ANALOGIES BETWEEN FUNCTION FIELDS AND NUMBER FIELDS

By B. MAZUR and A. WILES

Dedicated to André Weil for his 77th birthday

In *Analogies between number fields and function fields* [I], Iwasawa outlined his theory of p-cyclotomic extensions. Iwasawa was inspired by Weil's theory of the characteristic polynomial of Frobenius acting on the jacobian of a curve over a finite field. His object was to set up an undeniably analogous, but more difficult theory for number fields K and finite (1-dimensional, p-adic valued) characters χ of the Galois group $\mathrm{Gal}(\bar{K}/K)$ (of conductors not divisible by p^2). In place of the characteristic polynomial of the Frobenius operator, Iwasawa obtained his characteristic polynomial by considering the action of the Galois group of the p-cyclotomic extension of K_χ (the abelian extension cut out by χ) on a certain p-adic vector space. This vector space was constructed by first taking a limit of χ-parts of p-primary components of ideal class groups, and then tensoring over Z_p with Q_p.

Let p be an odd prime. In [M-W] we establish a conjecture of Iwasawa that, when $K = Q$ and χ is odd, the zeroes of Iwasawa's characteristic polynomial are given, after a change of variables, by the zeroes of the Kubota-Leopoldt p-adic L function $L_p(\omega\chi^{-1}, s)$ in the extended s-disc, where ω is the Teichmuller character (cf. Section 1).

A point made quite convincingly in [I] is that archetypes for the study of number fields can be found in the context of function fields (which are considered to be easier).*

More recently, there has been some traffic in the opposite direction.

One may view the work of Hayes [H], Galovich-Rosen [G-R], and Goss [G] (as well as some of the prior work of Carlitz and Drinfeld) as

---

Manuscript received December 21, 1982.

*In this connection, see also Weil's *Sur l'analogie entre les corps de nombres algébriques et les corpes de fonctions algébriques* [W] where a (positive real number) invariant is defined for a number field, which plays a role analogous to that of the genus of a function field of one variable.

taking the classical theory of cyclotomic fields (as developed by Kummer, Stickelberger, Iwasawa) as model, and obtaining closely analogous theories in the setting of curves over finite fields. Moreover these new theories for curves over finite fields, at least at present view, show every sign of being just as difficult as their classical number-theoretic counterpart.

In the course of our work on the Iwasawa conjecture, we came across another specific analogue of the classical theory of cyclotomic fields in the context of function fields over finite fields. We consider the tower of Igusa curves of level p^n for $n \geq 0$ (Section 3). For each even nontrivial character $\chi: \mathbf{F}_p^* \to Z_p^*$ we form the direct limit of the χ-part of the p-primary component of the group of $\mathbf{F}_p$-rational points of the jacobians of these curves. If Λ is Iwasawa's ring (cf. Section 1), the Pontrjagin dual of this module has a natural Λ-module structure and we obtain a canonical element $D_p(\chi)$ in Λ which is a generator of its characteristic ideal. As usual, we may view $D_p(\chi)$ as giving rise to a p-adic analytic function of the variable s, $D_p(\chi, s)$, convergent in the extended s-disc (cf. Section 1). What are the zeroes of the analytic function $D_p(\chi, s)$ in the extended disc?

The main result of this article (which draws from the theory developed in [M-W]) is that the zeroes of $D_p(\chi, s)$ *include* the zeroes of the Kubota-Leopoldt p-adic L function $L_p(\chi\omega^2, -1 - s)$. More precisely, the quotient of these two functions is again an Iwasawa function (and hence analytic in the extended s-disc). Consequently our function field analogue is more than just an analogue! We are at a loss, however, to explain the significance, if any, of the remaining zeroes of $D_p(\chi, s)$. Certain of these other zeroes arise from the existence of unramified Grossencharacters for $Q(\sqrt{-p})$ when $p \equiv -1 \bmod 4$, and the class number of $Q(\sqrt{-p})$ is >1 (cf. Proposition 10), but Atkin has found a few others as well (cf. the end of Section 3).

