ON THE COEFFICIENTS OF DRINFELD MODULAR FORMS

ERNST-ULRICH GEKELER

Max-Planck-Institut
für Mathematik
Gottfried-Claren-Str. 26

5300 Bonn 3

MPI/87-14

Contents

ON THE COEFFICIENTS OF DRINFELD MODULAR FORMS

ERNST-ULRICH GEKELER

Introduction

Let E_k be the Eisenstein series of weight k, defined on the complex upper half-plane H. The coefficients of E_k in its q-expansion ($q = \exp(2\pi iz)$) are given by constant times $\sigma_{k-1}(n)$, where σ_k is the arithmetic function defined by $\sigma_k(n) = \Sigma\, d^k$, d running through the set of divisors of n. Many interesting properties of σ_k (and of related arithmetic functions like Ramanujan's function $\tau(n)$, or the partition function $p(n)$) may be derived from function theoretic and algebro-geometric properties of E_k (or of other modular forms). These results, which include integrality and congruence properties, orders of magnitude, as well as various "unexpected" identities, justify to state that the coefficients of modular forms like E_k, or the discriminant function Δ, contain a good portion of the arithmetic of $\mathbb{Z}$.

Let now $A = \mathbb{F}_q[T]$ be the polynomial ring over a finite field $\mathbb{F}_q$ in an indeterminate T, and replace $\mathbb{Z}$ by A as our object of basic interest. There is a deep analogy between A and $\mathbb{Z}$:

- A is an euclidean ring;
- A is discretely embedded in K_∞, the completion of $K = \mathrm{Quot}(A) = \mathbb{F}_q(T)$ at the infinite place;
- similar to Kronecker's theorem, (abelian) class field theory of K may explicitely be described by "cyclotomic" polynomials; etc..

Amongst the reasons for investigating A or similar rings, let us just mention Langlands's program to develop non-abelian class field theory, or the applications in coding theory.

In 1973, making an attempt to extend the analogy to include modular forms theory, Drinfeld introduced the notion of "elliptic module", nowadays called Drinfeld module. Roughly, the idea is as follows: Classical modular forms may be considered as homogeneous functions on the set of lattices (+ some extra structure) $\Lambda \subset \mathbb{C}$. The set of similarity classes of lattices is canonically parametrized by $\Gamma \backslash H$, where Γ is the modular group $SL(2,\mathbb{Z})$, or some congruence subgroup. Now $\Gamma \backslash H$ is the set of complex points of an affine algebraic curve X_Γ which is defined over an abelian number field, and modular forms correspond to certain multi-differentials on X_Γ. Thus, Drinfeld was led to study discrete rank two lattices $\Lambda \subset C$, where now $C = \hat{\bar{K}}_\infty$ = completion of an algebraic closure $\bar{K}_\infty$ of K_∞ replaces the field $\mathbb{C}$. By means of the lattice function e_Λ (which is similar to a Weierstraß $\wp$-function), the "analytical" object Λ may be "algebraically" interpreted as some sort of diophantine object, namely a rank two Drinfeld module over C . (By the way, there is no reason to restrict to rank two A-lattices Λ: The rank r of Λ may be any natural number, leading to rank r Drinfeld modules. Secondly, A may be an arbitrary function ring $A = \mathcal{O}(X)$, where $X = \bar{X} \setminus \{\infty\}$ is the complement of one closed point in a smooth projective curve $\bar{X}$ over $\mathbb{F}_q$.) As in the classical case, the set of classes of such Λ is in bijection with $\Gamma \backslash \Omega$, where now $\Omega = C \backslash K_\infty$ is the "Drinfeld upper half-plane " acted upon by $\Gamma = GL(2,A)$.

Now Ω is a rigid analytic space of dimension one over C , and the function theoretic apparatus applies.

There are two different translations of classical modular forms theory into our context (perhaps converging some day):

(i) Representation theoretic point of view. The algebraic description of Drinfeld modules implies the existence of a modular scheme (a certain A-scheme of relative dimension one) whose C-points will agree with $\Gamma \backslash \Omega$. Considering Galois actions on (the cohomology of) that scheme yields l-adic representations of $Gal(\bar{K}:K)$. The main result is Drinfeld's reciprocity law Thm. 2 in [2] which states a 1-1 correspondence between (certain) Galois representations of K and (certain) cuspidal automorphic representations of $GL(2,\mathbb{A})$, where $\mathbb{A}$ is the Adele ring of K .

As a corollary, a variant of Taniyama/Weil's conjecture is true, i.e. each elliptic curve over K having a prescribed reduction behavior at ∞ may be parametrized by some Drinfeld modular curve!

(ii) Function theoretic point of view. Letting Λ vary with $z \in \Omega$, the coefficients of the corresponding Drinfeld module become modular forms, i.e. holomorphic functions $\Omega \longrightarrow C$ that satisfy the usual transformation rule with respect to $\gamma \in \Gamma$ and some holomorphy conditions at "cusps". There is a canonical uniformizer t "at infinity" which replaces $q = \exp(2\pi i z)$, and the t-expansion of a modular form f is defined. Thus we may study the coefficients of f. The main results known in this case include product expansions of certain distinguished modular forms which imply rationality, integrality, and congruence properties for the coefficients, dimensions of spaces of modular forms, and some statements on the geometry of the algebraic curve associated with $\Gamma \backslash \Omega$, see [7].

The results mentioned in (i) and (ii) are of a general nature and do not make use of $A = \mathbb{F}_q[T]$, i.e. are valid for $A = \mathcal{O}(X)$ arbitrary. The aim of this paper is to get a better understanding of the expansion coefficients, now restricting to the special case $A = \mathbb{F}_q[T]$ as defined above, and considering modular forms for the full group Γ only. In that case, there are two distinguished modular forms g and Δ that have integer (i.e. in A) coefficients, and the C-algebra M° of modular forms of type zero is the polynomial ring $C[g,\Delta]$ generated by g and Δ. (This result has first been obtained by D. Goss [11].) Hence we are forced to investigate g and Δ. In [5], we proved a product expansion for Δ which is entirely analogous with Jacobi's formula for the discriminant function of elliptic curves. From this formula, one derives the existence of a $(q-1)$-th root h of $-\Delta$ as a function on Ω. Its transformation law involves the determinant character $\det: \Gamma \longrightarrow \mathbb{F}_q^*$. This leads to an extension of the definition of modular form (compared to that given in [11] or [7]) which is necessary even for a full understanding of g and Δ.

We will systematically use the series $G_{k,\Lambda}(X)$ of Goss polynomials of a (finite or infinite) $\mathbb{F}_q$-lattice $\Lambda \subset C$. Remember the occurrence of $\sigma_k(n)$ in the q-expansion of classical modular forms comes from the formula

$$(*) \qquad \sum_{n\in\mathbb{Z}} (z+n)^{-k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{n\geq 1} n^{k-1} q^n$$

which is valid for $k \geq 2$. Now, as Goss observed, if Λ is a discrete $\mathbb{F}_q$-submodule of C, the sum $S_{k,\Lambda} = \Sigma (z+a)^{-k}$ (a running through Λ) is a polynomial $G_{k,\Lambda}$ of degree k in the meromorphic function $S_{1,\Lambda}$. This already gives first results on the expansions of Eisenstein series $E^{(k)}$, and on the Hecke eigenvalues of Δ [11]. As we shall see, the $G_{k,\Lambda}$ are a good substitute for (*). But note there is no number theoretic counterpart of $G_{k,\Lambda}$ if Λ is finite since $\mathbb{C}$ has no finite subgroups.

Specifying the generating function $G = \Sigma\, G_k(X)\, U^k$, we are able to compute G_k which yields a particularly simple formula in the most interesting case where k is of the form q^i-1. The resulting coefficients of $E^{(k)}$ are slightly more complicated than $\sigma_k(n)$. They involve arithmetic functions like

$[i] = T^{q^i} - T$ = product of monic primes of degree dividing i, or

D_i = product of all monics of degree i.

They are further related with the "cyclotomic" polynomials $f_a(X)$ $(a \in A)$ which are true analogues of $1 - X^a$ $(a \in \mathbb{Z})$. Using the G_k that correspond to certain finite $\mathbb{F}_q$-lattices (groups of torsion points of the Carlitz module), we are able to describe the effect of Hecke operators on the t-expansions (which was unknown before). As should be remarked, our Hecke operators behave rather differently from the number field case. For example:

- $T_{(p^2)} = (T_p)^2$ for a prime p;
- g (of weight $q-1$) and Δ (of weight q^2-1) possess the same eigenvalues;
- there is no Euler product for the coefficients of eigenforms, due to the fact that the set of positive divisors of A does not agree with $\mathbb{N}$.

In order to relate additive and multiplicative expansions of modular forms, we introduce the differential operator ∂ on the ring $M = C[g,h]$ of modular forms (any weight and type) whose definition relies heavily on the product for Δ . We are giving three different characterizations of the form h :
(i) $h = \sqrt[q-1]{-\Delta}$; (ii) $h = P_{q+1,1}$ (a certain Poincaré series); (iii) $h = \partial g$, and sketch a fourth one related to modular forms for congruence subgroups. Besides giving an identity of two a priori entirely different expansions, this solves the problem of determining the expansion of $P_{q+1,1}$ which had been defined in [8].

Let now p be a fixed prime ideal of A of degree d , and let M_p the ring of modular forms having expansion coefficients in K with denominator prime to p . Let further
$\tilde{M} = \{\tilde{f} \in A/p((t)) \mid \exists\ f \in M_p \text{ s.t. } f \bmod p \equiv \tilde{f}\}$ be the A/p-algebra of modular forms mod p. In [18], Swinnerton-Dyer has determined the structure of the number theoretic counterpart of $\tilde{M}$, involving a prime number $p > 3$. His result is in short:
(*) $\tilde{E}_{p-1} \equiv 1$ (reduction mod p of the Eisenstein series of weight $p-1$) , and (*) is the only relation, i.e. each congruence mod p is implied by (*). In our case, we first define the Hasse invariant H "in characteristic p". H is a modular form mod p that measures the group of p-torsion points of a Drinfeld module. Our results concerning $\tilde{M}$ are:

(A) $g_d \equiv 1 \bmod p$, where g_d is the normalized Eisenstein series of weight q^d-1 ;

(B) $H \equiv g_d \bmod p$;

(C) if $B_d(X,Z)$ is the A-polynomial such that $B_d(g,h) = g_d$, and $\sim$ denotes reduction $\bmod p$, $(A/p)[X,Z]/(\tilde{B}_d-1) \xrightarrow{\cong} \tilde{M}$, where X resp. Z maps to g resp. h mod p .

Note the differences with [18]: a result corresponding to (C) is first proved for H , then we use (A) and (B) to get (C). Further, there are no special primes like p = 2,3 in number theory. Going deeper into the modular theory of Drinfeld modules, a geometric description of Spec $\tilde{M}$ might be given. Suffice to say for the moment that $\tilde{M}$ is normal, i.e. a Dedekind ring.

The plan of the article is as follows: in the first two sections, we fix notations and give the necessary background of Drinfeld modules and lattice functions. Next, the notion of Goss polynomial for a lattice is defined which will be our basic technical tool in various situations. After having introduced the Carlitz module and the relevant arithmetic functions (i.e. the one-dimensional theory), some important examples of modular forms are given, and the ring of modular forms is described. In section 6, we derive the t-expansion of Eisenstein series and draw some conclusions. By means of the coefficient description of Hecke operators given in section 7, we easily determine the eigenvalues on Δ (first obtained by D. Goss) and on h . Next, we introduce the "false Eisenstein series" E and use it to define the differential operator ∂ by which we relate g and h . Section 10 presents computations of the t-expansions of the product function U and of the functions E,g,h,g_2 , and Δ up to the (roughly) q^3-th (or q^4-th) term, the bound depending on the function in question. These computations are valid independently of q . Finally, in the last two sections, modular forms mod p are investigated, and the assertions (A), (B), (C) are proved.

The congruence results may (possibly) be generalized into two directions:

(i) consider congruence subgroups Γ' of Γ ; i.e. modular forms "with level";

(ii) replace A by a more general function ring $\mathcal{O}(X)$ as indicated above; i.e. take the point of view of [7].

Whereas (i) should cause no serious problems, still some work will have to be done for (ii). In order to define the expansion of an algebraic modular form, one has to consider a family of Tate--Drinfeld modules $TD^{(\mathfrak{a})}$, where $\mathfrak{a}$ runs through the ideal class group of A . But $TD^{(\mathfrak{a})}$, which will have its coefficients in the normalizing field of A (notations as in [7]) , will not be defined canonically. Thus, one arrives at a problem of normalizing $TD^{(a)}$ (as well as the Hasse invariant) that still has to be solved.

Occasionally, our methods involve some easy analysis in C like convergence of infinite sums, interchanging summation orders etc.. The philosophy is not to worry about such questions, nearly everything being clear from the non-archimedean property of C .

