikzcd}
H^1_{cris}(C \otimes k/W(k)) \arrow[r, "\sim"] \arrow[rr, bend right, "ß"'] & H^1_{DR}(C/W(k)) \arrow[r, "restr."] & H^1_{DR}(\hat{C}_x/W(k)).
\end{tikzcd}$$

By construction, α is functorial in $(C, x) \otimes k$. By lemma (5.8.2), ß is similarly functorial. To see that the sequence is *exact*, use the fact that the Albanese map induces isomorphisms on both crystalline (or de Rham!) and etale H^1's, (cf. SGAI, Exp, XI, last page, for the etale case), i.e., we have a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & (H^1_{et}(J \otimes \bar{k}, Z_p) \otimes W(\bar{k}))^{Gal} \arrow[r, "\alpha."] \arrow[d, "(\varphi_x \otimes k)^*", "\wr"'] & H^1_{cris}(J \otimes k/W(k)) \arrow[r] \arrow[d, "(\varphi_x \otimes k)^*", "\wr"'] & D(\hat{J}/W(k)) \arrow[r] \arrow[d, hook, "(\hat{\varphi}_x)^*"] & 0 \\
& (H^1_{et}(C \otimes \bar{k}, Z_p) \otimes W(\bar{k}))^{(Gal(\bar{k}/k)} \arrow[r, "\alpha"] & H^1_{cris}(C \otimes k/W(k)) \arrow[r, "ß"] & H^1_{DR}(\hat{C}_x/W(k)).
\end{tikzcd}$$

Corollary 5.9.6. *(1) The kernel of the "formal expansion at a point" map*

$$H^1_{DR}(C/W(k)) \longrightarrow H^1_{DR}(\hat{C}_x/W(k))$$

in $H^1_{DR}(C/W(k)) \simeq H^1_{cris}(C \otimes k/W(k))$ is the "slope-zero" part of the F-crystal $H^1_{cris}(C \otimes k/W(k))$, i.e., we have a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & (H^1_{et}(C \otimes \bar{k}, Z_p) \otimes W(\bar{k}))^{(Gal(\bar{k}/k)} \arrow[r] \arrow[d, equal] & H^1_{DR}(C/W) \arrow[r] & (image\ of\ H^1_{DR}(C/W)\ in\ H^1_{DR}(\hat{C}_x/W(k)) \arrow[r] & 0 \\
0 \arrow[r, dashed] & (slope\ 0) \arrow[r] & H^1_{cris}(C \otimes k/W(k)) \arrow[r] \arrow[u, "\wr"] & (slope > 0) \arrow[r] \arrow[u, "\wr"] & 0.
\end{tikzcd}$$

(2) The image of the "formal expansion at a point" map is the "slope > 0" quotient of $H^1_{cris}(C \otimes k/W(k))$; this quotient is isomorphic, via the Albanese map φ_x, to $D(\hat{J}/W(k))$.

VI. Applications to congruences and to Honda's conjecture.

Let C be a projective smooth curve over $W(F_q)$ with geometrically connected fibres. Let G be a finite group of order prime to p, all of whose absolutely irreducible complex representations are realizable over $W(F_q)$ (e.g., if the exponent of G divides $q-1$, this is automatic). Suppose that G operates on C by $W(F_q)$-automorphisms. Then G operates also on $C \otimes F_q$ by F_q-automorphisms. For each absolutely irreducible representation ρ of G, let $P_{1,\rho}(T) \in W(F_q)[T]$ be the numerator of the associated L-function $L(C \otimes F_q/F_q, G, \rho; T)$;

$$P_{1,\rho}(T) = 1 + a_1(\rho)T + \ldots + a_r(\rho)T^r.$$

Let $\omega \in H^0(C, \Omega^1_{C/W})^\rho$ be a differential of the first kind on C which lies in the ρ-isotypical component of $H^0(C, \Omega^1_{C/W})$. Let $x \in C(W(F_q))$ be a rational point on C, and let X be a parameter at x (i.e., X is a coordinate for the one-dimensional pointed formal Lie variety $\hat{C}_x$ over $W(F_q)$). Consider the formal expansion of ω around x:

$$\omega = \sum_{n \geq 1} b(n) \cdot X^n \frac{dX}{X} \qquad b(n) \in W(F_q).$$

We extend the definition of b(n) to rational numbers $n > 0$ by decreeing that $b(n) = 0$ unless n is an integer.

Theorem 6.1. *In the above situation, the coefficients $b(n)$ satisfy the congruences*

$$\frac{b(n)}{n} + a_1(\rho) \cdot \frac{b(nq)}{nq} + \ldots + a_r(\rho) \frac{b(nq^r)}{nq^r} \in pW(F_q)$$

for every rational $n > 0$.

Proof. Let J denote the Jacobian of $C/W(F_q)$, and denote by $\tilde{\omega} \in \underline{\omega}_J$ the unique invariant one-form on J which pulls back to give ω under the Albanese mapping φ_x. The group G operates, by functoriality, on J and on $\underline{\omega}_J$, and the isomorphism $\underline{\omega}_J \xrightarrow{\sim} H^0(C, \Omega^1_{C/W})$ is G-equivariant. Therefore $\tilde{\omega}$ lies in $(\underline{\omega}_J)^\rho$. Via the G-equivariant inclusion

$$\underline{\omega}_J \subset D_{(p)}(\hat{J}/W)$$

we have

$$\tilde{\omega} \in (\mathbf{D}_{(p)}(\hat{J}/W))^{\rho}.$$

Now let F denote the Frobenius endomorphism of $J \otimes \mathbf{F}_q$ relative to $\mathbf{F}_q$. Then both F and the group G act on $J \otimes \mathbf{F}_q$. By (4.2), we know that

$$(F^r + a_1(\rho)F^{r-1} + \ldots + a_r(\rho)) \cdot \mathrm{Proj}(\rho) = 0$$

in $\mathrm{End}(J \otimes \mathbf{F}_q) \underset{\mathbf{Z}}{\otimes} W(\mathbf{F}_q)$. Because $\mathbf{D}(\hat{J}/W)$ is an additive functor of $J \otimes \mathbf{F}_q$ with values in $W(\mathbf{F}_q)$-modules, and $\tilde{\omega}$ lies in its ρ-isotypical component, it follows that

6.1.1 $$F^r(\tilde{\omega}) + a_1(\rho)F^{r-1}(\tilde{\omega}) + \ldots + a_r(\rho) \cdot \tilde{\omega} = 0$$

in $\mathbf{D}_{(p)}(\hat{J}/W)$.

The Albanese map $\varphi_x : C \longrightarrow J$ induces a map

$$\hat{\varphi}_x : \hat{C}_x \longrightarrow \hat{J},$$

whence a map

$$\mathbf{D}_{(p)}(\hat{J}/W) \subset H^1_{DR}(\hat{J}/W;(p)) \xrightarrow{(\hat{\varphi}_x)^*} H^1_{DR}(\hat{C}_x;(p))$$

which is functorial in the pointed schemes $(\hat{J},0) \otimes \mathbf{F}_q$ and $(\hat{C}_x,x) \otimes \mathbf{F}_q$. So if we denote also by F the q-th power Frobenius endomorphism of $\hat{C}_x \otimes \mathbf{F}_q$, we have

$$(\hat{\varphi}_x)^* \circ F = F \circ (\hat{\varphi}_x)^*,$$

whence a relation

6.1.2 $$F^r(\omega) + a_1(\rho)F^{r-1}(\omega) + \ldots + a_r(\rho) \cdot \omega = 0$$

in $H^1_{DR}(\hat{C}_x/W;(p))$.

The asserted congruences on the b(n)'s are simply the spelling out of this relation. Explicitly, in terms of the chosen coordinate X for $\hat{C}_x$, a particularly convenient pointed lifting of F on $\hat{C}_x \otimes \mathbf{F}_q$ is provided by

$$F : X \longmapsto X^q.$$

In terms of the isomorphism

$$H^1_{DR}(\hat{C}_x/W;(p)) \xleftarrow{\sim} \frac{\{f \in K[[X]] \mid f(0) = 0, df \text{ integral}\}}{\{f \in pW[[X]] \mid f(0) = 0\}},$$

the cohomology class of ω is represented by the series

$$f(X) = \sum_{n>0} \frac{b(n)}{n} X^n,$$

and the cohomology class of $F^i(\omega)$ is represented by

$$f(X^{q^i}) = \sum \frac{b(n)}{n} X^{nq^i}.$$

The relation (6.1.3) thus asserts that

$$f(X^{q^r}) + a_1(\rho)f(X^{q^{r-1}}) + \ldots + a_r(\rho)f(X)$$

is a series whose coefficients all lie in $pW(\mathbf{F}_q)$. The congruence asserted in the statement of the theorem is precisely that the coefficient of X^{nq^r} in this series lies in $pW(\mathbf{F}_q)$. QED

REMARK. In the special case $G = \{e\}$, ρ trivial, the polynomial $P_{1,\rho}(T)$ is the numerator of the zeta function of $C \otimes \mathbf{F}_q$, and every differential of the first kind $\omega \in H^i(C, \Omega^1_{C/W})$ is ρ-isotypical. The resulting congruences on the coefficients of differentials of the first kind were discovered independently by Cartier and by Honda in the case of elliptic curves, and seem by now to be "well-known" for curves of any genus. [1],[5],[8],[22]).