As an element of Iwasawa's ring Λ, the Iwasawa function $D_p(\chi, s)$ is "proalgebraic" (see Section 1). Under a special assumption (see Proposition 4) $1 + D_p(\chi, s)$ is "proalgebraic of Weil type" (again see Section 1 for the definition; roughly speaking it means that it can be expressed in terms of an infinite sequence of algebraic integers, all of whose complex absolute values are equal to p^r, where r is a fixed half-integer). In general, the function $D_p(\chi, s)$ can be expressed up to a unit in Λ as the Norm to Λ of a certain element in a certain Hecke algebra $\mathbf{T}(\chi)$. The algebra $\mathbf{T}(\chi)$ arises as a faithful ring of endomorphisms of our theory, generated by the Hecke operators T_l ($l \neq p$), the Frobenius endomorphism Φ, and by the "diamond operators." We show that $\mathbf{T}(\chi)$ is a finite flat Λ-algebra, and conse-

quently it is a Cohen-Macaulay complete semi-local noetherian ring of dimension 2.

The present paper is a preliminary investigation (and we confine our attention to the simplest case: powers of the Teichmuller character) carried out in the hope that it may find a use in some future study of the zeroes of p-adic L functions.

1. Iwasawa's ring. Let p be an odd prime number. The subgroup of 1-*units*,

$$\Gamma \subset Z_p^*$$

is the kernel of the homomorphism $Z_p^* \to \mathbf{F}_p^*$ given by reduction mod p. The *Teichmuller character*

$$\omega : \mathbf{F}_p^* \to Z_p^*$$

is the unique homomorphism which is an inverse to reduction mod p. Viewing $\mathbf{F}_p^*$ as subgroup of Z_p^* via the Teichmuller character, we have a canonical product decomposition

$$Z_p^* \cong \mathbf{F}_p^* \times \Gamma.$$

Any $\gamma \in \Gamma$ such that $\gamma \not\equiv 1 \bmod p^2$ is a topological generator of Γ. Let Γ_n denote the unique subgroup of index p^{n-1}, $\Gamma_n = \Gamma^{p^{n-1}}$. Let *Iwasawa's ring* Λ be equal to the completed Z_p-integral group ring of Γ, $Z_p[[\Gamma]]$; it is defined to be the projective limit

$$\Lambda = \varprojlim_n \Lambda_n \quad \text{where} \quad \Lambda_n = Z_p[\Gamma/\Gamma_n].$$

Given a choice of topological generator γ, there is a unique isomorphism $\Lambda \cong_{i_\gamma} Z_p[[T]]$, of Λ onto the power series ring in one variable with coefficients in Z_p, which sends the image of γ to the power series $1 + T$.

Although there is no natural choice of topological generator γ, fix such a choice. If D is an element of Λ, we will denote by $\mathfrak{D}(T) \in Z_p[[T]]$ the power series in T corresponding to D, under the isomorphism i_γ.

For any p-adic integer s, let $r_s : \Gamma \to Z_p$ be the continuous mapping $x \mapsto x^s$. Then r_s extends to a ring-homomorphism $r_s : \Lambda \to Z_p$. If $D \in \Lambda$, let $D(s) \in Z_p[[s]]$ denote the p-adic analytic function of the variable s defined by

$$D(s) = r_s(D) = \mathfrak{D}(r_s(\gamma) - 1).$$

The function $D(s)$ extends to an analytic function in the domain $|s|_p < p^{(p-2)/(p-1)}$, which we refer to as the *extended s-disc*. Here $|\ |_p$ is the normalized p-adic absolute value, $|p|_p = 1/p$. The transformation $T \mapsto r_s(\gamma) - 1$ is an isomorphism between the open unit T-disc and the extended s-disc.

We refer to an analytic function on the extended s-adic as an *Iwasawa function* if it can be expressed as $D(s)$, for some element D in Λ. If $D(s)$ is an Iwasawa function, then the element D which gives rise to it is unique. One can then identify an Iwasawa function $D(s)$ with this element in Iwasawa's ring, and we shall do so when it is convenient.

Recall that the Kubota-Leopoldt p-adic L functions $L_p(\omega^j, s)$ are Iwasawa functions for even $j \not\equiv 0 \bmod p - 1$. The *$\mu$-invariant* of an element $D \in \Lambda$ is the maximal integer ($\mu \leq +\infty$) such that p^μ divides D in Λ. The *λ-invariant* ($\lambda \leq +\infty$) of D is the number of zeroes of $D(s)$ in the extended s-disc. Equivalently, it is the number of zeroes of $\mathfrak{D}(T)$ in the unit T-disc. Equivalently, it is the dimension of the Q_p-vector space