Let me finally confess that I regard as a non-trivial problem to find adequate terminology for the theory presented here. Good notation should be a) consistent; b) simple; c) reflect the classical notation, whenever possible, and d) be in accordance with some basic articles like [2], [7], or [12]. Unfortunately, these conditions seem to conflict, and I had to make a compromise which, perhaps, may appear unsatisfactory. For compensation, I added an extensive index for symbols with a global meaning.

1. Notations

Let $\mathbb{F}_q$ be the finite field with q elements. Throughout the paper, $A = \mathbb{F}_q[T]$ and $K = \mathbb{F}_q(T)$ denote the ring of polynomials and the field of rational functions in an indeterminate T, respectively. On K, we consider the degree valuation deg: $K \longrightarrow \mathbb{Z} \cup \{-\infty\}$ $x \longmapsto \deg x$ associated with the infinite place "∞" of K. The corresponding absolute value "$|\ |$" is normalized by $|T| = q$. Completing K with respect to $|\ |$, we obtain the field $K_\infty = \mathbb{F}_q((T^{-1}))$ of formal Laurent series in T^{-1}. The absolute value $|\ |$ has a unique extension, also denoted by $|\ |$, to an algebraic closure $\bar{K}_\infty$ of K_∞. The completion C of $\bar{K}_\infty$ is an algebraically closed complete valued field of positive characteristic, determined up to isomorphism by its value group $q^{\mathbb{Q}} \subset \mathbb{R}$ and its residue class field $\bar{\mathbb{F}}_q$ = alg. closure of $\mathbb{F}_q$.

For a ring R and $r \in R$, R^*, (r), R/r denote the multiplicative group, the principal ideal generated by r, the factor ring $R/(r)$ respectively. Further, (r,s) is the g.c.d. of r and s, and $r|s$ means r divides s. If f is a power series in t, $f = o(t^k)$ says f is divisible by t^k.

2. Review of Drinfeld modules and lattices

By an $\mathbb{F}_q$-lattice (resp. A-lattice) in C, we understand an $\mathbb{F}_q$-submodule (resp. A-submodule) Λ of C having finite intersection with each ball $B \subset C$ of finite radius. For such Λ, we define the lattice function

(2.1) $$e_\Lambda(z) = z \prod_{\lambda\in\Lambda}{}' (1 - z/\lambda) ,$$

where as usual, $\prod'$ (resp. Σ') denotes the product (resp. sum) over the non-zero elements of a lattice. The product converges, locally uniformly on bounded sets in C, and defines a function $e_\Lambda : C \longrightarrow C$ whose essential properties are summarized as follows:

(2.2) (i) e_Λ is entire (in the rigid analytic sense) and surjective;

(ii) e_Λ is $\mathbb{F}_q$-linear and Λ-periodic;

(iii) e_Λ has simple zeroes at the points of Λ, and no further zeroes;

(iv) if $\Lambda, \Lambda' = c\Lambda$ $(c \in C^*)$ are similar lattices, their functions are related by $ce_\Lambda(z) = e_{\Lambda'}(cz)$;

(v) $\dfrac{de_\Lambda}{dz} = e'_\Lambda = 1$, so we have the identity of meromorphic functions

$1/e_\Lambda(z) = e'_\Lambda(z)/e_\Lambda(z) = \Sigma\, 1/(z - \lambda)$ $(\lambda \in \Lambda)$.

All of this is easily seen by first assuming Λ to be finite, then choosing an exhausting sequence $\Lambda_i \subset \Lambda$ consisting of finite sublattices and going over to the limit. Let now Λ be an A-lattice of rank r, and $0 \neq a \in A$. In the diagram

(2.3)
$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda & \longrightarrow & C & \xrightarrow{e_\Lambda} & C & \longrightarrow & 0 \\ & & \downarrow a & & \downarrow a & & \downarrow \phi_a & & \\ 0 & \longrightarrow & \Lambda & \longrightarrow & C & \longrightarrow & C & \longrightarrow & 0 , \end{array}$$

the map $\phi_a = \phi_a^\Lambda$ is uniquely determined by commutativity. In fact, ϕ_a is an additive polynomial, and $\phi^\Lambda : a \longmapsto \phi_a^\Lambda$ defines a ring homomorphism of A into the ring $\mathrm{End}_C(G_a)$ of additive polynomials over C. $\mathrm{End}_C(G_a)$ is the non-commutative ring of polynomials of the form $\Sigma\, a_i X^{p^i}$ $(p = \mathrm{char}(\mathbb{F}_q))$, where "multiplication" is defined by substitution. Let $\tau = X^q$ and $C\{\tau\} \subset \mathrm{End}_C(G_a)$ the subalgebra generated by τ, i.e. the non-commutative polynomial ring in τ with the commutator rule $z^q\tau = \tau z$ $(z \in C)$. Then ϕ^Λ takes values in $C\{\tau\}$, and for $a \in A$ of degree d, we have

(2.4)
$$\phi_a = \sum_{0 \le i \le rd} \ell_i \tau^i ,$$

where (i) $\ell_0 = a$ and (ii) $\ell_{rd} \neq 0$.

(2.5) For an arbitrary field L over A (e.g. $L = K$, or $L = A/\mathfrak{p}$, where $\mathfrak{p}$ is a maximal ideal of A), a ring homomorphism $\phi : A \longrightarrow L\{\tau\}$ satisfying (2.4) is called a <u>Drinfeld module</u> of rank r over L . By means of ϕ , the additive group scheme G_a over L gets a new structure as an A-module. An element x in some extension field of L which is annihilated by ϕ_a is called an a-division point of ϕ . The a-division points constitute a finite A-submodule scheme of G_a of degree $|a|^r$.

(2.6) Now the above association $\Lambda \longmapsto \phi^\Lambda$ is a bijection of the set of A-lattices of rank r in C with the set of Drinfeld modules of rank r over C , i.e. one may reconstruct Λ by means of $\phi = \phi^\Lambda$. First observe the power series expansion

$$e_\Lambda(z) = \Sigma\ \alpha_i z^{q^i}$$

resulting from the $\mathbb{F}_q$-linearity of e_Λ. By $e'_\Lambda = 1$, there exists a composition inverse

$$\log_\Lambda(z) = \Sigma\ \beta_i z^{q^i}$$

which has a positive radius of convergence. Let $d = \deg a > 0$ and

$$\phi_a(z) = \sum_{i \leq rd} \ell_i z^{q^i} \quad , \ \ell_i = \ell_i(a,\Lambda) \ .$$

Applying $\log_\Lambda$ on both sides of $e_\Lambda(az) = \phi_a(e_\Lambda(z))$, we obtain

$$a \log_\Lambda(z) = \log_\Lambda(\phi_a(z)) ,$$

i.e. for $k \geq 0$

(2.7) $$a\beta_k = \sum_{i+j=k} \beta_i \ell_j^{q^i} ,$$

which, in view of $\ell_0 = a$, gives a recursive procedure for computing the β_k from ϕ_a . Finally, Λ is determined as the set of zeroes of e_Λ = composition inverse of

$\Sigma\ \beta_i z^{q^i}$.

(2.8) We still need another type of lattice invariants.

Write $z/e_\Lambda(z) = \Sigma\ \gamma_i z^i$. Now

$$z/e_\Lambda(z) = z\ \Sigma\ 1/(z-\lambda) \qquad (\lambda \in \Lambda)$$

$$= \Sigma\ 1/(1-\lambda/z)$$

$$= 1 - \Sigma'\ (z/\lambda)/(1-z/\lambda)$$

$$= 1 - \sum_{k\geq 1} E^{(k)}(\Lambda) z^k ,$$

where $E^{(k)}(\Lambda) = \sum'_{\lambda\in\Lambda} \lambda^{-k}$ is the Eisenstein series of weight k for Λ. An easy induction shows:

(2.9) For $j = q^k - q^i$, we have $\gamma_j = \beta_{k-i}^{q^i}$.

Putting $E^{(0)}(\Lambda) = -1$ and using (2.7), we obtain the important relation, valid for $k \geq 0$:

$$(2.10) \qquad a \cdot E^{(q^k-1)} = \sum_{i+j=k} E^{(q^i-1)} \ell_j^{q^i} .$$

all the terms involved depending on Λ.

3. Goss polynomials

For convenience, we first recall the well known Newton formulae for power sums of the zeroes of a polynomial. Let

$$f(X) = X^n + a_1 X^{n-1} + \ldots \quad a_{n-1}X + a_n$$

be a monic polynomial over an arbitrary field, and let S_k be the sum of k-th powers of the zeroes of f (multiplicities counted). Then the following relations hold for $k \in \mathbb{N}$:

$$(3.1) \qquad S_k + a_1 S_{k-1} + \ldots \qquad + a_{k-1}S_1 + ka_k = 0 \qquad (k \leq n)$$

$$S_k + a_1 S_{k-1} + \ldots \qquad + a_{k-n+1}S_{k-n+1} + a_k S_{k-n} = 0 \qquad (k \geq n) .$$

Let now Λ be a fixed $\mathbb{F}_q$-lattice in C which we first assume to be finite, of dimension m over $\mathbb{F}_q$. Put

$$(3.2) \qquad e(z) = e_\Lambda(z) = z \prod_{\lambda \in \Lambda}{}' (1 - z/\lambda) = \sum_{i \leq m} \alpha_i z^{q^i}$$

and

$$t(z) = t_\Lambda(z) = \Sigma\, 1/(z - \lambda) = e_\Lambda^{-1}(z) .$$

The polynomial $e(X - z) = e(X) - e(z)$ over $C(z)$ has $\{z + \lambda \mid \lambda \in \Lambda\}$ as its set of zeroes, whereas $\{1/(z + \lambda) \mid \lambda \in \Lambda\}$ appears as the set of zeroes of the "inverse polynomial" $\tilde{f}(X) = e(X^{-1} - z)X^{q^m} \in C(z)[X]$. From $\alpha_0 = 1$ results the leading coefficient $-e(z)$ of $\tilde{f}(X)$, so

$$f(X) = -e^{-1}(z) \cdot e(X^{-1} - z)X^{q^m}$$

$$= X^{q^m} - \sum_{0 \leq i \leq m} t\alpha_i X^{q^m - q^i}$$

is monic, and we may compute $S_k = S_{k,\Lambda} = \Sigma(z + \lambda)^{-k}$ via Newton. Putting $S_0 = 0$, we obtain for $k \geq 2$

$$(3.3) \qquad S_k = t(S_{k-1} + \alpha_1 S_{k-q} + \alpha_2 S_{k-q^2} + \dots) ,$$

where the sum involves those α_i with $k - q^i \geq 0$ only. Note this includes both cases of (3.1). If Λ is no longer finite, we still define S_k by the same formula. The sum is easily seen to converge outside of Λ, defining a meromorphic function on C with poles at most at Λ.

3.4. Proposition ([12], Ch. VI): Let Λ be a not necessarily finite $\mathbb{F}_q$-lattice in C. There exists a polynomial $G_k = G_{k,\Lambda}$ with the following properties:

(i) $S_k = G_k(t)$, where $t = t_\Lambda = S_{1,\Lambda}$;

(ii) $G_k(X) = X(G_{k-1} + \alpha_1 G_{k-q} + \ldots + \alpha_i G_{k-q^i} + \ldots)$, $k - q^i \geq 0$;

(iii) G_k is monic of degree k;

(iv) $G_k(0) = 0$;

(v) $k \leq q \Rightarrow G_k = X^k$;

(vi) $G_{pk} = (G_k)^p$, $p = \mathrm{char}(\mathbb{F}_q)$;

(vii) $X^2 G_k'(X) = kG_{k+1}$.

Proof: Assume first Λ to be finite. The existence of G_k and (i) - (v) then follow from (3.3). We further have

$$G_{pk}(t) = \Sigma\ (z-\lambda)^{-pk} = (\ \Sigma\ (z-\lambda)^{-k})^p = G_k(t)^p \text{ , i.e. (vi) .}$$

For (vii), we compute

$$\frac{d}{dz} S_{k,\Lambda}(z) = -kS_{k+1,\Lambda}(z) = -kG_{k+1}(t) .$$

On the other hand, $\frac{dt}{dz} = \frac{d}{dz} e_{\Lambda}^{-1}(z) = -e_{\Lambda}^{-2}(z) = -t^2$, thus $\frac{d}{dz} S_{k,\Lambda}(z) = G_k'(t) \frac{dt}{dz} = -t^2 G_k'(t)$. Let now Λ be infinite, $\Lambda_1 \subset \Lambda_2 \subset \dots$ a sequence of finite sublattices with $\cup \Lambda_i = \Lambda$, and let e_i, t_i, $S_{k,i}$, $G_{k,i}$ the objects corresponding to Λ_i . Elementary estimates show

a) $e_i \longrightarrow e_\Lambda$ locally uniformly as functions on C ;

b) $S_{k,i} \longrightarrow S_k$ uniformly on closed balls which are disjoint from Λ .

This in turn implies the coefficientwise convergence of $G_{k,i}$ against a polynomial G_k having the properties stated.