THEOREM 6.2. *Hypothesis and notation as above, suppose that the polynomial $P_{1,\rho}(T)$ is linear*

$$P_{1,\rho}(T) = 1 + a_1(\rho)T,$$

i.e., that ρ occurs in H^1 with multiplicity one. Then

(1) $a_1(\rho)$ is equal to the exponential sum $S(C \otimes F_q/F_q, \rho, 1)$ and for every $n \geq 1$ we have

$$(-a_1(\rho))^n = -S(C \otimes F_q/F_q, \rho, n).$$

(2) If ρ *occurs in* $H^0(C, \Omega^1_{C/W})$, *then* $ord_p(a_1(\rho)) > 0$, *i.e.* $a_1(\rho)$ *is not a unit in* $W(F_q)$.

(3) If ρ *occurs in* $H^0(C, \Omega^1_{C/W})$, *choose* $\omega \in H^0(C, \Omega^1_{C/W})^\rho$ *to be non-zero, and such that at least one of coefficients* $b(n)$ *is a unit in* $W(F_q)$. *For any n such that* $b(n)$ *is a unit, the coefficients* $b(nq), b(nq^2), \ldots$ *are all non-zero, and we have the limit formulas (in which* $\bar{\rho}$ *denotes the contragradient representation)*

$$-S(C \otimes F_q/F_q, \rho, 1) = -a_1(\rho) = \lim_{N \to \infty} \frac{q \cdot b(nq^N)}{b(nq^{N+1})}$$

$$-S(C \otimes F_q/F_q, \bar{\rho}, 1) = -a_1(\bar{\rho}) = \frac{-q}{a_1(\rho)} = \lim_{N \to \infty} \frac{b(nq^{N+1})}{b(nq^N)}.$$

Proof. If ρ occurs in H^1 with multiplicity *one*, then ρ must be a non-trivial representation of G (for if ρ were the trivial representation, G would have a one-dimensional space of invariants in H^1; but the space of invariants is H^1 of the quotient curve $C \otimes \mathbf{F}_q$ modulo G, so is *even-dimensional*!). Therefore ρ does *not* occur in H^0 or H^2, as both of these are the trivial representation of G. The first assertion now results from (1.1).

If ρ also occurs in $H^0(C, \Omega^1_{C/W})$, pick any non-zero ω in $H^0(C, \Omega^1_{C/W})^\rho$ and look at its formal expansion around x:

$$\omega = \sum b(n) X^n \frac{dX}{X}.$$

An elementary "q-expansion principle"-argument (cf. [28]) shows that if all b(n) are divisible by p, then ω is itself divisible by p in $H^0(C, \Omega^1_{C/W})$. So after dividing ω by the highest power of p which divides all b(n), we obtain an element $\omega \in H^0(C, \Omega^1_{C/W})^\rho$ which has some coefficient a unit.

Consider the congruences satisfied by the b(n):

$$\frac{b(n)}{n} + a_1(\rho)\frac{b(nq)}{nq} \in pW(\mathbf{F}_q).$$

If $a_1(\rho)$ were a *unit*, we could infer (by induction on the precise power of p dividing n) that

$$\text{for } all\ n \geq 1, \frac{q}{p} \cdot \frac{b(n)}{n} \in W(\mathbf{F}_q).$$

In particular, we would find that $\frac{q}{p} \cdot \omega$ is *formally* exact at x, which by (5.9.3) is impossible.

Given that $a_1(\rho)$ is a non-unit, choose n such that b(n) *is* a unit. Then

$$\text{ord}\,(b(n)/n) \leq 0.$$

From the congruences

$$\frac{b(n)}{n} \equiv -a_1(\rho)\frac{b(nq)}{nq} \mod pW$$

$$\vdots$$

$$\frac{b(nq^N)}{nq^N} \equiv -a_1(\rho)\frac{b(nq^{N+1})}{nq^{N+1}} \mod pW$$

and the fact that $\text{ord}\,(a_1(\rho)) > 0$, it follows easily by induction on N that

$$\text{ord}\,(\frac{b(nq^N)}{nq^N}) = \text{ord}\,(b(n)/n) - N\,\text{ord}\,(a_1(\rho)).$$

Therefore we may *divide* the congruences, and obtain

$$\text{ord}\left(\frac{qb(nq^N)}{b(nq^{N+1})} + a_1(\rho)\right) \geq 1 + (N+1)\text{ord}(a_1(\rho)) \quad -\text{ord}(b(n)/n)$$

$$\text{ord}\left(\frac{b(nq^{N+1})}{b(nq^N)} + \frac{q}{a_1(\rho)}\right) \geq 1 + \text{ord}(\frac{q}{a_1(\rho)}) + N\,\text{ord}(a_1(\rho)) - \text{ord}(\frac{b(n)}{n}).$$

Letting N ⟶ ∞, we get the asserted limit formulas for $-a_1(\rho)$ and for $-q/a_1(\rho)$. By the Riemann Hypothesis for curves over finite fields, we know that $-q/a_1(\rho)$ is the complex conjugate $\overline{a_1(\rho)}$. Let $\bar{\rho}$ denote the contragradient representation of ρ; because the definition of the L-series $L(C \otimes \mathbf{F}_q/\mathbf{F}_q, G, \rho; T)$ is purely algebraic, the L-series for $\bar{\rho}$ is obtained by applying (any) complex conjugation to the coefficients of the L-series for ρ. Therefore $\overline{a_1(\rho)} = a_1(\bar{\rho})$, and $\bar{\rho}$ also occurs in H^1 with multiplicity one.

QED

Example 6.3. Consider the Fermat curve of degree N over $W(\mathbf{F}_q)$, with $q \equiv 1 \bmod N$. For each integer $0 \leq r \leq N-1$, denote by χ_r the character of μ_N given by

$$\chi_r(\zeta) = \zeta^r .$$

We know that under the action of $\mu_N \times \mu_N$ (acting as $(x,y) \longrightarrow (\zeta x, \zeta' y)$ in the affine model $x^N + y^N = 1$), the characters which occur in H^1 are precisely

$$\chi_r \times \chi_s \qquad 1 \leq r,s \leq N-1, r+s \neq N,$$

each with multiplicity one. Those which occur in $H^0(\Omega^1)$ are precisely the

$$\chi_r \times \chi_s \qquad 1 \leq r,s \leq N-1, r+s < N,$$

the corresponding eigen-differential $\omega_{r,s}$ is given by

$$\omega_{r,s} = x^r y^s \frac{dx}{xy^N} .$$

If we expand $\omega_{r,s}$ at the point $(x = o, y = 1)$, in the parameter x, we obtain

$$\begin{aligned}\omega_{r,s} &= x^r (1-x^N)^{\frac{s}{N}-1} \cdot \frac{dx}{x} \\ &= \sum_{j \geq 0} (-1)^j \binom{\frac{s}{N}-1}{j} x^{r+Nj} \frac{dx}{x} \\ &= \sum_{n \geq 1} b(n) x^n \frac{dx}{x} .\end{aligned}$$

Conveniently, the first non-vanishing coefficient b(r) is 1. The successive coefficients $b(rq^n)$ are given by

$$b(rq^n) = (-1)^{\frac{r}{N}(q^n-1)} \cdot \binom{\frac{s}{N}-1}{\frac{r}{N}(q^n-1)} .$$

The eigenvalue of F on the $\chi_r \times \chi_s$-isotypical component of H^1 is the *negative* of the Jacobi sum $J_q(\chi_r, \chi_s)$. There we obtain the limit formulas

$$-J_q(\chi_r, \chi_s) = \lim_{n \to \infty} \frac{(-1)^{\frac{r}{N}(q-1) \cdot q^n} \cdot q \cdot \binom{\frac{s}{N}-1}{\frac{r}{N}(q^n-1)}}{\binom{\frac{s}{N}-1}{\frac{r}{N}(q^{n+1}-1)}}$$

$$-J_q(\chi_{N-r}, \chi_{N-s}) = \lim_{n \to \infty} \frac{(-1)^{\frac{r}{N}(q-1) \cdot q^n} \cdot \binom{\frac{s}{N}-1}{\frac{r}{N}(q^{n+1}-1)}}{\binom{\frac{s}{N}-1}{\frac{r}{N}(q^n-1)}}$$

valid for $1 \leq r,s \leq N-1, r+s \neq N$. These formulas are the ones originally conjectured by Honda, and recently interpreted by Gross-Koblitz [1·'' in terms of Morita's p-adic gamma function.

VII. Application to Gauss sums.

In this chapter we will analyze the cohomology of certain Artin-Schreier curves, and then obtain a limit formula for Gauss sums in the style of the preceding section.

We fix a prime p, an integer $N \geq 2$ prime to p, and consider the smooth affine curve U over $\mathbf{Z}[1/N(p-1)]$ defined by the equation

$$T^p - T = X^N .$$

It may be compactified to a projective smooth curve C over $\mathbf{Z}[1/N(p-1)]$ with geometrically connected fibres by adding a single "point at infinity", along which $T^{-1/N}$ is a uniformizing parameter.

The group-scheme $\mu_{N(p-1)}$ operates on U, by

$$\zeta : (T,X) \longrightarrow (\zeta^N T, \zeta X).$$

This action extends to C, and fixes the point at infinity.

A straightforward computation gives the following lemma.

LEMMA 7.1. *1) The genus of C is $\frac{1}{2}(N-1)(p-1)$, and a basis of everywhere holomorphic differentials on C is given by the forms*

$$X^a T^b \frac{dT}{X^{N-1}}$$

with $0 \leq a \leq N\text{-}2, 0 \leq b \leq p\text{-}2$, and $pa + Nb < (p-1)(N-1)-1$.

(2) The space $H^1_{DR}(C \otimes Q/Q) \xrightarrow{\sim} H^1_{DR}(U \otimes Q/Q)$ has dimension $(N-1)(p-1)$, any d basis is given by the cohomology classes of the forms

$$X^a T^b \frac{dT}{X^{N-1}} \qquad 0 \leq a \leq N-2, \quad 0 \leq b \leq p-2.$$

(3) The characters of $\boldsymbol{\mu}_{N(p-1)}$ which occur in $H^1_{DR}(C \otimes Q/Q)$ are precisely those whose restrictions to $\boldsymbol{\mu}_N$ is non-trivial, and each of these occurs with multiplicity one.

In characteristic p, there are new automorphisms. The additive group $\mathbf{F}_p$ operates on $C \otimes \mathbf{F}_p$ by

$$a : (T, X) \longrightarrow (T + a, X).$$

This action does not commute with the action of $\boldsymbol{\mu}_{N(p-1)}$. However, the two together define an action of the semi-direct product

$$\mathbf{F}_p \ltimes \boldsymbol{\mu}_{N(p-1)}$$

formed via the homomorphism

$$\boldsymbol{\mu}_{N(p-1)} \xrightarrow{-N} \boldsymbol{\mu}_{p-1} \simeq \mathbf{F}_p^{\times} = \mathrm{Aut}(\mathbf{F}_p)$$

Explicitly, the multiplication is

$$(a, \zeta)(b, \zeta_1) = (a + \zeta^{-N} b, \zeta\zeta_1),$$

and the action is

$$(a, \zeta) : (T, X) \longrightarrow (\zeta^N T + \zeta^N a, \zeta X).$$

The group $\mathbf{F}_p \ltimes \boldsymbol{\mu}_{N(p-1)}$ contains $\mathbf{F}_p \times \boldsymbol{\mu}_N$ as a normal subgroup, acting on $C \otimes \mathbf{F}_p$ in the usual manner.

REMARK. This action of a group of order $p(p-1)N$ on a curve of genus $g = \frac{1}{2}(p-1)(N-1)$ provides a nice example of how "wrong" the characteristic zero estimate $84(g-1)$ can become in the presence of wild ramification!

Let E be a number field containing the $N(p-1)$ 'st roots of unity, P a p-adic place of E, $\mathbf{F}_q$ a finite extension of the residue field $F_{N(P)}$, of P, G the abstract group $\mathbf{F}_p \ltimes \boldsymbol{\mu}_{N(p-1)}(\mathbf{F}_q)$. Let H^1 denote any of the vector spaces $H^1_l(C \otimes \mathbf{F}_q) \underset{Z_l}{\otimes} E_\lambda$ for $l \neq p$, or $H^1_{cris}(C \otimes \mathbf{F}_q / W(\mathbf{F}_q)) \otimes K$. By functoriality, the group G operates on H^1. Because the center of G is $\boldsymbol{\mu}_N(\mathbf{F}_q)$, the decomposition

$$H^1 = \otimes (H^1)^\chi$$

of H^1 according to the characters of $\boldsymbol{\mu}_N$ is G-stable.

PROPOSITION 7.2. *For each of the $N-1$ non-trivial E-valued characters χ of $\boldsymbol{\mu}_N(E) \xrightarrow{\sim} \boldsymbol{\mu}_N(F_{N(P)}) = \boldsymbol{\mu}_N(F_q)$, the corresponding eigenspace $(H^1)^\chi$ is a $p-1$ dimensional absolutely irreducible representation of G; the restriction to F_p of $(H^1)^\chi$ is the augmentation representation of F_p; the restriction to $\boldsymbol{\mu}_{N(p-1)}(F_q)$ of $(H^1)^\chi$ is the induction, from $\boldsymbol{\mu}_N$ to $\boldsymbol{\mu}_{N(p-1)}$, of χ.*

Proof. All assertions except for the G-irreducibility of $(H^1)^\chi$ follow immediately from the preceding lemma, giving the action of $\boldsymbol{\mu}_{N(p-1)}$, and from Corollary (2.2), giving the action of $\mathbf{F}_p \times \boldsymbol{\mu}_N$. The irreducibility follows from these facts together with the fact that in *any* complex representation of G, the set of characters of $\mathbf{F}_p$ which occur is stable under the action of $\boldsymbol{\mu}_{N(p-1)}$ in $\mathbf{F}_p$ by conjugation; because this action has only the two orbits $\mathbf{F}_p^\times$ and 0, as soon as any one non-trivial character of $\mathbf{F}_p$ occurs, *all* non-trivial characters must also occur.

COROLLARY 7.3. *1) Over any finite extension F_q of F_p which contains all the $N(p-1)$'st roots of unity (i.e., $q \equiv 1 \bmod N(p-1)$), the Frobenius F relative to F_q operates as a scalar on each of the spaces $(H^1)^\chi$, χ a non-trivial character of $\boldsymbol{\mu}_N$. This scalar is the common value*

$$-g_q(\psi, \chi; P)$$

of the Gauss sums attached to any of the non-trivial additive characters ψ of $\boldsymbol{F}_p$.

Proof. Over such an $\mathbf{F}_q$, Frobenius commutes with the action of G on H^1, so it acts on each $(H^1)^\chi$ as a G-morphism. Because $(H^1)^\chi$ is G-irreducible, this G-morphism must be a scalar, and this scalar is equal to *any* eigenvalue of F on $(H^1)^\chi$. As we have already seen (2.1), these eigenvalues are precisely the asserted Gauss sums, corresponding to the decomposition of $(H^1)^\chi$ under $\mathbf{F}_p$.

The common value of these Gauss sums over a sufficiently large $\mathbf{F}_q$ is itself a Jacobi sum, in consequence of the fact that universally, i.e., over $Z[1/N(p-1)]$, the curve C is the *quotient* of the Fermat curve Fermat $(N(p-1))$ of degree $N(p-1)$ by the *subgroup* H of $\mu_{N(p-1)} \times \mu_{N(p-1)}$ consisting of all (ζ_1, ζ_2) satisfying

$$\zeta_1^{p-1} = \zeta_2^p$$

Explicitly, the map is given rationally by the formulas

$$\begin{gathered}(W,V) \text{ on } W^{N(p-1)} + V^{N(p-1)} = 1\\ \downarrow\\ (T,X) \text{ on } T^p - T = X^N\\ T = 1/V^N,\ X = W^{p-1}/V^p.\end{gathered}$$

LEMMA 7.4. *Let χ_1 be a character of $\mu_{N(p-1)}$ whose restriction to μ_N is non-trivial. Under the map*

$$H^1_{DR}(C\otimes Q/Q) \xrightarrow{\sim} H^1(Fermat(N(p-1))\otimes Q/Q)^H$$

we have

$$H^1_{DR}(C\otimes Q/Q)^{\chi_1} \xrightarrow{\sim} H^1_{DR}(Fermat(N(p-1))\otimes Q/Q)^{\chi_1^{p-1}\times\chi_1^{-p}}$$

Proof. That $H^1(C) \xrightarrow{\sim} H^1(\text{Fermat})^H$ in rational cohomology results from the Hochschild-Serre spectral sequence. Since the characters of $\mu_{N(p-1)}$ (resp of $\mu_{N(p-1)} \times \mu_{N(p-1)}$) occur, if at all, with multiplicity one in $H^1(C)$ (resp $H^1(\text{Fermat})$), it suffices to check that the χ_1-eigenspace of $H^1(C)$ is mapped to the $(\chi_1^{p-1}, \chi_1^{-p})$-eigenspace of $H^1(\text{Fermat})$. This

we do by inspection:

$$\begin{aligned} X^aT^b \frac{dT}{X^{N-1}} &= \\ &= X^{a+1-N}\ T^{b+1}\frac{dT}{T} \longmapsto \left(\frac{W^{p-1}}{V^p}\right)^{a+1-N} \left(Z^{-N}\right)^{b+1}\left(\frac{-NdZ}{Z}\right).\end{aligned}$$

QED

COROLLARY 7.5. *If F_q contains the $N(p-1)$'st roots of unity, then for any non-trivial character χ of μ_N, any extension χ_1 of χ to $\mu_{N(p-1)}$ and any non-trivial additive character ψ of F_p, the scalar by which F acts on $H^1(C\otimes F_q)^\chi$ is given by*

$$\left\{\begin{array}{l} F|H^1(C\otimes F_q)^{\chi} = F|H^1(C\otimes F_q)^{\psi\times\chi} = -g_q(\psi, \chi; P)\\ \qquad\quad \Vert \\ F|H^1(C\otimes F_q)^{\chi_1} = F|H^1(Fermat\otimes F_q)^{\chi_1^{p-1}\times\chi_1^{-p}} = -J_q(\chi_1^{p-1}, \chi_1^{-p}; P)\end{array}\right.$$

We now turn to the "determination" of the Gauss sum $-g_q(\psi, \chi; P)$ over an $\mathbf{F}_q$ which is merely required to contain the *N'th* roots of unity. Unless $p-1$ and N are relatively prime, such an $\mathbf{F}_q$ need *not* contain the $N(p-1)$'st roots of unity! Moreover, the Gauss sum does *not* in general lie in the Witt vectors $W(\mathbf{F}_q)$, as it does when $\mathbf{F}_q$ contains the $N(p-1)$'st roots of unity!