(3.5) For each lattice Λ , we call $G_{k,\Lambda}(X)$ the <u>k-th Goss polynomial of Λ</u> $(k \geq 1)$. We further put $G_0 = 0$. Now fix Λ and consider the generating function.

$$G(U,X) = \sum_{k\geq 0} G_k(X) U^k .$$

(3.4 ii) translates to

$$G(U,X) - XU = XU\, G(U,X) + \alpha_1 XU^q G(U,X) + \dots ,$$

i.e. $$G(U,X) = \frac{XU}{1 - XU - \alpha_1 XU^q - \alpha_2 XU^{q^2} - \dots}$$

(3.6) $$= \frac{XU}{1 - Xe_\Lambda(U)} .$$

<u>3.7. Example:</u> Let $\Lambda = \mathbb{F}_q \cdot \lambda$ be one-dimensional, so $e_\Lambda(z) = z + \alpha z^q$, $\alpha = -\lambda^{1-q}$, and

$$G(U,X) = XU \sum_{j\geq 0} (U + \alpha U^q)^j X^j$$

$$= XU \sum_{j\geq 0} \sum_{i\geq 0} \binom{j}{i} U^{j-i}\alpha^i U^{iq} X^j$$

$$= XU \sum_{k\geq 0} \sum_{i\geq 0} \binom{k-i(q-1)}{i} \alpha^i X^{k-i(q-1)} U^k .$$

Thus $G_{k+1}(X) = \sum_{0\leq i\leq k/q} \binom{k-i(q-1)}{i} \alpha^i X^{k-i(q-1)+1}$.

Proceeding similarly, we get for an arbitrary lattice Λ with $e_\Lambda = \sum \alpha_i z^{q^i}$

(3.8) $$G_{k+1,\Lambda}(X) = \sum_{j\leq k} \sum_{\underline{i}} \binom{j}{\underline{i}} \alpha^{\underline{i}} X^{j+1} .$$

Here $\underline{i} = (i_0, \dots, i_s)$ runs over the set of $(s+1)$-tuples (s arbitrary) satisfying $i_0 + \dots + i_s = j$ and $i_0 + i_1 q + \dots + i_s q^s = k$. Further, $\alpha^{\underline{i}} = \alpha_0^{i_0} \cdots \alpha_s^{i_s}$, and $\binom{j}{\underline{i}}$

denotes the multinomial coefficient $j!/(i_0! \ldots i_s!)$.

<u>3.9. Corollary:</u> Let Λ be of finite dimension m over $\mathbb{F}_q$. Then $G_{k,\Lambda}(X)$ is divisible by X^n where $n = [kq^{-m}] + 1$.

It seems difficult to evaluate the sums occuring in (3.8) in general. However for special k , we can say more.

<u>3.10. Proposition:</u> Let Λ be an $\mathbb{F}_q$-lattice in C with log--function (see(2.6)) $\log_\Lambda(z) = \Sigma\, \beta_i z^{q^i}$. If k is of the form $k = q^j - 1$, we have

$$G_{k,\Lambda}(X) = \sum_{i<j} \beta_i X^{q^j - q^i}$$

<u>Proof:</u> We put $P(X) = G_k(X^{-1})X^{k+1}$ and $Q(X) = \sum_{i<j} \beta_i X^{q^i}$, so we have to show $P(X) = Q(X)$. Now both $P(X)$ and $Q(X)$ are polynomials of degree $< q^j$, and it will suffice to see that $P(e(z))$ and $Q(e(z))$ agree as power series in z up to the term of order $q^j - 1$ ($e = e_\Lambda$ the lattice function of Λ) . But

$$P(e(z)) = G_k(e^{-1}(z))e^{q^j}(z) = e^{q^j}(z) \sum_{\lambda\in\Lambda} (z-\lambda)^{1-q^j}$$

$$= e^{q^j}(z)(z^{1-q^j} + \Sigma'\ (z-\lambda)^{1-q^j}) .$$

The sum Σ' contains no terms z^{-i} with negative exponents, and $e^{q^j}(z) = (z + \ldots)^{q^j} = z^{q^j} + \ldots$, so $P(e(z)) = z + o(z^{q^j})$.

On the other hand, $Q(e(z)) = \sum_{i<j} \beta_i (e(z))^{q^i} = z + o(z^{q^j})$ for Q is the partial sum of $\log_\Lambda$.

3.11. Corollary: Let $s \neq 0$ be fixed. Then

$$\sum_{c\in \mathbb{F}_q} (z - cs)^{1-q^j} = \sum_{0\leq i<j} s^{1-q^i} t(z)^{q^j-q^i} ,$$

where $t(z) = 1/(z - s^{1-q}z^q)$.

Proof: This is the case $\Lambda = \mathbb{F}_q \cdot s$, noting that $e_\Lambda(z) = z - s^{1-q}z^q$ and $\log_\Lambda(z) = \sum_{i\geq 0} s^{1-q^i} z^{q^i}$.

4. The Carlitz module

(4.1) The most important Drinfeld module for $A = \mathbb{F}_q[T]$ is Carlitz's module ρ of rank one, defined by

$$\rho_T = T\tau^0 + \tau = TX + X^q .$$

It has been studied by several authors, e.g. [1], [13], [9]. Under the bijection of (2.6), ρ corresponds to a certain one-dimensional A-lattice $L = \bar{\pi} A$, where the "period" $\bar{\pi}$ is well-defined up to an element of $\mathrm{Aut}(A) = \mathbb{F}_q^*$, i.e. a $(q-1)$-th root of unity. We choose one such $\bar{\pi}$ and fix it once for all. In the sequel, $e(z) = e_L(z)$, $t(z) = e_L^{-1}(\bar{\pi} z) = \bar{\pi}^{-1} e_A^{-1}(z)$ and $G_k = G_{k,L}$ will always denote the functions associated with L . Then $t(z)$ will play the role of the exponential function $\exp(2\pi i z)$ in the classical context. In order to describe these functions, we have to introduce some A-valued arithmetic functions. For $i \in \mathbb{N}$, put

$$(4.2) \qquad [i] = T^{q^i} - T$$

$$D_i = [i][i-1]^q \ldots [1]^{q^{i-1}}$$

$$L_i = [i][i-1] \ldots [1] ,$$

and $D_0 = L_0 = 1$. Then $[i]$ equals the product of all monic primes whose degree divides i , D_i the product of all monics of degree i , and L_i the ℓ.c.m. of all monics of degree i . As is easily verified from (2.7) ,

$$(4.3) \qquad e(z) = \sum_{i \geq 0} D_i^{-1} z^{q^i} \qquad \text{and}$$

$$\log_L(z) = \sum_{i \geq 0} (-1)^i L_i^{-1} z^{q^i} .$$

Note the difference in sign with [9], due to the modified definition of the Carlitz module. Let now a be an arbitrary non-zero element of A , and $\rho_a = \sum \ell_i(a)\tau^i$. From $\rho_{aT} = \rho_a\rho_T = \rho_T\rho_a$ in $\mathrm{End}_C(G_a)$, the recursion formula

$$(4.4) \qquad \ell_i = \frac{\ell_{i-1}^q - \ell_{i-1}}{[i]} \qquad (i \geq 1)$$

results. From $\ell_0 = a$, we see for $0 \leq i \leq d$

$$(4.5) \qquad \deg \ell_i = (d-i)q^i \leq (q^d - q^i)/(q-1) \ .$$

Define the <u>a-th cyclotomic polynomial</u> $f_a(X) \in A[X]$ by

$$(4.6) \qquad f_a(X) = \rho_a(X^{-1})X^{|a|} \ ,$$

considering ρ_a as a polynomial in X , i.e. replacing τ by X^q . Then $f_a(X)$ has degree $|a| - 1$, leading coefficient a , and $f_a(0)$ = leading coefficient of a . Actually, f_a is a polynomial in X^{q-1} . For example, $f_1(X) = 1$,
$f_T(X) = TX^{q-1} + 1$, $f_{T^2}(X) = T^2X^{q^2-1} + (T^q + T)X^{q^2-q} + 1$.
In the following formulae, let $a,b \in A$, a monic,
$d' = \deg b < \deg a = d$.

(4.7)

(i) $$f_{a+b} = f_a + X^{q^d - q^{d'}} f_b \ ;$$

(ii) $$\prod_{c \in \mathbb{F}_q} f_{aT+c} = f_{aT}^q - X^k f_{aT} \ , \quad k = (q^{d+1} - 1)(q-1) \ ;$$

(iii) $$f_{aT} = f_a^q + TX^k f_a \ , \quad k = q^d(q-1) \ .$$

Here, (i) is obvious, (ii) follows from (i), and (iii) from $\rho_a\rho_T = \rho_T\rho_a$.

The reason for investigating ρ comes from the next theorem.

<u>4.8. Theorem</u> [13]:

(i) The roots λ of ρ_a generate an abelian extension $K(a)$ of K with Galois group $(A/a)^*$.

(ii) If σ_b corresponds to the residue class of b mod a then $\sigma_b(\lambda) = \rho_b(\lambda)$.

(iii) The fixed field $K_+(a)$ of $\mathbb{F}_q^* \hookrightarrow (A/a)^*$ (a assumed non-constant) is the ray class field of a, i.e. the maximal abelian extension of K that splits completely at ∞ and whose conductor divides a.

Note that $K(a)$ = splitting field of f_a (resp. $K_+(a)$ = splitting field of $\tilde{f}_a$, where $\tilde{f}_a(X^{q-1}) = f_a(X)$), and $K(a) : K_+(a)$ is unramified at finite places and totally ramified above ∞. Although we do not need all of them, we will write down some formulae for the period $\bar{\pi}$ of ρ:

(4.9) $$\bar{\pi}^{q-1} = [1]\, E^{(q-1)}(A) = (T^q - T) \sum_{a \in A}{}' a^{1-q} ;$$

(4.10) $$\bar{\pi}^{q-1} = -[1] \prod_{i \geq 1} (1 - [i]/[i+1])^{q-1} ;$$

(4.11) $$\bar{\pi}^{q-1} = -T^q \lim_{N \to \infty} \prod_{\substack{0 \neq a \in A \\ \deg a \leq N}} (a/T^{\deg a})^{q-1} .$$

Formula (4.9) is an easy consequence of (2.8) and is analogous with Euler's formula $(2\pi i)^2 = -12 \sum_{n\in\mathbf{Z}}{}' n^{-2}$. A proof of (4.10) may be found in [9], whereas "Wallis's formula" (4.11) is proved in [7]. Further, an old result of Wade, considerably generalized by Yu [19], asserts the transcendence of $\bar{\pi}$ over K.

5. Modular forms for GL(2,A)

(5.1) Let us now consider the rank two case. A rank two Drinfeld module ϕ is given by

$$\phi_T = T\tau^0 + g\tau + \Delta\tau^2 ,$$

where g and $\Delta \neq 0$ are elements of C. It corresponds to a rank two A-lattice $Y_{\omega_1,\omega_2} = A\omega_1 \oplus A\omega_2$ in C.
Define $j = j(\phi) = g^{q+1}/\Delta$.

Replacing Y by some similar lattice $\lambda\cdot Y$ $(\lambda \in C^*)$ will change (g, Δ) to $(\lambda^{1-q}g, \lambda^{1-q^2}\Delta)$ but will leave j invariant. Thus, considering g, Δ, and j as functions of (ω_1, ω_2), we may restrict to pairs $(\omega_1, \omega_2) = (z,1)$. The discreteness condition on Y translates to the condition "$\{\omega_1, \omega_2\}$ K_∞-linearly independent", i.e. $z = \omega_1/\omega_2$ lies in $\Omega = \mathbb{P}_1(C)\setminus\mathbb{P}_1(K_\infty) = C\setminus K_\infty$. On the "upper half-plane" Ω, the group $GL(2, K_\infty)$ acts by fractional linear transformations $\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = (az+b)/(cz+d)$.

Let $Y_z = Az \oplus A$ the lattice corresponding to $z \in \Omega$. Two elements z, z' define similar lattices (i.e. isomorphic Drinfeld modules) if and only if they are equivalent by $\Gamma = GL(2, A)$. Therefore,

(5.2) $\Gamma\backslash\Omega =$ set of isomorphism classes of rank two Drinfeld modules over C $\xrightarrow{\cong} C$

$z \longmapsto j(z)$.

Next, we introduce the "imaginary part" $|z|_i$ of $z \in C$. Put $|z|_i = \inf |z-x| (x \in K_\infty)$, and for c in the value group $q^{\mathbb{Q}}$ of C, $\Omega_c = \{z \in \Omega \mid |z|_i \geq c\}$. Then $|z|_i = 0$ is equivalent with $z \in K_\infty$, and an easy computation shows

$$(5.3) \qquad |\gamma z|_i = |\det \gamma| \, |cz+d|^{-2} \, |z|_i$$

for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, K_\infty)$. We still have to say a few words about the analytic structure on Ω.

<u>5.4. Proposition:</u>

(i) Ω has the structure of a connected admissible open subspace of the rigid analytic space $\mathbb{P}_1(C)$.

(ii) Ω_c is an open admissible subspace of Ω.

(iii) $GL(2, K_\infty)$ acts as a group of analytic automorpisms on Ω. (In fact, $PGL(2, K_\infty)$ is the full group of automorphisms of Ω.)