Let π denote any solution of

$$\pi^{p-1} = -p.$$

We recall without proof the following standard lemma (cf. [31] or [32]).

LEMMA 7.6. *The fields $Q_p(\zeta_p)$ and $Q_p(\pi)$ coincide. There is a bijective correspondence*

$$\textit{primitive p'th roots of 1} \longleftrightarrow \textit{solutions } \pi \textit{ of } \pi^{p-1} = -p$$

under which $\zeta \longleftrightarrow \pi$ if and only if

$$\zeta \equiv 1 + \pi \bmod \pi^2.$$

For each solution π of $\pi^{p-1} = -p$, we denote by

$$\psi_\pi : \mathbf{F}_p \longrightarrow \mathbf{Q}_p(\zeta_p)^\times$$

the unique non-trivial additive character which satisfies

$$\psi_\pi(1) \equiv 1 + \pi \bmod \pi^2 .$$

If we fix a $W(\mathbf{F}_q)$-valued point x on C, we have the map "formal expansion at x"

$$H^1_{\mathrm{cris}}(C \otimes \mathbf{F}_q/W(\mathbf{F}_q)) \longrightarrow H^1_{\mathrm{DR}}(\hat{C}_x \otimes W(\mathbf{F}_q)/W(\mathbf{F}_q)).$$

If we denote by R the ring

$$R = W(\mathbf{F}_q)[\pi]$$

which is a free W-module of finite rank (p−1), we may tensor with R to obtain

$$\begin{tikzcd} H^1_{\mathrm{cris}}(C \otimes \mathbf{F}_q/W(\mathbf{F}_q)) \underset{W}{\otimes} R \arrow[r] \arrow[d, "\wr"', equal] & H^1_{\mathrm{DR}}(\hat{C}_x \otimes R/R). \\ H^1_{\mathrm{DR}}(C \otimes R/R) \arrow[ur] & \end{tikzcd}$$

THEOREM 7.7. *(1) For any $W(\mathbf{F}_q)$-valued point x on C, the "formal expansion" map is injective:*

$$H^1_{\mathrm{cris}}(C \otimes \mathbf{F}_q/W(\mathbf{F}_q)) \hookrightarrow H^1_{\mathrm{DR}}(\hat{C}_x \otimes W(\mathbf{F}_q)/W(\mathbf{F}_q))$$

(2) Let π be any solution of $\pi^{p-1} = -p$, ψ_π the corresponding additive character, a an integer $1 \leq a \leq N-1$ and χ_a the corresponding nontrivial character of μ_N $(\chi_a(\zeta) = \zeta^a)$. If we take for x the point $(T = 0, X = 0)$ on C, with parameter X, then the image of

$$(H^1_{\mathrm{cris}}(C \otimes F_q/W(F_q)) \otimes Q_p(\pi))^{\psi_\pi \times \chi_a} \longrightarrow H^1_{\mathrm{DR}}(\hat{C}_x \otimes R/R) \underset{R}{\otimes} Q_p(\pi)$$

is the one-dimensional $Q_p(\pi)$-space spanned by the cohomology class of

$$exp(-\pi X^N)\, X^a \frac{dX}{X} = \sum b(n) X^n \frac{dX}{X}.$$

COROLLARY 7.8. *Notations as above, let f(X) denote the power series*

$$f(X) = \sum_{n \geq 1} b(n) \frac{X^n}{n} = \sum_{n \geq 0} \frac{(-\pi)^n}{n!} \frac{X^{nN+a}}{nN+a}.$$

Then the series

$$f(X^q) + g_q(\psi_\pi, \chi_a; \mathrm{P}) \cdot f(X)$$

has coefficients with bounded denominators, and we have a limit formula

$$7.8.1 \quad \left\{ \begin{array}{l} -g_q(\psi_\pi, \chi_a; \mathrm{P}) = \lim\limits_{r \to \infty} \dfrac{q \cdot b(aq^r)}{b(aq^{r+1})} \\ \\ \text{with } b(aq^r) = \dfrac{(-\pi)^{(q^r-1)\frac{a}{N}}}{((q^r-1)\frac{a}{N})!}. \end{array} \right.$$

We first deduce the corollary from the theorem. We know that F has eigenvalue $-g_q(\psi_\pi, \chi_a; \mathrm{P})$ on the $\psi_\pi \times \chi_a$-eigenspace of $H^1_{\mathrm{cris}} \otimes \mathbf{Q}_p(\pi)$, hence F has the same eigenvalue on the image of this one-dimensional eigenspace in $H^1_{\mathrm{DR}}(\hat{C}_x \otimes R/R) \otimes \mathbf{Q}_p(\pi)$. This image is spanned by the cohomology class of df: therefore $F + g_q(\psi_\pi, \chi_a; p)$ annihilates the class of df mod torsion, whence

$$f(X^q) + g_q(\psi_\pi, \chi_a; \mathrm{P}) \cdot f(X)$$

has bounded denominators. The final limit formula comes from looking successively at the coeficients of $X^{aq^{r+1}}$ in the above expression; one has

$$\mathrm{ord}\left(\frac{b(aq^r)}{aq^r} + g_q(\psi_\pi, \chi_a; p) \cdot \frac{b(aq^{r+1})}{aq^{r+1}} \right) \geq -A$$

for some constant A independent of r. An explicit elementary calculation shows that

$$\mathrm{ord}\left(\frac{b(aq^r)}{aq^r} \right) \longrightarrow -\infty \qquad \text{as } r \longrightarrow +\infty ,$$

and this allows us to "divide" the additive congruence and obtain the asserted limit formula.

It remains to prove the theorem. In view of the exact sequence of (5.9.5), the injectivity of

$$H^1_{\mathrm{cris}}(C \otimes \mathbf{F}_q/W(\mathbf{F}_q)) \longrightarrow H^1_{\mathrm{DR}}(\hat{C}_x \otimes W/W)$$

is equivalent to the *absence* of any p-adic unit eigenvalues of F in H^1_{cris}. But these eigenvalues are the Gauss sums

$$-g_q(\psi, \chi) \equiv -\sum \psi_q(x)\chi_q(x).$$

Because $\psi_q(x) \equiv 1\,(\pi)$ for all x, while χ_q is a *non-trivial* character of $\mathbf{F}_q^{\times}$, we have

$$-g(\psi, \chi) \equiv -\sum \chi_q(x) = 0 \bmod \pi.$$

(Alternately, one could observe that each non-trivial character χ of μ_N has at least one extension χ_1 to $\mu_{N(p-1)}$ which occurs in $H^0(C\otimes \mathbf{Q}, \Omega^1_{C\otimes \mathbf{Q}})$; the eigenvalue of F^{p-1} on this eigenspace is then a non-unit by (6.2.2); as F^{p-1} is a scalar on $(H^1)^{\chi}$, this scalar is non-unit.)

It remains to verify that the image of the $\psi_\pi \times \chi_a$-eigenspace is indeed spanned by

$$\exp(-\pi X^N) X^a \frac{dX}{X}$$

This seems to require the full strength of the Washnitzer-Monsky "dagger" cohomology, as follows. Let $A^{\dagger}$ denote the "weak completion" of the coordinate ring $R[T,X]/(T^p - T - X^N)$ of $U\otimes R$. Because $U\otimes \mathbf{F}_q$ is a "special affine variety" with corrdinate X, there are *unique* liftings to $A^{\dagger}$ of the actions of F and of the group $\mathbf{F}_p \otimes \mu_N$ whose effect on X is given by

$$\begin{cases} F(X) = X^q \\ (a,\zeta)(X) = \zeta X. \end{cases}$$

Thanks to Dwork, we know that the power series in T

$$\exp(\pi T - \pi T^p)$$

actually lies in $R[T]^{\dagger}$, and hence in $A^{\dagger}$, for any π satisfying $\pi^{p-1} = -p$. As Monsky pointed out, under the action of $\mathbf{F}_p$ on $A^{\dagger}$, this series transforms by the character ψ_π. It follows that for $1 \le a \le N-1$ the differential form

$$\exp(\pi T - \pi T^p) X^a \frac{dX}{X}$$

transforms by $\psi_\pi \times \chi_a$ under the action of $\mathbf{F}_p \times \mu_N$. Therefore its cohomology class in

$$H^1_{W-M}(U\otimes \mathbf{F}_q; R)\otimes \mathbf{Q} \overset{\text{dfn}}{=\!=} H^1(\Omega^{\bullet}_{U\otimes R/R}\otimes A^{\dagger})\otimes \mathbf{Q}$$

lies in the $\psi_\pi \times \chi_a$ eigenspace of H^1_{W-M}. A direct computation ([31], [32]) shows that each of these eigenspaces is one-dimensional, and is spanned by the above-specified form.