For a proof, see [8], IV, sect. 1, [3], or [17], Ch. I.

Intuitively, $|z|_i$ measures the distance "to infinity". We can make this precise.

5.5. Lemma: There exists a real constant $c_0 > 1$ such that for $|z|_i > 1$, we have $|z|_i \leq -\log_q |t(z)| \leq c_0 |z|_i$.

Proof: $t^{-1}(z) = e_L(\bar{\pi} z) = \bar{\pi} e_A(z)$, so let us compute $|e_A(z)|$. This latter being A-invariant, we may assume $|z| = |z|_i > 1$. Let $|z| = q^{d-\varepsilon}$, $0 \leq \varepsilon < 1$, $d \in \mathbb{N}$. Then

$$|e_A(z)| = |z| \prod_{\substack{0 \neq a \in A \\ |a| \leq |z|}} |(1 - z/a)| = |z| \prod_{|a|<|z|} |z/a| = |z|^{q^d} / \prod_{\deg a < d} |a| .$$

Counting the number of a with a given degree and noting $\log_q |\bar{\pi}| = q/(q-1)$ gives $-\log_q |t(z)| = q^d (q/(q-1) - \varepsilon)$. Now always $q^{-\varepsilon} \leq q/(q-1) - \varepsilon \leq c_0 \cdot q^{-\varepsilon}$ for suitable c_0, thus the result.

From (5.5) we derive

5.6. Corollary: For $c > 1$, t induces an isomorphism of $A \setminus \Omega_c$ with some pointed ball $B_r \setminus \{0\}$.

Thus, we may use $t(z)$ as a uniformizing parameter "at infinity", similar to the use of $q(z) = \exp(2\pi i z)$ in the classical case. We are now ready to define modular forms.

5.7. Definition: A function $f\colon \Omega \longrightarrow C$ is called a modular form of weight k and type m (where $k \geq 0$ is an integer and m a class in $\mathbb{Z}/(q-1)$), if the following conditions are satisfied:

(i) if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma = GL(2, A)$, then
$$f(\gamma z) = (\det \gamma)^{-m}(cz + d)^k f(z) ;$$

(ii) f is holomorphic;

(iii) f is holomorphic at infinity.

Let us explain the last condition. By (i), $f(z + b) = f(z)$ for $b \in A$. Now (iii) says: f has an expansion $f(z) = \tilde{f}(t(z))$ with respect to t, where $\tilde{f}(X) = \Sigma\, a_i X^i$ is a power series with a positive radius of convergence. The zero order of f at infinity is defined to be that of $\tilde{f}$. Let M_k^m be the C-vector space of modular forms of weight k, type m. Obviously, $M_k^m \cdot M_{k'}^{m'} \subset M_{k+k'}^{m+m'}$, hence $M = \bigoplus_{k,m} M_k^m$ and $M^0 = \bigoplus_k M_k^0$ are graded C-algebras.

5.8 Remarks:

(i) $M_k^m \neq 0$ implies $k \equiv 2m \bmod (q-1)$. In particular, if q

is odd, k always will be even.

(ii) Each modular form of zero weight is a constant, as results from the geometry of Ω as a "Stein domain" [8].

(iii) The expansion $f(z) = \Sigma\, a_i t^i(z)$ will in general not converge on all of Ω but only for $|t(z)|$ small, i.e. $|z|_i$ large. Nevertheless, Ω being connected in the rigid analytic sense, the coefficients a_i fully determine f. By abuse of language, we often write $f = \Sigma\, a_i t^i$.

(iv) Due to the occurrence of non-trivial types, the definition of order at infinity is different from that in [7].

<u>5.9. Example</u> [10]: Let $E^{(k)}(z) = E^{(k)}(Y_z) = \sum'_{a,b\in A} (az+b)^{-k}$ be the <u>Eisenstein series of weight k</u>. Then (i) (with $m = 0$) and (ii) are easily verified, and (iii) will follow from (6.3). Hence $E^{(k)} \in M_k^0$.

<u>5.10. Example</u>: Expressing g and Δ through Eisenstein series (see (2.10)) shows g (resp. Δ) to lie in M_k^0, where $k = q-1$ (resp. q^2-1). Therefore, (5.2) actually comes from an isomorphism of analytic spaces. The same argument works for the forms $\ell_i(a, z)$, where $a \in A$ and $\phi_a = \Sigma\, \ell_i(a, z)\tau^i$. Thus $\ell_i \in M_K^0$, where $k = q^i - 1$.

<u>5.11. Example</u> [8]: We are obliged to present an example where $m \neq 0$. Let H be the subgroup $\left\{\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}\right\}$ of Γ, and

$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. Observe:

(i) $\alpha(\gamma,z) = (\det \gamma)^{-m}(cz+d)^k$ is a factor of automorphy, i.e. $\alpha(\gamma\delta,z) = \alpha(\gamma,\delta z)\alpha(\delta,z)$;

(ii) $H\backslash\Gamma \xrightarrow{\cong} \{(c,d) \mid c,d \in A,\ (c,d) = 1\}$;
$\gamma \longmapsto (c,d)$

(iii) $\alpha^{-1}(\gamma,z)t^m(\gamma z)$ depends only on the class of γ in $H\backslash\Gamma$.

Thus the <u>Poincaré series</u>

$$P_{k,m}(z) = \sum_{\gamma \in H\backslash\Gamma} \alpha^{-1}(\gamma,z)t^m(\gamma z)$$

is holomorphic of weight k and type m mod $(q-1)$, provided the sum converges and behaves well at infinity. For $k > 0$, this is easily shown using (5.5). Further, $P_{k,m}$ is non-zero if $k > 0$, $k \equiv 2m \bmod (q-1)$, and $m \leq k/(q+1)$.

The next theorems completely describe the structure of M^0 resp. M as C-algebras.

<u>5.12. Theorem</u> [11]: M^0 is the polynomial ring generated by g and Δ .

<u>5.13. Theorem</u>: Let h be the Poincaré series $P_{q+1,1}$. Then M is the polynomial ring $C[g,h]$.

Let us roughly sketch a proof of (5.12) and (5.13) . The stabilizer group Γ_z of $z \in \Omega$ in Γ is of order $q^2 - 1$ if z is Γ-conjugate to an element of $\mathbb{F}_{q^2} \subset C$, and of order $q - 1$ if not. Such a point is called an elliptic point of Γ . For non-zero $f \in M_k^m$, the following formula holds:

$$(5.14) \qquad \sum_{z \in \Gamma \backslash \Omega}^{*} \nu_z(f) + \nu_0(f)/(q+1) + \nu_\infty(f)/(q-1) = k/(q^2-1) ,$$

where on the left, we are summing over the non-elliptic equivalence classes of $z \in \Omega$, and ν_z (resp. ν_0, resp. ν_∞) is the order of f at z (resp. at the elliptic points, resp. at ∞) . This may be proved either by a rigid analytic analogue of contour integration (see [8], p. 302), or by employing the relationship between modular forms and differentials on the modular curve $\Gamma \backslash \Omega \cup \{\infty\} \xrightarrow{\cong}$ projective j-line [7].

We have

(5.15)

(i) $\nu_0(g) = 1$, $\nu_z(g) = 0$, non-elliptic;

(ii) $\nu_\infty(h) = 1$, $\nu_z(h) = 0$, $z \neq \infty$;

(iii) $\nu_\infty(\Delta) = q - 1$, $\nu_z(\Delta) = 0$, $z \neq \infty$.

Statement (i) is clear from (5.14) as g has to vanish at elliptic points. Further, h being of type $m = 1$, $\nu_\infty(h) \equiv 1 \bmod (q-1)$

which shows $\nu_\infty(h) \geq 1$ if $q \neq 2$, so (ii) comes out. (In case $q = 2$, the argument is a little bit more involved, see e.g. (9.1).) (iii) follows from $\nu_z(\Delta) = 0$ $(z \in \Omega)$. Now (5.12) and (5.13) are easy consequences of (5.14) and (5.15).

5.16. Corollary: Δ = constant times h^{q-1}.

It will be one of our objectives to determine that factor. Let us finally note another consequence of (5.14):

5.17. Corollary: Any non-zero $f \in M_k^m$ is determined by its first n coefficients, where $n = [k/(q+1)]+1$. (Here, [ ] = greatest integer function.)

6. t-expansions

Let us first mention the product formula, proved in [5], of the "discriminant function" Δ introduced in the last section.

6.1. Theorem: $\bar{\pi}^{1-q^2}\Delta(z) = -t^{q-1} \prod_{a\in A \text{ monic}} f_a(t)^{(q^2-1)(q-1)}$,

the product converging normally for $|z|_i$ sufficiently large.

Next, we derive the expansions of Eisenstein series with respect to t. For non-zero $a \in A$, let

$$t_a(z) = t(az) = e_L^{-1}(\bar{\pi}az).$$

An easy computation shows

(6.2) $$t_a = t^{|a|}/f_a(t)$$

as a power series in t with coefficients in A . For $k \not\equiv 0 \bmod (q-1)$, $E^{(k)}$ vanishes. Thus let $k \equiv 0 \bmod (q-1)$. Then

$$\begin{aligned} E^{(k)}(z) &= \sum_{a,b\in A}{}' (az+b)^{-k} \\ &= \sum_{b\in A}{}' b^{-k} - \sum_{a \text{ monic}} \sum_{b\in A} (az+b)^{-k} \\ &= \bar{\pi}^{k} E^{(k)}(L) - \bar{\pi}^{k} \sum\sum (\bar{\pi}az + \bar{\pi}b)^{-k} . \end{aligned}$$

By (2.8) and the definition of $L = \bar{\pi}A$, $E^{(k)}(L) \in K$. Further, $\sum_{b\in A} (\bar{\pi}z + \bar{\pi}b)^{-k} = G_k(t(z))$, hence

(6.3) $$\bar{\pi}^{-k} E^{(k)}(z) = E^{(k)}(L) - \sum_{a \text{ monic}} G_k(t_a) .$$

6.4. Examples:

k	Expansion of $\bar{\pi}^{-k} E^{(k)}$	
$q-1$	$[1]^{-1}$	$-\sum t_a^{q-1}$
$j(q-1), j \le q$	$(-1)^{j+1}[1]^{-j}$	$-\sum G_{j(q-1)}(t_a)$
q^2-1	$-L_2^{-1}$	$-\sum (t_a^{q^2-1} - [1]^{-1} t_a^{q^2-q})$
q^3-1	L_3^{-1}	$-\sum (t_a^{q^3-1} - L_1^{-1} t_a^{q^3-q} + L_2^{-1} t_a^{q^3-q^2})$

The sums on the right are over the set of monics in A , and $G_{j(q-1)}$ is the Goss polynomial associated with L . In our case, it is

$$G_{j(q-1)}(X) = \sum_{i \leq j-1} \binom{(j-i)(q-1)-1}{i} [1]^{-i} X^{(j-i)(q-1)} .$$

The constant terms in the table are easily computed using (2.8) .

Note that in both (6.1) and (6.3), for each fixed exponent i of t , only a finite number of a contribute. Therefore, Δ and the $E^{(k)}$ get rational (i.e. in K) t-expansion coefficients if divided by $\bar{\pi}$ to their weight.

From now on, we adopt a different notation for g and Δ , namely

$$g_{new} = \bar{\pi}^{1-q} g_{old} ,$$

$$\Delta_{new} = \bar{\pi}^{1-q^2} \Delta_{old} .$$

Let $M(A)$ (resp. $M^0(A)$) be the A-algebra of modular forms having its coefficients in A . Then by $g = 1 + \ldots$, $\Delta = -t^{q-1} + \ldots$, the next corollary results.

<u>6.5. Corollary</u> [11]: $M^0(A) = A[g,\Delta]$.

<u>6.6 Remark:</u> A coordinate change $T \longrightarrow T + c$ $(c \in \mathbb{F}_q)$ in A does not affect g and Δ . Therefore, the coefficients of g

and Δ (i.e. of all the elements of $M^0(A)$) have to be invariant under $T \longmapsto T + c$. The ring of invariants is easily seen to be the polynomial ring $\mathbb{F}_q[T^q - T]$ in $[1] = T^q - T$.

We next collect some facts on the coefficients of g, Δ, and the <u>product function</u> $U = \prod f_a(t)$ (a monic) which is related with Δ. As only powers of t divisible by $q-1$ occur, put $s = t^{q-1}$. Let B_0 be the set of power series

(*) $f = \Sigma\, m_j s^j$, where $m_j \in A$ and $\deg m_j \leq j$.

B_0 is closed under addition and multiplication, and $f = 1 + \ldots \in B_0$ implies $1/f \in B_0$. Let $B = \{f \in A[[s]] \mid f = af' \text{ for some } a \in A, f' \in B_0\}$ be the A-algebra generated by B_0.

<u>6.7. Proposition:</u>

(i) The power series $U, \Delta/s$, and $(g-1)/[1]$ lie in B_0.

(ii) $M^0(A) \hookrightarrow B$.

<u>Proof:</u>

(i) By (4.5), the cyclotomic polynomials f_a satisfy (*), and this property is inherited by U and Δ/s. Further, $(g-1)/[1] = \Sigma\, t_a^{q-1} = \Sigma\, s^{|a|}/f_a^{q-1} \in B_0$ for $1/f_a \in B_0$.

(ii) By (i), g and $\Delta \in B$. Now apply (6.5).

Define for $k \geq 0$

(6.8) $$g_k = (-1)^{k+1}\,\bar{\pi}^{1-q^k}\,L_k E^{(q^k-1)}$$

either as a modular form or as a formal series in t.

6.9. Proposition:

(i) $g_k = 1 + \dots$;

(ii) g_k has coefficients in A ;

(iii) $g_0 = 1$, $g_1 = g$,

$$g_k = -[k-1]g_{k-2}\Delta^{q^{k-2}} + g_{k-1}g^{q^{k-1}} \qquad (k \geq 2).$$

Proof:

(i) comes from $E^{(q^k-1)}(L) = (-1)^{k+1}/L_k$ which is derived from (2.9) and (4.3). Further, by (3.10), L_k is a denominator for the coefficients of G_i, $i = q^k - 1$, thus (ii). Finally, (iii) is the translation of (2.10) applied to $a = T$ and $\phi_T = T\tau^0 + \bar{\pi}^{q-1} g\tau + \bar{\pi}^{q^2-1}\Delta\tau^2$.

6.10. Proposition (compare [11]): Let $\Sigma a_i s^i$ be the expansion of one of the forms Δ, g_k with respect to $s = t^{q-1}$.

Then $a_i \neq 0$ implies $i = 0$ or $1 \bmod q$.

Proof: Let (#) denote the stated congruence property. Now:

(i) f_a , considered as a power series in s , satisfies (#). Let $j = q^k - 1$, $k \geq 1$.

(ii) t^j satisfies (#).

(iii) Let $a \in A$ be non-constant. Then $t_a^j = (s^{|a|j/(q-1)} f_a^{-q^k}) f_a$ satisfies (#) since the first factor is a q-th power.

(iv) $G_j(t_a)$ satisfies (#) by (ii), (iii) and (3.10).

Thus (#) results for g_k and, in view of (6.9 iii), for Δ .

Finally, we investigate congruences modulo ideals of A . For power series f and $f' \in A[[t]]$ and an ideal $\mathfrak{a}$ of A , $f \equiv f' \bmod \mathfrak{a}$ means the congruence mod $\mathfrak{a}$ of all the coefficients.

6.11. Proposition: Let $\mathfrak{p}$ be a prime ideal of A of degree d . Then $g_{k+d}(t) \equiv g_k(t^{q^d}) \bmod \mathfrak{p}$.

6.12. Corollary: $g_d \equiv 1 \bmod [d]$.

Proof (of (6.11)): The coefficients of the $(q^d - 1)$ - th Goss polynomial are $\pm L_i^{-1}$ where $i < d$. Thus by (6.3) and (6.8), $g_d \equiv 1 \bmod L_d/L_{d-1}$, i.e. mod [d] . In particular,

$g_d \equiv g_0 \equiv 1 \bmod p$. Further, mod p we have $T^{q^d} \equiv T$, so $[k+d] \equiv [k]$. By induction, using (6.9 iii), $g_{k+d} \equiv g_k^{q^d}$. Modulo p , the latter equals $g_k(t^{q^d})$.

7. Hecke operators

For $f \in M_k^m$ and a prime ideal $p = (p)$, where p is monic of degree d , let

$$(7.1) \qquad T_p f(z) = p^k f(pz) + \sum_{\substack{b \in A \\ \deg b < d}} f((z+b)/p) \; .$$

T_p is called the p-th Hecke operator. As expected, $T_p f \in M_k^m$, and is cuspidal (i.e. vanishes at infinity) if f is. (We could define Hecke operators for all the ideals a of A , as one usually does. But unlike the classical case, $T_{ab} = T_a T_b$ [7], so we may restrict to prime ideals.)

<u>7.2. Proposition:</u> $T_p E^{(k)} = p^k E^{(k)}$.

This follows by direct computation, see [10] or [7]. Next, we consider the effect of T_p on t-expansions. Let $G_{k,p}$ be the k-th Goss polynomial with respect to the $\mathbb{F}_q$-lattice $\Lambda_p = \ker \rho_p$ of dimension d .

For $i \geq 1$, we compute

$$\sum_{\deg b<d} t^{i}(z+b) = \sum (e(\bar{\pi}z/p) + e(\bar{\pi}b/p))^{-i}$$

$$= \sum_{\lambda\in\Lambda_p} (e(\bar{\pi}w)+\lambda)^{-i}, \quad \text{where} \quad z = pw$$

$$= G_{i,p}(\sum (e(\bar{\pi}w)+\lambda)^{-1})$$

$$= G_{i,p}(p/\rho_p(e(\bar{\pi}w)))$$

$$= G_{i,p}(p/e(\bar{\pi}z))$$

$$= G_{i,p}(pt) .$$

For $i = 0$, $\sum t^{0}(\ldots) = 0 = G_{0,p}(pt)$. Hence

(7.3) $$T_p(\sum a_i t^i) = p^k \sum a_i t_p^i + \sum a_i G_{i,p}(pt) ,$$

$$t_p(z) = t(pz) = t^{|p|}/f_p(t) .$$

Note that by (3.9), for j fixed, only a finite number of terms of the right hand side contribute to the coefficient of t^j .

<u>7.4. Example:</u> Let p be of degree one. Then $t_p = t^q/(1+pt^{q-1})$ and $G_{i,p}$ is given by (3.7). If $f = \sum a_i t^i$ and $T_p f = \sum a_i' t^i$ are of weight k , we derive

$$a_i' = p^k \sum_{\substack{u,v\geq 0\\ uq+v(q-1)=i}} \binom{-u}{v} p^v a_u + \sum_{0\leq v<i} \binom{i-1}{v} p^{i-v} a_{i+v(q-1)} .$$

We refrain from writing down the general formula that follows from (3.8) and (7.3).

<u>7.5. Corollary</u> (first obtained by D. Goss [11]): $T_p\Delta = p^{q-1}\Delta$.

<u>Proof:</u> As the space of cusp forms of weight $k = q^2 - 1$, type zero is one-dimensional, we just have to determine the coefficient a'_{q-1} of t^{q-1} in $T_p\Delta$. Obviously, the first sum in (7.3) does not contribute, so it is enough to see $a_i G_{i,p}(X)$ has no X^{q-1} - term if $i \neq q-1$. Let the i - th coefficient a_i of Δ be non-zero, so $i \equiv 0 \bmod (q-1)$ and $i \equiv 0$ or $-1 \bmod q$, and suppose $i > q-1$. If $i \equiv 0 \bmod q$ then $G_{i,p}$ has no X^{q-1} - term by (3.4 vi), whereas for $i+1 = rq$, we use $X^2 G'_{i,p} = -G_{rq,p} = -(G_{r,p})^q$. Now $r > 1$, so $G_{r,p}$ has no X - term which implies G_i has no X^{q-1} - term.

Note Δ has the same eigenvalues as g which is completely different from the number theoretic case. I do not know whether "Hecke eigenvalues plus weight" suffices to determine an eigenform.

<u>7.6. Corollary:</u> $T_p h = p \cdot h$.

<u>Proof:</u> The same reasoning as in (7.5), noting $G_i(X) = o(X^2)$ for $i \geq 2$.

<u>7.7. Problem:</u> Compute the action of Hecke on powers of Δ !

8. Derivations

Let dL be the logarithmic derivative operator

$$dL : f(z) \longmapsto \bar{\pi}^{-1} \frac{d}{dz} f(z)/f(z) .$$

Obviously, $dL(f_1 \cdot f_2) = dL(f_1) + dL(f_2)$. From
$\frac{d}{dz} t(z) = \frac{d}{dz} e^{-1}(\bar{\pi}z) = -\bar{\pi}e^{-2}(\bar{\pi}z) = -\bar{\pi}t^2(z)$ and
$\frac{d}{dX} f_a(X) = -aX^{|a|-2}$ ($a \in A$ non-constant), we have

$$(8.1) \qquad dL(f_a)(t) = at_a \qquad \text{(a non-constant)}$$

$$= 0 \qquad \text{(a constant)}$$

and $$dL(t) = -t .$$

Let $U(z) = \prod_{a \text{ monic}} f_a(t(z))$ be the product function. Using (6.1), we have for $E = dL(\Delta)$

$$(8.2) \qquad E = (q-1)dL(t) + (q^2-1)(q-1)dL(U)$$

$$= t + \sum_{1 \neq a \text{ monic}} at_a$$

$$= \sum_{a \text{ monic}} at_a .$$

E is a conditionally convergent two-dimensional lattice sum

$$E(z) = \bar{\pi}^{-1} \sum_{a \text{ monic}} \left(\sum_{b \in A} a/(az+b) \right)$$

and should be considered as an analogue of the "false Eisenstein series of weight 2" in the classical theory. Let now $f \in M_k^m$. Applying $(\det \gamma)^{-1}(cz+d)^2 d/dz$ to both sides of the equation $f(\gamma z) = (\det \gamma)^{-m}(cz+d)^k f(z)$, where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, we obtain

$$(8.3) \quad f'(\gamma z) = (\det \gamma)^{-(m+1)}(cz+d)^{k+2} f'(z) + kc(\det \gamma)^{-(m+1)}(cz+d)^{k+1} f(z) .$$

Putting $f = \Delta$ and dividing (8.3) by $\bar{\pi}\Delta(\gamma z)$, the functional equation

$$(8.4) \quad E(\gamma z) = (\det \gamma)^{-1}(cz+d)^2 E(z) - c\bar{\pi}^{-1}(\det \gamma)^{-1}(cz+d)$$

results.

(8.5) We define $\Theta = \bar{\pi}^{-1} d/dz$ and $\partial_k = \Theta + kE$ as operators on M_k^m. Then (8.3) and (8.4) imply $\partial_k(f) \in M_{k+2}^{m+1}$. Direct computation shows: If f_i is of weight $k_i (i = 1,2)$ and $k = k_1 + k_2$, then

$$\partial_k(f_1 \cdot f_2) = \partial_{k_1}(f_1) \cdot f_2 + f_1 \cdot \partial_{k_2}(f_2) ,$$

i.e. ∂ may be considered as a differential operator of weight two on the graded algebra M. We further observe: $\Theta = -t^2 d/dt$ and ∂ have coefficients in A if expressed with respect to the t - expansion. Let us now collect some results on the values of ∂ . From (6.10) we see $\Theta^2\Delta = 0$,thus

(8.6) $$\Theta E = - E^2 .$$

8.7. Corollary: The power series $\sum_{a \neq b \text{ monic}} abt_a t_b$ in t vanishes identically.

Proof: It is the expansion of $E^2 - \Theta E$.

From $g = 1 - [1]t^{q-1} + o(t^{q^2-1})$ and $E = t + o(t^{q^2-2q+2})$,we derive $\partial g = - t + o(t^{q^2-2q+2}) \neq 0$, so ∂g has to be proportional with h . Further $\partial^2 g = o(t^{q^2-2q+1})$ vanishes identically by (5.17).

8.8. Proposition: We have $\partial\Delta = 0$ and $\partial^2 f = 0$ for each of the functions $f(z) = g_k(z)$, $\ell_k(a,z)$, or $\alpha_k(z) = \alpha_k(Az + A)$ (see section 2).

Proof: The assertion on $\partial\Delta$ is immediate from the definition. Those concerning the functions f are proved using the relations (2.6) - (2.10), the fact ∂ is a differential operator, and $\partial^2 g = 0 = \partial\Delta$.

8.9. Corollary: Let $F(X,Z) \in C[X,Z]$ be such that $F(g,h) = f$ where f is as in (8.8). Then $\left(\frac{\partial}{\partial X}\right)^2 F(X,Z) = 0$.

Proof: $0 = \partial^2 f = \text{const} \times \left(\frac{\partial}{\partial X}\right)^2 F(g,h) \cdot h^2$ since $\partial g = \text{const} \times h$ and $\partial h = 0$.

9. Comparing ∂g and h

In this section, we prove

9.1. Theorem: $\partial g = h$.

We thus have at least three different characterizations of that form, namely

(a) $h = P_{q+1,1}$ the Poincaré series of weight $q+1$, type 1 (which we have used as a definition of h);

(b) $h = \partial g$;

(c) $h^{q-1} = -\Delta$.

9.2. Corollary: We have the identity of power series in t

$$-\sum_{a \text{ monic}} a t_a + [1] \sum_{a \neq b \text{ monic}} a t_a t_b^{q-1} = -t \prod_{a \text{ monic}} f_a^{q^2-1}(t) .$$

Proof: $g = 1 - [1] \sum_{a \text{ monic}} t_a^{q-1}$ and $\Theta(t_a) = -a t_a^2$, so an easy computation gives the result.