Furthermore, there is a natural "formal expansion map" attached to any R-valued point x of U;

$$H^1_{W-M}(U\otimes \mathbf{F}_q; R) \longrightarrow H^1_{DR}(\hat{U}_x \otimes R/R).$$

For the particular choice of point $(T = 0, X = 0)$, the formal expansion map carries

$$\exp(\pi T - \pi T^p) X^a \frac{dX}{X} \longmapsto \exp(-\pi X^N) X^a \frac{dX}{X}.$$

To conclude the proof, we need to *identify* $H^1_{WM}(U\otimes \mathbf{F}_q; R)\otimes \mathbf{Q}$ with $H^1_{\text{cris}}(C\otimes \mathbf{F}_q/R)\otimes \mathbf{Q}$ in a way compatible with the formal expansion map and with the action of F and of $\mathbf{F}_p \times \mu_N$. We will do this with a somewhat ad hoc argument.

Because U is the complement of a single point in C, it follows from the theory of residues for both H_{DR} and H_{W-M} that we have isomorphisms

$$H^1_{DR}(C\otimes R/R)\otimes \mathbf{Q} \xrightarrow{\sim} H^1_{DR}(U\otimes R/R)\otimes \mathbf{Q} \xrightarrow{\sim} H^1_{W-M}(U\otimes \mathbf{F}_q; R)\otimes \mathbf{Q}.$$

These sit in a commutative diagram

$$\begin{tikzcd}
H^1_{\text{cris}}(C\otimes \mathbf{F}_q/R)\otimes \mathbf{Q} \arrow[r] \arrow[d, "\textcircled{2}"] \arrow[dr] \arrow[rr, bend left, "\textcircled{8}"] \arrow[dddr, bend right, "\textcircled{1}"'] & H^1_{DR}(U\otimes R/R)\otimes \mathbf{Q} \arrow[r] \arrow[d] & H^1_{WM}(U\otimes \mathbf{F}_q; R)\otimes \mathbf{Q} \arrow[dl, "\textcircled{6}"] \arrow[dddl, bend left, "\textcircled{7}"] \\
(\varprojlim H^1_{\text{cris}}(U\otimes \mathbf{F}_q/R_n))\otimes \mathbf{Q} \arrow[r, "\sim", "\textcircled{5}"'] \arrow[ddr, "\textcircled{3}"] & (\varprojlim H^1_{DR}(U\otimes R_n/R_n))\otimes \mathbf{Q} \arrow[d] & \\
 & (\varprojlim H^1_{DR}(\hat{U}_x\otimes R_n/R_n))\otimes \mathbf{Q} \arrow[d, "\wr"] & \\
 & H^1_{DR}(\hat{U}_x\otimes R/R)\otimes \mathbf{Q} &
\end{tikzcd}$$

In this diagram, the maps ②, ⑤ and ⑥ are each compatible with the actions of F and of $\mathbf{F}_p \times \mu_N$ imposed by crystalline and by W-M theory (simply because these actions *lift* to the $U \otimes W_n$). Therefore the compatibility of the isomorphism ⑧ with the actions of F and of $\mathbf{F}_p \times \mu_N$ would follow from the *injectivity* of arrows ② and ⑥. The injectivity of these arrows follows from the commutativity of the diagram and the already noted injectivity of arrow ① (which is injective exactly because F has no p-adic unit eigenvalues in H^1_{cris} of our particular C). Q.E.D.

A QUESTION *(7.8.2). Let U be a smooth affine W-scheme which is the complement of a divisor with normal crossings in a proper and smooth W-scheme.*

Are the maps

$$H^1_{DR}(U/W) \otimes Q \longrightarrow (\varprojlim H^1_{DR}(U \otimes W_n/W_n)) \otimes Q$$

always injective?

7.9 THE GROSS-KOBLITZ FORMULA. In this section we will derive the Gross-Koblitz formula from our limit formulas.

Morita's p-adic gamma function is the unique continuous function

$$\Gamma_p \quad : \mathbf{Z}_p \longrightarrow \mathbf{Z}_p^\times$$

whose values on the strictly positive integers are given by the formula

$$7.91 \qquad \Gamma_p(1+n) = (-1)^{n+1} \cdot \prod_{\substack{1 \le i \le n \\ p \nmid n}} i = \frac{(-1)^{n+1} \cdot n!}{[n/p]!\, p^{[n/p]}}.$$

where [ ] denotes "integral part."

LEMMA 7.9.2. *For any integer $n \geq 0$, and any π satisfying $\pi^{p-1} = -p$, we have the identity*

$$(7.9.3) \qquad \frac{(-\pi)^n/n!}{(-\pi)^{[n/p]}/[n/p]!} = (-1) \cdot \frac{(\pi)^{n-p[n/p]}}{\Gamma_p(1+n)}.$$

PROOF. This is just a rearrangement of (7.9.1). Q.E.D.

COROLLARY 7.9.4. *Let $q = p^f$ with $f \geq 1$, π any solution of $\pi^{p-1} = -p$ and $n \geq 0$ any integer. Let*

$$n = n_0 + n_1 p + \cdots \qquad 0 \le n_i \le p-1$$

be the p-adic expansion of n. Then we have

$$7.9.5 \qquad \frac{(-\pi)^n/n!}{(-\pi)^{[n/q]}/[n/q]!} = \frac{(-1)^f \cdot (\pi)^{n_0+n_1+\cdots+n_{f-1}}}{\prod_{i=0}^{f-1} \Gamma_p(1+[n/p^i])}$$

PROOF. Simply apply (7.9.3) successively to n, [n/p], . . . [n/p^{f-1}]. Q.E.D.

For a fixed integer $i \geq 0$, the map on positive integers

$$n \longmapsto [n/p^i]$$

extends to a continuous function $\mathbf{Z}_p \longrightarrow \mathbf{Z}_p$ which we denote

$$n \longmapsto [n/p^i]_p.$$

In terms of the p-adic "digits" of n, this map is just the i-fold shift:

$$(7.9.6) \qquad n = \sum n_j p^j \longmapsto \sum_{j>0} n_{j+i}\, p^j = [n/p^i]$$

LEMMA 7.9.7. *Let $0 < \alpha < 1$ be a rational number with a prime-to-p denominator. If $p^f = 1$ mod denom (α) for some $f \geq 1$, then we have the identity*

$$(7.9.8) \qquad -<p^{f-1}\alpha> = [-\alpha/p^i]_p \ \textit{in}\ \mathbf{Z}$$

for $i = 0, 1, \ldots, f-1$ (where< > denotes the "fractional part" of a rational number).

PROOF. Write $(p^f - 1)\alpha = A$. Then A is an integer, $0 < A < p^f - 1$, so we may write its p-adic expansion as

$$A = a_0 + a_1 p + \ldots + a_{f-1} p^{f-1}; \qquad \begin{array}{l} 0 \le a_i \le p-1 \\ a_i < p-1 \text{ for } \textit{some}\ i. \end{array}$$

We now *extend* the definition of a_n to *all* n $\in \mathbf{Z}$ by requiring

$$a_n = a_{n+f} \qquad \forall\, n \in \mathbf{Z}.$$

Then

$$p^{f-i}\alpha = p^{f-i}\frac{A}{p^f-1} = \frac{\sum_{j=0}^{f-1} a_j p^{f+j-i}}{p^f-1}$$

$$\equiv \frac{\sum_{j=0}^{f-1} a_{j+i} p^j}{p^f-1} \bmod \mathbf{Z}$$

whence

$$-<p^{f-i}\alpha> = \frac{\sum_{j=0}^{f-1} a_{j+i}p^j}{1-p^f} = \sum_{j\geq 0} a_{j+i}p^j$$

$$= \left[\frac{\sum_{j\geq 0} a_j p^j}{p^i}\right]_p$$

But we readily calculate

$$-\alpha = \frac{A}{1-p^f} = \sum_{j\geq 0} a_j p^j.$$

QED

Corollary 7.9.9. *Let $q = p^f$ with $f \geq 1$, π any solution of $\pi^{p-1} = -p$, and α any rational number satisfying*

$$\begin{cases} 0 \leq \alpha \leq 1 \\ (q-1)\,\alpha \in \mathbf{Z}. \end{cases}$$

Let

$$A = (q-1)\,\alpha = a_0 + a_1 p + \ldots + a_{f-1}p^{f-1}, \qquad 0 \leq a_i \leq p-1$$

be the p-adic expansion of $(q-1)\,\alpha$, and let

$$S(\,(q-1)\,\alpha\,) = a_0 + a_1 + \ldots + a_{f-1}$$

be the sum of the p-adic digits of $(q-1)\,\alpha$. Then we have the formula

$$(7.9.10) \qquad \lim_{n\to-\alpha} \frac{(-\pi)^n/n!}{(-\pi)^{[n/q]}/[n/q]!} = \frac{(-1)^f\cdot(\pi)^{S((q-1)\alpha)}}{\prod_{i=0}^{f-1}\Gamma_p(1-<p^i\alpha>)}$$

in which the limit is taken over positive integers n which approach $-\alpha$ p-adically.