(9.3) Let us shortly mention still another interpretation. For u running through a set of representatives of $(T^{-1}A/A)^2 = V$, let $$E_u(z) = \sum_{(a,b) \equiv u \bmod A^2} (az+b)^{-1} ,$$

which is a modular form of weight one for the congruence subgroup $\Gamma(T) = \{\gamma \in \Gamma \mid \gamma \equiv 1 \bmod T\}$. Choose a non-degenerate alternating form $<\ ,\ >$ on the two-dimensional $\mathbb{F}_q$-vector space V , and put

$$f = \sum_{\substack{u,v \in V \\ <u,v>=1}} E_u^q E_v .$$

It is easy to verify f to be of weight $q+1$, type 1, so $f = \text{const} \times h$. Using the expansions for E_u given in [6], one may actually compute the constant which happens to be non-zero. This gives a quite general "algebraic" method to construct modular forms of weight $q^d + 1$ and type 1.

Let us now turn to the proof of (9.1). Consider the sum defining $h = P_{q+1,1}$

(9.4) $$h(z) = \sum_{\substack{c,d \in A \\ (c,d)=1}} t(\gamma_{c,d}(z)) / (cz+d)^{q+1}$$

where $\gamma_{c,d} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,A)$. We are going to isolate the contributions of the different $c \in A$ to the linear coefficient of h . Let us define for c fixed

$$h_c = \sum_{\substack{d \in A \\ (c,d)=1}} \cdots \quad \text{and, for } c,d \text{ fixed} \quad h_{c,d} = \sum_{\substack{d' \in A \\ d' \equiv d \bmod c}} \cdots .$$

Then for $c \neq 0$, $h_c = \sum_{\substack{d \bmod c \\ (d,c)=1}} h_{c,d}$ and $h = \sum_{c \in A} h_c$.

In view of the matrix equation $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a, & b+ar \\ c, & d+cr \end{pmatrix}$,

$h_{c,d}$ is the sum over the double class of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in

$\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \backslash \Gamma / \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$, so in particular is A-invariant and has a t-expansion. Now for the proof of (9.1) it is enough to show the following three facts:

(9.5) $\quad h_0 = -t + o(t^2)$;

(9.6) $\quad h_c = o(t^2)$ if $\deg c = 0$;

(9.7) $\quad h_{c,d} = o(t^2)$ if $\deg c > 0$.

The first one is clear: $c = 0$ implies $d \in \mathbb{F}_q^*$, so

$$h_0 = \sum_{d \in \mathbb{F}_q^*} t(d^{-2}z) / d^{q+1} = \sum_{d \in \mathbb{F}^*} t(z)/d^{q-1} = -t(z) .$$

<u>Proof</u> of (9.6): Without loss of generality, $c = 1$ and $\gamma_{c,d} = \begin{pmatrix} 0 & -1 \\ 1 & d \end{pmatrix}$. Then

$$-h_1 = \sum_{d \in A} t(1/(z+d))/(z+d)^{q+1} = \bar{\pi}^{-1} \sum_{d} (z+d)^{-q} \frac{\bar{\pi}/(z+d)}{e(\bar{\pi}(z+d))} .$$

For $|z|_i$ sufficiently large, $w = \bar{\pi}/(z+d)$ satisfies $|w| \leq |\bar{\pi}|/|z|_i < 1$, and for such arguments w , the series

$w/e(w) = \Sigma\, \gamma_k w^k$ converges uniformly. Thus

$$-h_1 = \bar{\pi}^{-1} \sum_d (z+d)^{-q} \sum_{k\geq 0} \gamma_k (\bar{\pi}/(z+d))^k$$

$$= \bar{\pi}^{-1} \sum_{k\geq 0} \gamma_k \bar{\pi}^{q+2k} \sum_d (\bar{\pi}(z+d))^{-k-q}$$

$$= \bar{\pi}^{q-1} \sum_{k\geq 0} \gamma_k \bar{\pi}^{2k} G_{k+q}(t)$$

which has no linear term in t.

The proof of (9.7) is slightly more complicated. For (c,d) given, choose $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,A)$. Note: $\lambda = e(\bar{\pi}a/c)$ and $\mu = e(\bar{\pi}d/c)$ are non-zero c-division points of the Carlitz module ρ. The expression of $t(z+a/c)$ with respect to t is given by

(9.8) $$t(z+a/c) = 1/e(\bar{\pi}(z+a/c)) = 1/(e(\bar{\pi}z)+\lambda)$$

$$= t/(1+\lambda t) = t - \lambda t^2 + \ldots ,$$

similarly for a replaced by d. The geometric series converges for $|t| < |\lambda|$ which is satisfied for $|z|_i$ large enough, see (5.5). Let now $\delta = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}$. An easy computation yields $e(\bar{\pi}\gamma\delta z) = \lambda - e(w)$, where $w = w(z,r) = \bar{\pi}/c(cz+d+cr)$. The second term is small for $|z|_i$ large:

$$|e(w)| = |\bar{\pi}/c(cz+d+cr)| \leq |\bar{\pi}|\,|c|^{-2}|z|_i^{-1}$$

uniformly in z and r, as long as $|z|_i$ is large enough. In particular,

$$t(\gamma\delta z) = (\lambda - e(w))^{-1} = \sum_{k\geq 0} \lambda^{-k-1} e^k(w) \quad , \quad \text{and}$$

$$h_{c,d} = \sum_{r\in A} (cz + d + cr)^{-1-q} \sum_{k\geq 0} \lambda^{-k-1} e^k(w) \; .$$

As above, we may interchange the order of summation. It then suffices to see

$$h_{c,d,k} = \sum_{r\in A} e^k(w(z,r))/(cz + d + cr)^{q+1}$$

has no t-terms of order ≤ 1. Let $e^k(w) = \sum e_{k,i} w^i$. Then

$$h_{c,d,k} = \sum_r (cz + d + cr)^{-1-q} \sum_i e_{k,i} (\bar{\pi}/c(cz + d + cr))^i$$

$$= \sum_i (\bar{\pi}/c)^{q+1+2i} e_{k,i} \sum_r (\bar{\pi}(z + d/c + r))^{-q-1-i}$$

(again the change of summation order is justified, the $e_{k,i}$ decreasing very rapidly)

$$= \sum_i (\bar{\pi}/c)^{q+1+2i} e_{k,i} G_{q+1+i}(t(z + d/c)) \; .$$

Now each of the polynomials $G_{q+1+i}(X)$ is divisible at least by X^2. Hence by (9.8), $h_{c,d,k}$ has no term of order zero or one in t, and (9.7) is established.

10. Some special forms

Here, we are computing the first coefficients of $f \in \{E, g, h, g_2, \Delta, U\}$ up to a certain bound which will depend on f. Let us first treat the product function $U(t) = \prod_{a \text{ monic}} f_a(t)$. From U, we will easily deduce the expansions of E, h, and Δ.

As in section 6, we put $s = t^{q-1}$. In what follows, a will always denote a monic element of A of degree d. As is obvious from the definition of f_a, the i-th coefficient of U (with respect to s) may only contributed by those a satisfying $q^{d-1} \leq i$. This estimate may be sharpened. Let $U_d = \prod_{a \text{ monic, } \deg a = d} f_a$. Then $U_{d+1} = \prod_{a \text{ monic, } \deg a = d} f_a^*$, where we have put ad hoc $f_a^* = \prod_{c \in \mathbb{F}_q} f_{aT+c}$. Expanding f_a^* by means of (4.7), we find

$$
\begin{aligned}
(10.1) \quad f_a^* = {} & 1 - s^{q^{d+1}-1} + (\ell_{d-1}^{q^2} + T^q) s^{q^{d+1}} - (\ell_{d-1}^q + T) s^{q^{d+1}+q^d-1} \\
& + (\ell_{d-2}^{q^2} + T^q \ell_{d-1}^q) s^{q^{d+1}+q^d} - (\ell_{d-2}^q + T) s^{q^{d+1}+q^d+q^{d-1}-1} \\
& + T^q \ell_{d-2}^q s^{q^{d+1}+q^d+q^{d-1}} - T \ell_{d-2} s^{q^{d+1}+q^{d-1}+q^{d-2}-1} \\
& + \text{terms involving } \ell_{d-3} \text{ which are of order} \geq q^{d+1}+q^d+q^{d-1} \text{ in } s,
\end{aligned}
$$

where the $\ell_i = \ell_i(a)$ are defined by (4.4).

Suppose for the moment $d \geq 3$. If we first take the product over those a of the form $a = T^d + a_{d-1}T^{d-1} + \ldots$ where a_{d-1} and $a_{d-2} \in \mathbb{F}_q$ are fixed (so ℓ_{d-1} and ℓ_{d-2} are fixed too), we see $\prod_{a \text{ as above}} f_a^* = 1 + o(s^k)$, thus $U_{d+1} = 1 + o(s^k)$ with $k = q^{d+1} + q^d + q^{d-1}$. For $d = 2$, (10.1) becomes an exact formula. Multiplying the f_a^* in a convenient order shows (by a lengthy computation which we omit) $U_3 = 1 + o(s^{q^4})$. Thus, $U = U_1 \cdot U_2 + o(s^{q^4})$. As above, we omit the details of computing U_1 and U_2 (which is straightforward from (10.1)) and give just the result.

<u>10.2. Theorem:</u> The first q^4 coefficients u_i of U with respect to $s = t^{q-1}$ are given by the following table where an index missing indicates the corresponding coefficient to be zero.

i	u_i	i	u_i
0	1	q^3+q	$[1]([2]^q - [2])$
$q-1$	-1	q^3+q^2-q-1	-1
q	$[1]$	q^3+q^2-1	$[2] + [1]^q$
q^3-q^2	-1	q^3+q^2	$[1][2]$
q^3-1	2	q^3+q^2+q-1	$[2][1]^q$
q^3	$[2]+[1]$	q^3+q^2+q	$[2][1]^{q+1}$
q^3+q-1	$-([2]^q - [2])$	q^4-1	0

More shortly, we have

$$U = U_1 - s^{q^3-q^2} + 2s^{q^3-1} + o(s^{q^3})$$

where $U_1 = 1 - s^{q-1} + [1]s^q = \prod_{a \text{ monic, deg } a=1} f_a$.

10.3. Corollary :

$$\Delta = - s\, U_1^{1-q} + s^{q^3-q^2+q} - [1]s^{q^3-q^2+q+1} - s^{q^3} + o(s^{q^3+1}) \, .$$

Expanding out the power series U_1^{1-q} , we get the table (δ_i = coefficient of s^i in Δ):

i	δ_i	i	δ_i
1	-1	q^2+q	$-[1]^q$
q	1	q^2+q+1	$[1]^{q+1}$
$q+1$	$-[1]$	$2q^2-2q+1$	-1
q^2-q+1	-1	$2q^2-q$	1
q^2	1	$2q^2-q+1$	$2[1]^q-[1]$
q^2+1	$[1]^q-[1]$	$2q^2$	$-2[1]^q$

Proof: $\Delta = - s\, U^{q^3} \cdot U/U^q \cdot U^{q^2}$. Up to terms of order q^3 in s , $U^{q^3} \equiv 1$, $U^{q^2} \equiv 1 - s^{q^3-q^2}$, and $U^q \equiv U_1^q$. Putting together these congruences gives the result.

10.4. Corollary: $h/t = - U_1^{-1} + s^{q^3-q^2} U_1^{-1} - s^{q^3-q^2} U_1^{-2} + 2s^{q^3-1} + o(s^{q^3})$. In particular, $h/t = - U_1^{-1} + o(s^{q^3-q^2})$.

This follows the same way as (10.3).

10.5. Corollary:

$$E/t = 1 + s^{q-1}U_1^{-1} + s^{q^3-q^2+q-1}U_1^{-2} - 2s^{q^3-1} + o(s^{q^3}) .$$

Proof: $E = \Theta\Delta/\Delta = \Theta s/s + \Theta U/U$. But $\Theta = -t^2 d/dt$, so $\Theta s = t^q = ts$, $(\Theta U)/t = s^{q-1} - 2s^{q^3-1} + o(s^{q^3})$, and the assertion comes from computing modulo terms of order $\geq q^3$ in s .

Next, we investigate the form $g = 1 - [1] \Sigma t_a^{q-1}$. As usual, let $d = \deg a$, a monic, $\rho_a = \Sigma \ell_i \tau^i$. Then

$t_a = t^{q^d}/(1 + \ell_{d-1}s^{q^{d-1}} + \ldots)$, hence $t_a^{q-1} = s^{q^d} + o(s^{q^d+q^{d-1}})$,

and the contribution of all the a of degree d cancels up to $o(s^{q^d+q^{d-1}})$. We are going to sharpen this bound. Let

$C_d = \sum_{a \text{ monic, } \deg a=d} t_a^{q-1}$ as a power series in s . To compute C_d , we use

(10.6)

(i) $$\sum_{c \in \mathbb{F}_q} (X + cY)^{-1} = - Y^{q-1}(X^q - XY^{q-1})^{-1}$$ and

(ii) $$\sum_{c \in \mathbb{F}_q} (X + cY)^{1-q} = \left(\Sigma (X + cY)^{-1}\right)^{q-1} ,$$

where (i) comes from the logarithmic derivative of

$X^q - X = \prod (X-c)$ and (ii) is a special case of (3.4). Of course, $C_0 = t^{q-1} = s$. Next, for $a = T + c$, $f_a(t) = 1 + (T+c)t^{q-1}$,

thus $C_1 = s^q \sum_{c \in \mathbb{F}_q} (1 + (T+c)s)^{1-q} \underset{(ii)}{=} s^q(\Sigma(1 + Ts + cs)^{-1})^{q-1}$

$$\underset{(i)}{=} s^q(-s^{q-1}/(1 + T^q s^q - (1+Ts)s^{q-1}))^{q-1}$$

$$= s^{q^2-q+1} U_1^{1-q} \quad , \quad U_1 \text{ as in } (10.2) .$$

Let now $d \geq 2$ and $a = T^d + \sum_{i<d} a_i T^i$. Then

$$f_a = \sum_{0 \leq i \leq d} a_i w_i \quad , \quad w_i = s^{(q^d - q^i)/(q-1)} f_{T^i} \quad .$$

Note the following facts:

(10.7)

(i) $i > j \Rightarrow \text{ord}(w_i) < \text{ord}(w_j)$, where ord denotes the order of a power series in s;

(ii) $f_a = X_0 + a_0 Y_0$, where $X_0 = \sum_{i>0} a_i w_i$ depends only on a_i with $i > 0$, and $Y_0 = w_0$ is independent of a;

(iii) $X_0 = 1 +$ higher terms in s, $Y_0 = s^k +$ higher terms.

Let us compute

$$t^{-q^d} \sum_{a \text{ monic, deg } a=d} t_a = \sum_{a_{d-1}} \cdots \sum_{a_0} 1/f_a \; .$$

First consider the innermost sum

$$\sum_{a_0} 1/f_a = \sum 1/(X_0 + a_0Y_0) = -Y_0^{q-1}/(X_0^q - X_0Y_0^{q-1}) \ .$$

Next put for $1 \leq i < d$

$$X_{i-1}^q - X_{i-1}Y_{i-1}^{q-1} = X_i + a_iY_i \ ,$$

X_i depending at most on $a_{i+1} \dots a_{d-1}$, Y_i independent of a , and X_i , Y_i satisfying (10.7 iii). Of course, X_i and Y_i are uniquely determined. Let us have a closer look of this last equation. The left hand side can be written in the form $\sum_{j \geq i} a_j w_{i,j}$ with polynomials $w_{i,j}$ in s that do not depend on a and satisfy (10.7 i) with respect to the second index. For the $w_{i,j}$, we have (putting $w_{0,j} = w_j$)

$$w_{i,j} = w_{i-1,j}^q - w_{i-1,j}w_{i-1,i-1}^{q-1} \ .$$

Hence, $\text{ord}\ (w_{i,j}) = q\cdot\text{ord}\ (w_{i-1,j})$. In particular, $\text{ord}\ (Y_i) = \text{ord}\ (w_{i,i}) = q^i\ \text{ord}\ (w_{0,i}) = q^i(q^d - q^i)/(q-1)$. By repeated application of (10.6 i), we get

$$(10.8) \quad \sum_{a_i} \dots \sum_{a_0} 1/f_a = (-1)^{i+1}(Y_0 \dots Y_i)^{q-1}/(X_i^q - X_iY_i^{q-1}) \ ,$$

and finally

$$(10.9) \qquad \sum_{a \text{ monic, deg } a=d} 1/f_a = (-1)^d s^k + \text{ higher terms, where}$$

$$k = \sum_{0 \le i < d} q^i (q^d - q^i)/(q-1) = (q^{d+1}-1)(q^d-1)/(q^2-1) .$$

Taken together,

$$(10.10) \quad C_d = \sum_{a \text{ monic, deg } a=d} t_a^{q-1} = s^{q^d} (\sum 1/f_a)^{q-1} = s^k + \text{higher terms,}$$

where now $k = (q^{2d+1}+1)/(q+1)$.

<u>10.11. Corollary:</u> $g = 1 - [1](s + s^{q^2-q+1} U_1^{1-q}) + o(s^{(q^5+1)/(q+1)})$.

It is easy to obtain similar results for the form g_2 , say. From (6.4), $g_2 = 1 - [2] \sum t_a^{q^2-q} + L_2 \sum t_a^{q^2-1}$. The term $\sum t_a^{q^2-q} = (\sum t_a^{q-1})^q$ is evaluated as above, whereas for $\sum t_a^{q^2-1}$, we use Goss polynomials to detect the contribution of a fixed degree d .

$$\sum_{a \text{ monic,deg } a=d} t_a^{q^2-1} = t^{q^d(q^2-1)} \sum f_a^{1-q^2} = s^{q^d(q+1)} G_{q^2-1,\Lambda}(\sum f_a^{-1}) ,$$

where Λ is a certain d-dimensional $\mathbb{F}_q$-module. We will make this explit for $d = 1$. In that case, $\sum_a f_a^{-1} = \sum_{c \in \mathbb{F}_q} (1 + Ts + cs)^{-1}$, i.e. the corresponding lattice is $\mathbb{F}_q \cdot s$. Using (3.11), we find

$\sum\limits_{\substack{a \text{ monic, } \deg a=1}} f_a^{1-q^2} = G(\sum f_a^{-1})$ with the polynomial

$G(X) = X^{q^2-1} + s^{1-q}X^{q^2-q}$, which gives the value

$s^{(q-1)(q^2-1)}U_1^{1-q} + s^{q^3-2q^2+1}U_1^{q-q^2}$. A similar argument which will not be given in detail shows the contribution of those a of degree ≥ 2 to be $o(s^k)$, $k = q(q^5+1)/(q+1)$.

Summing up:

<u>10.12. Corollary:</u> $g_2 = 1 - [2]s^q + L_2 s^{q+1} - [2]s^{q^3-q^2+q}U_1^{q-q^2}$ $+ L_2 s^{q^3-q^2+q+1}U_1^{q-q^2} + L_2 s^{q^3+1}U_1^{1-q^2} + o(s^k)$, where $k = q(q^5+1)/(q+1)$.

(10.13) Hecke operators yield non-trivial relations between these coefficients. For checking on the s-expansion, let us note the translation of (7.4) into the s-notation: If $f = \sum a_i s^i \in M_k^0$, $\mathfrak{p} = (p)$ a prime of degree one and $T_\mathfrak{p} f = \sum a_i' s^i$ then

$$a_i' = p^{k+i} \sum_{u \leq i/q} \binom{-(q-1)u}{i-uq} p^{-uq} a_u + p^{(q-1)i} \sum_{v<(q-1)i} \binom{(q-1)i-1}{v} p^{-v} a_{i+v} .$$

<u>11. Hasse invariants</u>

In the whole section, $\mathfrak{p} = (p)$, p monic , will be a prime of degree d . The reduction homomorphism $A \longrightarrow \mathbb{F}_\mathfrak{p} = A/\mathfrak{p}$ and everything derived from it will be denoted by a tilde $a \longmapsto \tilde{a}$. We consider rank two Drinfeld modules ϕ defined over a field extension $\mathbb{F}$ of $\mathbb{F}_p$. Like Drinfeld modules over C , ϕ is defined by

$$\phi_T = \tilde{T}\tau^0 + g\tau + \Delta\tau^2$$

where now g and $\Delta \neq 0$ are in $\mathbb{F}$. If $\mathbb{F}$ is algebraically closed, $j(\phi) = g^{q+1}/\Delta$ characterizes ϕ up to isomorphism. It is a general fact that ϕ_p is of the form

(11.1) $$\phi_p = \ell_d\tau^d + \dots \ell_{2d}\tau^{2d} ,$$

i.e. the coefficients $\ell_0 \dots \ell_{d-1}$ of ϕ_p have to vanish. Thus the group scheme $\ker \phi_p$ is not reduced, and the abstract group $(\ker \phi_p)(\bar{\mathbb{F}})$ over the algebraic closure $\bar{\mathbb{F}}$ of $\mathbb{F}$ is at most one-dimensional as an $\mathbb{F}_p$-module. We call $H(\phi) = \ell_d$ the Hasse invariant of ϕ . Similar to elliptic curves in positive characteristic, we have the equivalence of the following assertions:

(11.2)

(i) $H(\phi) = 0$;

(ii) $(\ker \phi_p)(\bar{\mathbb{F}}_p) = 0$;

(iii) the endomorphism ring of ϕ is non-commutative.

The Drinfeld module ϕ (resp. its j-invariant $j(\phi)$) is called supersingular if these conditions are satisfied. If ϕ is supersingular, $j(\phi)$ is of degree at most two over $\mathbb{F}_p$. The number of supersingular j is given by $q(q^{d-1}-1)/(q^2-1)$ if d is odd, and $(q^d-1)/(q^2-1)$ if d is even. For all these facts, see [4]. H may be considered as an algebraic modular form of weight q^d-1 [10], and we will determine its t-expansion.

(11.3) Let $A((t))$ resp. $K((t))$ be the ring of formal Laurent series in t with coefficients in A resp. K. Consider the rank two Drinfeld module TD over $K((t))$ defined by

$$TD_T = T\tau^0 + g(t)\tau + \Delta(t)\tau^2 ,$$

where for the coefficients $g(t)$ and $\Delta(t)$, we insert the t-expansions of g and Δ given in section 6. TD is called the <u>Tate-Drinfeld module</u>. Having its coefficients in $A((t))$, TD may be reduced mod p, thereby defining the rank two module $\widetilde{TD}$ over $F_p((t))$. By definition, $H(\widetilde{TD})$ will be the t-expansion of H.

<u>11.4. Lemma:</u> Mod p, we have $(-1)^d p/L_d \equiv 1$.

<u>Proof:</u> Clearly, p divides L_d exactly once, so the assertion makes sense. Writing $(-1)^d p/L_d = (-1)^d p/D_d \cdot (D_d/L_d)$, we show

a) $p/D_d \equiv -1$ and b) $D_d/L_d \equiv (-1)^{d-1}$.

Now $D_d/p = \prod_{\substack{p \neq x \text{ monic} \\ \deg x = d}} x \equiv \prod (x-p) \equiv \prod_{0 \neq x \in \mathbb{F}_p} x = -1$, thus a).

For b), note $D_d = (T^{q^d} - T)(T^{q^d} - T^{q^{d-1}}) \ldots (T^{q^d} - T)$

and $L_d = (T^{q^d} - T)(T^{q^{d-1}} - T) \ldots (T^q - T)$.

In D_d/L_d , the first factors cancel, and, working mod p , we we may replace T^{q^d} by T , thus $D_d/L_d \equiv (-1)^{d-1}$.

<u>11.5. Theorem:</u> $H(\tilde{TD}) \equiv 1 \bmod p$, i.e. the t-expansion of H is constant with value 1.

<u>Proof:</u> We have to show the corresponding congruence for the coefficients of $TD_p = \sum_{0 \leq i \leq 2d} \ell_i \tau^i$, $\ell_i \in A[[t]]$. The ℓ_i and the g_i are related by

$$(-1)^{k+1} p\, g_k/L_k = \sum_{i+j=k} (-1)^{i+1} (g_i/L_i)\, \ell_j^{q^i}$$

which follows from (2.10) and the definition of g_i . For $k = d$,

$$\ell_d + (-1)^{d+1} p(g_d/L_d) = \sum_{1 \leq i \leq d} (-1)^{i+1} (g_i/L_i)\, \ell_{d-i}^{q^i} .$$

As noted in (11.1), $\ell_i \equiv 0 \bmod p$ if $i < d$. Thus, if $1 \leq i < d$, $\ell_{d-i}^{q^i}/L_i \equiv 0$ since L_i is not divisible by p .

Also, if $i = d$ then $\ell_{d-i}^{q^i}/L_i = p^{q^d}/L_d \equiv 0 \bmod p^{(q^d-1)}$.

Thus $$\ell_d \equiv (-1)^d (p/L_d) g_d \bmod p^n$$

$$n = \inf (q^d - 1, q)$$

$$\equiv g_d \bmod p \quad \text{by } (11.4)$$

$$\equiv 1 \bmod p \quad \text{by } (6.12) .$$

Let now $F_i(X,Y) \in A[X,Y]$ be the uniquely determined polynomial such that

$$F_i(g,\Delta) = \ell_i = i\text{-th coefficient of } TD_p .$$

<u>11.6. Lemma:</u>

(i) We have $F_0 = p$, $F_1 = (p^q - p)/[1]\cdot X$, and for $i \geq 2$

$$[i]F_i = XF_{i-1}^q - X^{q^{i-1}} F_{i-1} + YF_{i-2}^{q^2} - Y^{q^{i-2}} F_{i-2} .$$

(ii) Considered as a polynomial in X , F_d has degree $(q^d - 1)/(q - 1)$ and leading coefficient 1.

(iii) $F_{2d} = Y^{(q^{2d}-1)/(q^2-1)}$ and $F_{2d+1} = 0$.