Proof. Simply combine (7.9.5) and (7.9.8), and use the p-adic continuity of both Γ_p and of $n \longrightarrow [n/p^i]$ QED

Combining this last formula with our limit formula for Gauss sums, we obtain the Gross-Koblitz formulas.

Theorem 7.10. *(Gross-Koblitz). Let $N \geq 2$ prime to p, E a number field containing the Np'th roots of unity, P a p-adic place of E, $\pi \in E_P$ a solution of $\pi^{p-1} = -p$, ψ_π the corresponding additive character of $\mathbf{F}_p$, a an integer $1 \leq a \leq N-1$, χ_a the corresponding characer $\zeta \longmapsto \zeta^a$ of μ_N, and $\mathbf{F}_q$, $q = p^f$, a finite extension of the residue field $F_{N(P)}$ of E at P. We have the formulas, in E_P,*

$$(7.10.1) \qquad -g_q(\psi_\pi, \chi_a; P) = \frac{(-1)^f\cdot q\cdot \prod_{i \bmod f}\Gamma_p(i-<\frac{p^i a}{N}>)}{(\pi)^{S((q-1)\frac{a}{N})}}$$

$$(7.10.2) \qquad -g_q(\psi_\pi, \overline{\chi}_a; P) = (\pi)^{S((q-1)\frac{a}{N})} \prod_{i \bmod f}\Gamma_p(<\frac{p^i a}{N}>)$$

Proof. The sequence $n_r = (q^r-1)(a/N)$ tends to $-a/N$ as r grows, and satisfies $[n_r/q] = n_{r-1}$ for $r \geq 1$. Therefore the first formula follows from the limit formula (7.8.1) and from the preceding formula (7.9.10) with $\alpha = a/N$. The second formula is obtained from the first by replacing a by N−a. QED

VIII. Interpretation via the De Rham-Witt Complex. Throughout this chapter, we fix an algebraically closed field k of characteristic p, and a proper smooth connected scheme X over its Witt vectors W = W(k). For each n ≥ 1, we denote by X_n the W_n-scheme $X \underset{W}{\otimes} W_n$.

The "second spectral sequence" of de Rham cohomology of X_n/W_n

$$E_2^{p,q}(n) = H^p(X_n, \mathscr{H}^q_{DR}(X_n/W_n)) \Rightarrow H^{p+q}(X_n/W_n)$$

has an intrinsic interpretation in terms of $X \otimes k$ as the Leray spectral sequence for the "forget the thickening" map

$$(X \otimes k/W_n)_{cris} \longrightarrow (X \otimes k)_{Zar} .$$

As such, it may be rewritten

$$E_2^{p,q}(n) = H^p(X \otimes k, \mathscr{H}^q_{cris}(X \otimes k/W_n)) \Rightarrow H^{p+q}_{cris}(X \otimes k/W_n).$$

An explicit construction of this spectral sequence may be given in terms of the De Rham-Witt pro-complex on $X \otimes k$

$$\{W_n\Omega^{\bullet}\}_n$$

of Deligne and Illusie; it is simply the second spectral sequence of this complex:

$$E_2^{p,q}(n) = H^p(X \otimes k, \mathscr{H}^q(W_n\Omega^{\cdot})) \Rightarrow H^{p+q}(X \otimes k, W_n\Omega^{\cdot}).$$

It is known that the E_2 terms of this spectral sequence are finitely generated $W_n(k)$-modules. Therefore we may pass to the inverse limit and obtain a spectral sequence

$$E_2^{p,q} = \varprojlim_n E_2^{p,q}(n) \Rightarrow H^{p+q}_{cris}(X \otimes k/W).$$

Let x be a W-valued point of X, and assume X connected. The formal expansion map we have exploited

$$H^i_{cris}(X \otimes k/W) \simeq H^i_{DR}(X/W) \longrightarrow H^i_{DR}(\hat{X}_x/W)$$

is the composition of the edge-homomorphism

$$H^i_{cris}(X/W) \twoheadrightarrow E_\infty^{o,i} \hookrightarrow E_2^{0,i}$$

with the natural map

$$E_2^{0,i} = \varprojlim_n H^0(X_n, \mathscr{H}^i_{DR}(X_n/W_n)) \longrightarrow \varprojlim H^i_{DR}(\hat{X}_x \otimes W_n/W_n).$$

LEMMA 8.1. *This map is in fact injective; indeed, the induced maps*

$$H^0(X_n, \mathscr{H}^i_{DR}(X_n/W_n)) \longrightarrow H^i_{DR}(\hat{X}_x \otimes W_n/W_n)$$

are injective.

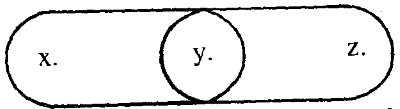
Proof. Because X_n is irreducible, it suffices to show

(*) for any closed point y of X_n, and any affine open V ∋ y which is étale over standard affine space $A = \mathrm{Spec}(W_n[T_1, \ldots, T_d])$, the natural map

$$H^0(V, \mathscr{H}^i_{DR}(X_n/W_n)) \longrightarrow \mathscr{H}^i_{DR}(\hat{V}_y/W_n).$$

is injective.

For once (*) is established we argue as follows. Let ξ be a global section over X_n of $\mathscr{H}^i_{DR}$ which dies formally at x. We must show that for any closed point z in X_n, there is an open set V ∋ z such that ξ dies on V. Let U be an affine open neighborhood of x étale over A, and V an affine open neighborhood of z étale over A. Because X_n is irreducible, U ∩ V is non-empty. Let y be a closed point of X_n contained in U ∩ V.



Then (*) for U ∋ x shows that ξ dies on U. Therefore ξ dies formally at y. Applying (*) to V ∋ y, we find that ξ dies on V, as required.

We now prove (*). Let $F: A \longrightarrow A^{(\sigma)}$ be *any* σ-linear map lifting absolute Frobenius (e.g. $T_i \longrightarrow T_i^p$). Because V is étale over A, F extends uniquely to a σ-linear map $F: V \longrightarrow V^{(\sigma)}$ which lifts absolute Frobenius. Because all iterates of F, especially $F^n: V \longrightarrow V^{(\sigma^n)}$, are homeomorphisms, the functor $(F^n)_*$ is exact. Therefore we have

$$\begin{cases} H^0(V, \mathscr{H}^i_{DR}(V/W_n)) = H^0(V^{(\sigma^n)}, (F_n)_*(\mathscr{H}^i_{DR}(V/W_n))) \\ (F^n)_*\mathscr{H}^i_{DR}(V/W_n) = \mathscr{H}^i((F^n)_*(\Omega^{\bullet}_{V/W_n})) \end{cases}$$

But the complex $(F^n)_*(\Omega^{\bullet}_{V/W_n})$ on $V^{(\sigma^n)}$ is a complex of locally free sheaves of finite rank on $V^{(\sigma^n)}$, with $\mathcal{O}$-linear differential. For any closed point y V, the formal stalk at $y^{(\sigma^n)}$ is

$$(F^n)_*(\Omega^\bullet_{V/W_n}) \underset{\mathcal{O}_{V^{(\sigma^n)}}}{\otimes} \widehat{\mathcal{O}}_{V^{(\sigma^n)},y^{(\sigma^n)}} \simeq (F^n)_* \Omega^\bullet_{\hat{V}_y/W_n}.$$

Therefore the sheaves on $V^{(\sigma^n)}$

$$\mathscr{F}^i = \mathscr{F}^i_{V/W_n} \overset{\mathrm{dfn}}{=} (F^n)_*(\mathscr{H}^i_{DR}(V/W_n)) = \mathscr{H}^i((F^n)_*\Omega^\bullet_{V/W_n})$$

are *coherent*, and (by flatness of the completion) their formal stalks are given by

$$(\hat{\mathscr{F}}^i)_{y^{(\sigma^n)}} = H^i_{DR}(\hat{V}_y/W_n)$$

We must show that

$$H^\circ(V^{(\sigma^n)},\mathscr{F}^i) \hookrightarrow (\hat{\mathscr{F}}^i)_{y^{(\sigma^n)}}.$$

For this, it suffices to explicit a finite filtration

$$\mathscr{F}^i \supset \mathrm{Fil}^1\mathscr{F}^i \supset \ldots$$

whose associated graded sheaves are *locally free sheaves* on $V^{(\sigma^n)} \otimes k$. We claim that the filtration induced by the p-adic filtration on $\Omega^\bullet V/W_n$ has this property.

To see this, we first reduce to the case V = A, as follows. The diagram

$$\begin{tikzcd} V \arrow[r, "F^n"] \arrow[d] & V^{(\sigma^n)} \arrow[d] \\ A \arrow[r, "F^n"] & A^{(\sigma^n)} \end{tikzcd}$$

is cartesian (because V is étale over A). Therefore we have an isomorphism

$$(F^n)_* \Omega^\bullet_{V/W_n} \xleftarrow{\sim} ((F^n)_*\Omega^\bullet_{A/W_n}) \underset{\mathcal{O}_{A^{(\sigma^n)}}}{\otimes} \mathcal{O}_{V^{(\sigma^n)}}.$$

Because $\mathcal{O}_{V^{(\sigma^n)}}$ is *flat* over $\mathcal{O}_{A^{(\sigma^n)}}$, this isomorphism is a filtered isomorphism (for the p-adic filtrations of $\Omega^\bullet_{V/W_n}$ and of $\Omega^\bullet_{A/W_n}$).

By flatness again, this filtered isomorphism induces isomorphisms

$$gr^j_{Fil}(\mathscr{F}^i_{V/W_n}) \simeq (gr^j_{Fil}\mathscr{F}^i_{A/W_n}) \underset{\mathcal{O}_{A^{(\sigma^n)}}}{\otimes} \mathcal{O}_{V^{(\sigma^n)}}$$

It remains to show that $gr^j_{Fil}(\mathscr{F}^i_{A/W_n})$ is a locally free sheaf on $A^{(\sigma^n)} \otimes k$. It is certainly a *coherent* sheaf on $A^{(\sigma^n)}$ (because the p-adic filtration on $(F^n)_*\Omega^\bullet_{A/W_n}$ is $\mathcal{O}_{A^{(\sigma^n)}}$-linear), and it is killed by p; therefore it is a coherent sheaf on $A^{(\sigma^n)} \otimes$ k. Because it is coherent, it is locally free on a non-void open set; if we knew that it were translation-invariant, i.e. isomorphic to all it translates by k-valued points of $A^{(\sigma^n)} \otimes$ k, we would conclude that it is locally free everywhere.

As a sheaf of abelian groups, it is visibly translation-invariant. It's $\mathcal{O}_{A^{(\sigma^n)}\otimes k}$-module structure is the composite of its natural module-structure over the sheaf of rings

$$gr^o_{Fil}\mathscr{H}^o_{DR}(A/W_n)$$

with the σ^n-linear isomorphism

$$\mathcal{O}_{A\otimes k} \xrightarrow{\sim} gr^o_{Fil}\mathscr{H}^\circ(A/W_n)$$
$$f \longmapsto (F^n)^*(\tilde{f}) \quad ,$$

where $\tilde{f}$ denotes any local section of $\mathcal{O}_A$ lifting f.

To conclude the proof, we must verify that this isomorphism is translation-invariant. For this, it suffices to show that it is independent of the *particular choice* of F lifting Frobenius which figures in its definition. For this independence, we simply notice that an "intrinsic" description of the same σ^n-linear isomorphism

$$\mathcal{O}_{A\otimes k} \xrightarrow{\sim} gr^o_{Fil}\mathscr{H}^\circ(A/W_n)$$

is provided by

$$f \longmapsto (\tilde{f})^{p^n}$$

where again $\tilde{f} \in \mathcal{O}_A$ denotes any lifting of f. QED

LEMMA 8.2. *The $E_2^{i,0}$ terms of the spectral sequence are given by*

$$E_2^{i,0} \simeq H^i_{et}(X \otimes k, Z_p) \otimes W(k)$$

Proof. For each integer n ≥ 1, there is an isomorphism (cf. [24], [25])

$$W_n(O_{X\otimes k}) \xrightarrow{\sim} \mathscr{H}^0_{DR}(X_n/W_n)$$

defined by

$$(g_0, \dots, g_{n-1}) \longmapsto \sum_{i=0}^{n-1} p^i (\tilde{g}_i)^{p^{n-i}}$$

where $\tilde{g}_i$ is a local lifting of $g_i \in O_{X \otimes k}$ to O_{X_n} (Compare (5.52)).

For variable n, these isomorphisms sit in a commutative diagram

$$\begin{tikzcd}
W_{n+r}(O_{X \otimes k}) \arrow[r, "\sim"] \arrow[d, "\text{usual projection}"] & \mathscr{H}^0_{DR}(X_{n+r}/W_{n+r}) \arrow[dd, "\text{reduction mod } p^n"] \\
W_n(O_{X \otimes k}) \arrow[d, "F^r"] & \\
W_n(O_{X \otimes k}) \arrow[r, "\sim"] & \mathscr{H}^0_{DR}(X_n/W_n).
\end{tikzcd}$$

Therefore we may calculate

$$\begin{aligned}
E_2^{i,0} &= \varprojlim_n H^i(X \otimes k, \mathscr{H}^0_{DR}(X_n/W_n)) \\
&\xrightarrow{\sim} \varprojlim_n \left(\bigcap_r (\text{image of } F^r \text{ on } H^i(X \otimes k, W_n(O_{X \otimes k}))\right). \\
&\simeq \varprojlim (\text{fixed points of } F \text{ in } H^i(X \otimes k, W_n(O_{X \otimes k})) \underset{Z/p^n Z}{\otimes} W_n(k) \\
&\simeq \varprojlim_n H^i_{et}(X \otimes k, Z/p^n Z) \otimes W_n(k).
\end{aligned}$$

QED

Consider now the exact sequence of terms of low degree

$$0 \longrightarrow E_2^{1,0} \longrightarrow H^1_{cris}(X \otimes k/W) \longrightarrow E_2^{0,1} \xrightarrow{d_2} E_2^{2,0}$$

LEMMA 8.3. *The map $d_2^{0,1} : E_2^{0,1} \longrightarrow E_2^{2,0}$ vanishes*

Proof. Because both $H^1_{cris}(X \otimes k/W)$ and $E_2^{2,0} = H^2_{et}(X \otimes k, Z_p) \otimes W_j$ are finitely generated W-modules, we see that $E_2^{0,1}$ is a finitely generated W-module. Therefore its inverse limit topology (as $\varprojlim E_2^{0,1}(n)$) is equivalent to its p-adic topology. Because F^n annihilates the sheaf $\mathscr{H}^1_{cris}(X \otimes k/W_n)$, it annihilates its global sections $E_2^{0,1}(n)$, and hence F is topologically nilpotent on $E_2^{0,1}$. But F is an *automorphism* of the finitely generated W-module $E_2^{2,0}$; as d_2 commutes with F, this forces $d_2^{0,1}$ to *vanish*.

QED

Thus we obtain the following theorem.

THEOREM 8.4. *The exact sequence of terms of low degree*

$$\begin{tikzcd}
0 \arrow[r] & H^1_{et}(X \otimes k, Z_p) \otimes W \arrow[r] & H^1_{cris}(X \otimes k/W) \arrow[r] \arrow[d, "\wr"'] & E_2^{0,1} \arrow[r] \arrow[d, hook] & 0 \\
& & H^1_{DR}(X/W) \arrow[r, "\text{formal}", "\text{expansion}"'] & H^1_{DR}(\hat{X}_x/W) &
\end{tikzcd}$$

defines the Newton-Hodge filtration on H^1_{cris}

$$0 \longrightarrow (slope\, 0) \longrightarrow H^1_{cris}(X \otimes k/W) \longrightarrow (slope > 0) \longrightarrow 0.$$

[When X/W is a curve, or an abelian scheme, this exact sequence coincides with the exact sequence ((5.7.2) or (5.9.5)!]

Illusie and Raynaud have recently been able to generalize these results to H^i_{cris} for all i. Their remarkable result is the following.

THEOREM 8.5. *(Illusie-Raynaud). Let X_0 be proper and smooth over an algebraically closed field of characteristic $p > 0$. The second spectral sequence of the De Rham-Witt complex*

$$E_2^{p,q} = \varprojlim_n H^p(X_0, \mathscr{H}^q(W_n \Omega^\bullet)) \Rightarrow H^{p+q}_{cris}(X_0/W)$$

degenerates at E_2 after tensoring with Q:

$$E_2^{p,q} \underset{Z}{\otimes} Q \simeq E_\infty^{p,q} \underset{Z}{\otimes} Q, d_r \otimes Q = 0 \text{ for } r \geq 2,$$

and defines the Newton-Hodge filtration on $H_{cris}(X_0/W) \otimes Q$:

$$q - 1 < \text{slopes of } E_2^{p,q} \otimes Q \leq q.$$

COROLLARY 8.6. *If X_0/k lifts to X/W, then for any W-valued point x of X, and any integer i, the image of the formal expansion map*

$$H^i_{cris}(X \otimes k/W) \otimes Q \simeq H^i_{DR}(X/W) \otimes Q \longrightarrow H^i_{DR}(\hat{X}_x/W) \otimes Q$$

is precisely the quotient "slopes $> i-1$" of $H^i_{cris} \otimes Q$.

REFERENCES

1. Atkin, A. O. L. and P. H. F. Swinnerton-Dyer, : Modular forms on non-congruence subgroups. *Proc. Symposia Pure Math* XIX, 1–25, A. M. S. (1971).