<u>Proof:</u> (i) follows from the commutator relation

$TD_pTD_T = TD_TTD_p$. (ii) results from (i): By induction on i , one shows: For $i \leq d$, F_i has degree $(q^i - 1)/(q-1)$ in X , and the leading coefficient satisfies the recursion for the coefficients of ρ_p given in (4.4). Finally, (iii) is a direct consequence of the definition.

Now consider the reduced polynomials $\tilde{F}_i(X,Y)$. From $[\tilde{i}] \neq 0 \, (0<i<d)$ and (11.6 i), we see $\tilde{F}_i = 0$ if $i < d$. Thus, again from the recursion and $[\tilde{i}] \neq 0$ $(d < i < 2d)$, we derive: $\tilde{F}_d$ divides $\tilde{F}_i$ if $d \leq i < 2d$.

<u>11.7. Proposition:</u> $\tilde{F}_d(X,Y)$ is square-free.

<u>Proof:</u> Let $f(X) = \tilde{F}_{2d-1}(X,1)$. From (11.6 i) applied to $i = 2d+1$, we see $f'(X) = 1$. Now $\tilde{F}_{2d-1}$ being an isobaric polynomial in X and Y , this implies $\tilde{F}_{2d-1}$, thus $\tilde{F}_d$, to have at most a monomial in Y as a multiple divisor. Putting $t = 0$, the Tate-Drinfeld module TD reduces to the Carlitz module, in particular $\ell_d = 1 + o(t)$ as well as $\tilde{\ell}_d = 1 + o(t)$. But if Y divided $\tilde{F}_d$ then $\tilde{\ell}_d = o(t)$.

<u>12. Modular forms mod *p*</u>

We keep the notations of the last section. Let further $M_p = \oplus M^m_{p,k}$ be the ring of modular forms (any weight or type) having coefficients in K with denominators prime to p , and $\tilde{M} = \{\tilde{f} \in \mathbb{F}_p[[t]] \mid \exists\, f \in M_p \text{ s.t. } f \bmod p = \tilde{f}\}$ the <u>ring of modular forms mod *p*</u> . We are going to determine the structure of

$\tilde{M}$ as an $\mathbb{F}_p$ - algebra. M_p containing the prominent members g and Δ, we have the ring homomorphism

$$\varepsilon : \quad \mathbb{F}_p[X,Y] \longrightarrow \mathbb{F}_p[[t]] ,$$

$$(X,Y) \longmapsto (\tilde{g},\tilde{\Delta})$$

where $\tilde{g}$ resp. $\tilde{\Delta}$ are the expansions mod p of g resp. Δ. Accordingly, putting $Z^{q-1} = -Y$, we may consider

$$\varepsilon' : \quad \mathbb{F}_p[X,Z] \longrightarrow \mathbb{F}_p[[t]] .$$

$$(X,Z) \longmapsto (\tilde{g},\tilde{h})$$

By (11.5), $\tilde{F}_d(X,Y) - 1$ lies in $\ker \varepsilon$.

<u>12.1. Theorem:</u> $\tilde{F}_d(X,Y) - 1$ generates $\ker \varepsilon$.

<u>Proof:</u> A priori, $\ker \varepsilon$ is a non-maximal prime ideal. Therefore, by dimension reasons, we only have to show $\tilde{F}_d(X,Y) - 1$ is irreducible. This follows from (11.7) as in [18]: Suppose $\tilde{F}_d(X,Y) - 1 = R \cdot S$ is a non-trivial factorization. Writing $R = \sum_{i \le m} R_i$, $S = \sum_{j \le n} S_j$ as a sum of its isobaric components (of course, the weight of X resp. Y is $q-1$ resp. q^2-1), we have $R_m S_n = \tilde{F}_d$. Since m and n are > 0 and $\tilde{F}_d$ is square-free, $(R_m,S_n) = 1$. From $R_m S_{n-1} + R_{m-1} S_n = 0$ we derive $S_{n-1} = 0 = R_{m-1}$

and, exploiting the vanishing of the intermediate terms, $R_i = S_j = 0$ for $i < m$, $j < n$ which contradicts $R_0 S_0 = -1$.

Let now $A_k \in A[X,Y]$ (resp. $B_k \in A[X,Z]$) the polynomial defined by $A_k(g,\Delta) = g_k$ (resp. $B_k(g,h) = g_k$). Then $B_k(X,Z) = A_k(X, -Z^{q-1})$, and from (6.9), we deduce

$$(12.2) \qquad A_k = -[k-1]A_{k-2}Y^{q^{k-2}} + A_{k-1}X^{q^{k-1}} .$$

Thus, considered as a polynomial in X, A_k is monic of degree $(q^k - 1)/(q-1)$.

<u>12.3. Corollary:</u> $\tilde{A}_d = \tilde{F}_d$.

<u>Proof:</u> $\tilde{A}_d - 1 \in \ker \varepsilon$ is a multiple of $\tilde{F}_d - 1$. Comparing leading coefficients in X, (11.6 ii) shows they are equal.

<u>12.4. Corollary:</u> $\ker \varepsilon' = (\tilde{B}_d - 1)$.

<u>Proof:</u> (12.3) and the argument in (11.7) shows $\tilde{B}_d$ to be square-free which, as we know, implies the assertion.

The next corollary follows as in [16], p. 168.

<u>12.5. Corollary:</u> Let $f_i \in M_p$ be of weight $k_i (i = 1,2)$, and suppose $f_1 \equiv f_2 \not\equiv 0 \bmod p$. Then $k_1 \equiv k_2 \bmod (q^d - 1)$.

Thus $\widetilde{M}$ has a natural grading by $\mathbb{Z}/n$, $n = q^d - 1$:

$$\widetilde{M} = \bigoplus_{i \in \mathbb{Z}/n} \widetilde{M}_i \quad , \quad \widetilde{M}_i = \Big(\sum_{\substack{k,m \in \mathbb{Z} \\ k \equiv i \bmod n}} M^m_{p,k} \Big)^\sim .$$

Let further $\widetilde{M}^0 = \oplus \widetilde{M}^0_i$, $\widetilde{M}^0_i = \Big(\sum_{\substack{k \in \mathbb{Z} \\ k \equiv i \bmod n}} M^0_{p,k} \Big)^\sim$.

12.6. Theorem: $\widetilde{M}$ is normal (i.e. integrally closed in its quotient field).

Proof: We are going to show: The affine curve defined by $\widetilde{B}_d(X,Z) - 1 = 0$ is non-singular. As $\widetilde{M} \cong \mathbb{F}_p[X,Z]/(\widetilde{B}_d(X,Z) - 1)$, this will prove the assertion. We have $B_1(X,Z) = X$ and $B_2(X,Z) = [1]Z^{q-1} + X^{q+1}$ which shows the non-singularity of $B_k = 1$ for $k = 1,2$ as well as that of $\widetilde{B}_k = 1$. Consider now the case $k \geq 3$. From (12.2), we derive

$$(*) \qquad \frac{\partial}{\partial X} B_k(X,Z) = 0 = \frac{\partial}{\partial Z} B_k(X,Z)$$

is equivalent with the system of equations

$$(**) \qquad \begin{pmatrix} \frac{\partial}{\partial X} B_{k-2} & \frac{\partial}{\partial X} B_{k-1} \\ \frac{\partial}{\partial Z} B_{k-2} & \frac{\partial}{\partial Z} B_{k-1} \end{pmatrix} \begin{pmatrix} [k-1]\; Z^{q^{k-2}(q-1)} \\ X^{q^{k-1}} \end{pmatrix} = 0 .$$

Using Lemma 12.7, the determinant of the 2×2-matrix is a monomial in Z. Thus, (*) implies at least $Z = 0$. Now we apply induction to the assertion

"(*) implies $X = Z = 0$"

which is satisfied for $k = 3$. Let $k > 3$, and assume (*). By (**), $\frac{\partial}{\partial X} B_{k-1} X^{q^{k-1}} = 0 = \frac{\partial}{\partial Z} B_{k-1} X^{q^{k-1}}$, and either $X = 0$ or $\frac{\partial}{\partial X} B_{k-1} = 0 = \frac{\partial}{\partial Z} B_{k-1}$ which in turn, by induction hypothesis, implies $X = 0$. Thus in any case, (*) implies $X = Z = 0$. Since $(0,0)$ does not lie on $B_k(X,Z) = 1$, this curve is non-singular. If $2 \leq k \leq d$, $[k-1] \not\equiv 0 \bmod p$, and the above argument works $\bmod\, p$, thereby proving the non-singularity of $\tilde{B}_k(X,Z) = 1$.

<u>12.7. Lemma:</u> Let $V_k = \frac{\partial}{\partial X} B_{k-2} \frac{\partial}{\partial Z} B_{k-1} - \frac{\partial}{\partial X} B_{k-1} \frac{\partial}{\partial Z} B_{k-2}$.

Then $V_3 = -[1]Z^{q-2}$, and for $k \geq 3$

$$V_{k+1} = -[k-1]Z^{q^{k-2}(q-1)} V_k .$$

<u>Proof:</u> (12.2) and an easy induction.

<u>12.8. Remark:</u> From (12.6), the normality of various subrings of $\tilde{M}$ results, e.g. $\tilde{M}^0$, $\tilde{M}_0$, and $\tilde{M}_0^0$ are normal. The corresponding coverings of affine algebraic curves over $\mathbb{F}_p$ may be geometrically described in terms of modular curves. For example,

Spec $\tilde{M}_0^0$ = affine j-line over $\mathbb{F}_p$ minus { supersingular values of j } . This is analogous with results in the number theoretic case, e.g. [14] or [15].

12.9. Examples:

(i) Let $d = \deg p = 1$. Then $\tilde{g} = 1$, $\tilde{M}^0 = \mathbb{F}_p[\tilde{\Delta}]$, and $\tilde{M} = \mathbb{F}_p[\tilde{h}]$.

(ii) Let $d = 2$. From $B_2(X,Z) = [1]Z^{q-1} + X^{q+1}$ we see $\tilde{\Delta} = (\tilde{g}^{q+1} - 1)/[\tilde{1}]$, $\tilde{M}^0 = \mathbb{F}_p[\tilde{g}]$, and $\tilde{M} = \mathbb{F}_p[\tilde{g},\tilde{h}]$, where $[1]\tilde{h}^{q-1} + \tilde{g}^{q+1} = 1$.

(iii) Let $d = 3$. We have $B_3(X,Z) = [2]XZ^{q(q-1)} + [1]X^{q^2}Z^{q-1} + X^{q^2+q+1}$, thus the full set of relations between $\tilde{g}$, $\tilde{h}$, and $\tilde{\Delta}$.

Index

References

[1] L. Carlitz. An analogue of the Staudt-Clausen theorem. Duke Math. J. 3, 503-517, 1937, and 7, 62-67, 1940

[2] V.G. Drinfeld. Elliptic Modules (Russian). Math. Sbornik 94, 594-627, 1974. English Translation: Math. USSR-Sbornik 23, 561-592, 1976

[3] J. Fresnel - M. van der Put. Géométrie Analytique Rigide et Applications. Progress in Mathematics 18, Birkhäuser 1981

[4] E.-U. Gekeler. Zur Arithmetik von Drinfeld-Moduln. Math. Annalen 262, 167-182, 1983

[5] E.-U. Gekeler. A Product Expansion for the Discriminant Function of Drinfeld Modules of Rank Two. J. Number Theory 21, 135-140, 1985.

[6] E.-U. Gekeler. Modulare Einheiten für Funktionenkörper. J. reine angew. Math. 348, 94-115, 1984

[7] E.-U. Gekeler. Drinfeld Modular Curves. Lecture Notes in Mathematics 1231. Springer-Verlag 1986

[8] L. Gerritzen-M. van der Put. Schottky Groups and Mumford Curves. Lecture Notes in Mathematics 817. Springer-Verlag 1980

[9] D. Goss. Von Staudt for $\mathbb{F}_q[T]$. Duke Math. J. 45, 885-910, 1978

[10] D. Goss. π - adic Eisenstein Series for Function Fields. Comp. Math. 41, 3-38, 1980

[11] D. Goss. Modular Forms for $\mathbb{F}_r[T]$. J. reine angew. Math. 317, 16-39, 1980

[12] D. Goss. The Algebraist's Upper Half-Plane. Bull. Amer. Math. Soc. NS 2, 391-415, 1980

[13] D. Hayes. Explicit class field theory for rational function fields. Trans. Amer. Math. Soc. 189, 77-91, 1974

[14] J. Igusa. On the algebraic theory of elliptic modular functions. J. Math. Soc. Japan 20, 96-106, 1968

[15] N. Katz. Higher congruences between modular forms. Ann. Math. 101, 332-367, 1975

[16] S. Lang. Introduction to Modular Forms. Springer-Verlag 1976

[17] W. Radtke. Diskontinuierliche arithmetische Gruppen im Funktionenkörperfall. J. reine angew. Math. 363, 191-200, 1985

[18] H.P.F. Swinnerton-Dyer. On ℓ-adic representations and congruences for coefficients of modular forms. Lecture Notes in Mathematics 350, 1-55, 1973

[19] J. Yu. Transcendence and Drinfeld Modules. Inv. Math. 83, 507-517, 1986