2. Berthelot, P. : *Cohomologie Cristalline des Schémas de Caracteristique* $p > 0$. Springer Lecture Notes in Math 407, Springer-Verlag (1974).

3. Berthelot, P. and A. Ogus, : *Notes on Crystalline Cohomology*. Princeton University Press (1978).

4. Bloch, S. : Algebraic K-theory and crystalline cohomology. *Pub. Math. I. H. E. S.* 47, 187–268 (1978).

5. Cartier, P. : Groupes formels, fonctions automorphes et fonctions zeta des courbes elliptiques, *Actes, 1970 Congrés Intern. Math.* Tome 2, 291–299 (1971).

6. Deligne, P. : La conjecture de Weil I *Pub. Math. I. H. E. S.* 43, 273–307 (1974)

7. ————: Sommes trigonometriques, S. G. A. $4\frac{1}{2}$, *Cohomologie Etale*. Springer Lecture Notes in Math 569, Springer Verlag (1977).

8. Ditters, B. : *On the congruences of Atkin and Swinnerton-Dyer*. Report 7610, February 1976, Math Inst. Kath. Unis, Nijmegen, Netherlands (preprint).

9. Dwork, B. : On the zeta function of a hypersurface. *Pub. Math. I. H. E. S.* 12 (1962).

10. ————: On the zeta function of a hypersurface II. *Ann. Math.* (2) (80), 227–299 (1964).

11. ————: Bessel functions as p-adic functions of the argument. *Duke Math. J.* vol. 41, no. 4, 711–738 (1974).

12. M. Boyarsky, : P-adic gamma functions and Dwork cohomology, to appear in *T.A.M.S.*

13. Fontaine, J.-M. : *Groupes p-divisibles sur les corps locaux*. Asterisque 47–48, Soc. Math. France (1977).

14. Gross, B. H. and N. Koblitz, : Gauss sums and the p-adic Γ-functions. *Ann. Math.* vol. 109, no. 3 (1979).

15. Gross, B. H. : On the periods of abelian integrals and a formula of Chowla-Selberg, with an appendix by David Rohrlich. *Inv. Math.* 45, 193–211 (1978).

16. Grothendieck, A. : *Revêtements Etales et Groupe Fondamental (SGA 1)*. Springer Lecture Notes in Math. 244, Springer-Verlag (1971).

17. ————: Groupes de Barsotti-Tate et Cristaux. *Actes du Cong. Intern. Math.* 1970, tome 1, 431–436 (1971).

17 bis. ————: Groupes de Barsotti-Tate et cristaux de Dieudonné. *Sem. Math. Sup.* 45, Presses Univ. de Montréal (1970).

18. ————: Formule de Lefschetz et rationalité des fonctions L. *Exposé 279, Seminaire Bourbaki* 1964/65.

19. Hartshorne, R. : On the de Rham cohomology of algebraic varieties. *Pub. Math. I. H. E. S.* 45, 5–99 (1976).

20. Hasse, H. : Theorie der relativ-zyklischen algebraischen Funktionenkörpér, insbesondere bei endlichem Konstantenkörpér. *J. Reine Angew. Math.* 172, 37–54 (1934).

21. ———— and H. Davenport : Die Nullstellen der Kongruenz zeta-funktionen in gewissen zyklischen Fällen. *J. Reine Angew. Math.* 172, 151–182. (1934).

22. Honda, T. : On the theory of commutative formal groups. *J. Math. Soc. Japan*, 22, 213–246 (1970).

23. ————: On the formal structure of the Jacobian variety of the Fermat curve over a p-adic integer ring. *Symposia Matematica* XI, Istituto Nazionale Di Alta Matematica, 271–284, Academic Press (1973).

24. Illusie, L. : Complex de DeRham-Witt et cohomologie cristalline. to appear.

25. ————: Complex de DeRham-Witt. *Proceedings of the 1978 Journeés de Géométrie Algebriques de Rennés*, to appear in Asterisque.

26. ———— and M. Raynaud, : work in preparation.

27. Katz, N. : Nilpotent connections and the monodromy theorem. *Pub. Math. I. H. E. S.* 39, 175–232 (1970).

28. ————: *P-adic properties of modular schemes and modular forms.* Proc. 1972 Antwerp Summer School, Springer Lecture Notes in Math 350, 70–189 (1973).

29. ———— and W. Messing, : Some consequences of the Riemann hypothesis for varieties over finite fields. *Inv. Math.* 23, 73–77 (1974).

30. ————: *Slope filtration of F-crystals.* Proceedings of the 1978 Journeés de Géométrie Algébrique de Rennes, to appear in Asterisque.

31. Koblitz, N. : *A short course on some current research in p-adic analysis.* Hanoi, 1978, preprint.

32. Lang, S. : *Cyclotomic Fields II.* Springer Verlag.

33. LAZARD, M.: Lois de groupes et analyseurs. *Ann. Sci. Ec. Norm. Sup. Paris* 72, 299–400 (1955).

34. ———: *Commutative Formal Groups*. Springer Lecture Notes in Math. 443, Springer-Verlag (1975).

35. MAZUR, B. and W. MESSING,: *Universal Extensions and One-Dimensional Crystalline Cohomology*. Springer Lecture Notes in Math. 370, Springer-Verlag (1974).

36. MESSING, W.: *The Crystals Associated to Barsotti-Tate Groups*. Springer Lecture Notes in Math 264, Springer-Verlag (1972).

37. ———: The universal extension of an Abelian variety by a vector group. *Symposia Matematica* XI, Istituto Nazionale Di Alta Matematica 358–372, Academic Press (1973).

38. MONSKY, P.: *P-adic analysis and zeta functions*. Lectures at Kyoto University, Kinokuniya Book Store, Tokyo or Brandeis Univ. Math. Dept. (1970).

39. ——— and G. WASHNITZER,: Formal Cohomology I. *Ann. Math.* 88, 181–217 (1968).

40. ———: One-dimensional formal cohomology, *Actes, 1970 Congrés Intern. Math.* Tome 1, 451–456 (1971).

41. MORITA, Y.: A p-adic analogue of the Γ-function. *J. Fac. Sci. Univ.* Tokyo 22, 255–266 (1975).

42. MUMFORD D.: *Geometric Invariant Theory*. Springer-Verlag (1965).

43. ———: *Abelian Varieties*. Oxford Univ. Press (1970).

44. ODA, T.: The first de Rham cohomology group and Dieudonné modules. *Ann. Sci. Ec. Norm. Sup. Paris*, 3iéme serie, Tome 2, 63–135 (1969).

45. SERRE, J.-P.: *Groupes Algébriques et Corps de Classes*. esp. Chapt VII, Hermann (1959).

46. WEIL, A.: On some exponential sums. *Proc. Nat. Acad. Sci. U.S.A.* 34, 204–207 (1948).

47. ———: Number of solutions of equations in finite fields. *Bull. A. M. S.* 497–508 (1949).

48. ———: Jacobi sums as Grössencharaktere. *Trans. A. M S.* 73, 487–495 (1952).

ESTIMATES OF COEFFICIENTS OF MODULAR FORMS AND GENERALIZED MODULAR RELATIONS

By S. RAGHAVAN

WE SHALL BE concerned here with two questions, motivated by arithmetic, from the theory of modular forms. The first one deals with the estimation of the magnitude of the Fourier coefficients of Siegel modular forms, while the second pertains to certain generalized modular relations (which may also be called Poisson formulae of Hecke type and) which appear to provide some kind of a link between automorphic forms (of one variable), representation theory and arithmetic.

§ Modular forms of degree n

Let $r_m(t)$ denote the number of ways in which a natural number t can be written as a sum of m squares of integers. We have the well-known Hardy-Ramanujan asymptotic formula [H-R] for $m > 4$:

$$r_m(t) = \pi^{m/2}\ \sigma_m(t)\, t^{(m/2)-1} / \Gamma(m/2) + O(t^{m/4}) \tag{1}$$

with $\sigma_m(t)$ denoting the 'singular series'. Arithmetical functions such as $r_m(t)$ or, more generally, the number $A(S, t)$ of m-rowed integral columns x with ${}^t x\, S\, x = t$ for a given m-rowed integral positive-definite matrix S (where ${}^t x$ = transpose of x) occur as Fourier coefficients of modular forms. While Hardy and Ramanujan used the 'circle method' to prove (1), the approach of Hecke [H1] to (1) was via the decomposition of the space of (entire) modular forms into the subspace generated by Eisenstein series and the subspace of cusp forms, the explicit determination of the Fourier expansion of Eisenstein series and the estimation of the Fourier coefficients c(t) of cusp forms of weight k as $c(t) = O(t^{k/2})$.

More generally, let $A(S, T)$ be the number of integral matrices G such that ${}^t G S G = T$ for n-rowed integral T (For any matrix B, let ${}^t B$ denote its transpose and for a square matrix C, let tr(C) and det C denote its trace and determinant respectively). For $A(S, T)$, we have, as a 'generating function', the theta series $\vartheta(S, Z) = \sum_G \exp(2\pi\sqrt{-1}\,\mathrm{tr}({}^t G S G Z))$ where