$$Q_p \otimes_{Z_p} (\Lambda/D \cdot \Lambda).$$

We shall call an element D of Λ *proalgebraic* if, for every homomorphism $h : \Lambda \to \bar{Q}_p$ which factors through $\Lambda \to \Lambda_n$ for some n, the image $h(D)$ is an algebraic integer in $\bar{Q}_p$. We shall say that D is *proalgebraic of Weil type* if it is proalgebraic and there is a half-integer $r \in 1/2 \cdot Z$ such that for all homomorphisms h as above, and all archimedean imbeddings $x \mapsto x_v$ of $\bar{Q}$ in the complex numbers,

$$|h(D)_v| = p^r.$$

2. Towers. Let k be a perfect field of characteristic p. Let

$$\tau_{/k} : \cdots \to X_n \to X_{n-1} \to \cdots \to X_0$$

be a sequence of mappings of smooth connected projective curves over k such that X_n is a Galois covering of X_0 with Galois group canonically isomorphic to

$$(Z/p^n Z)^*/(\pm 1) = \Delta \times \Gamma/\Gamma_n \quad \text{for} \quad n \geq 1, \qquad \text{where} \quad \Delta = \mathbf{F}_p^*/(\pm 1).$$

Suppose further that for each $n \geq 2$, if $S_n \subset X_n(\bar{k})$ denotes the set of points of ramification for the covering $X_n \to X_1$, then S_n is a nonempty set on which $\mathrm{Gal}(X_n/X_0)$ operates trivially.

We shall call such a sequence of curves satisfying the above hypotheses a *tower over* k.

Fix $\chi = \omega^i : (Z/pZ)^* \to Z_p^*$ a nontrivial character which is an even power of the Teichmuller character.

Let $J_{n/k}$ denote the jacobian of $X_{n/k}$. For $m \geq n$, the mapping $X_m \to X_n$ induces an injection $J_n \hookrightarrow J_m$ obtained by identifying jacobians with Pic^0. It is injective since there are totally ramified points of the covering $X_m \to X_n$.

Let $J_n(k, \chi)$ denote the χ-component of the p-primary component of the group of k-valued points of J_n. The action of Γ/Γ_n induces a natural Λ_n-module structure on $J_n(k, \chi)$. An elementary calculation, using the fact that Δ operates trivially on the ramification points of the covering $X_m \hookrightarrow X_n$, and that χ is a nontrivial character on Δ, gives that the injection $J_n \hookrightarrow J_m$ induces an isomorphism:

$$J_n(k, \chi) \xrightarrow[\cong]{} J_m(k, \chi)^{\Gamma_n} \tag{1}$$

where the superscript Γ_n denotes the subspace of Γ_n-invariant elements.

Let $M_n(k, \chi)$ denote the Pontrjagin dual of $J_n(k, \chi)$ given its natural Λ_n-module structure. Then the injections $J_n \hookrightarrow J_m$ induce surjections $M_m(k, \chi) \twoheadrightarrow M_n(k, \chi)$ and the dual of (1) is an isomorphism

$$M_m(k, \chi) \underset{\Lambda}{\otimes} \Lambda_n \xrightarrow[\cong]{} M_n(k, \chi). \tag{2}$$

Let $M(k, \chi) = \lim_{\leftarrow n} M_n(k, \chi)$ endowed with its natural Λ-module structure. From (2) we obtain:

PROPOSITION 1. *The natural mapping* $M(k, \chi) \to M_n(k, \chi)$ *induces an isomorphism*

$$M(k, \chi) \underset{\Lambda}{\otimes} \Lambda_n \xrightarrow[\cong]{} M_n(k, \chi)$$

for any $n \geq 1$.

PROPOSITION 2. *If* k *is algebraically closed, then* $M(k, \chi)$ *is a free* Λ*-module of rank equal to the* Z_p*-rank of* $M_1(k, \chi)$.

Proof. In view of Proposition 1, an elementary argument shows that it is sufficient to prove that $M_n(k, \chi)$ is free over Λ_n (of finite rank), for all n. For this, it is sufficient to show that the χ-component of

$\mathrm{Hom}(J_n(k)[p^m], Q_p/Z_p)$ is free over $\Lambda_n/p^m \cdot \Lambda_n$ for all m, n. But, identifying J_n with the Albanese variety of X_n we have a canonical isomorphism

$$\mathrm{Hom}(J_n(k)[p^m], Q_p/Z_p) \cong H^1_{\text{ét}}(X_n, Z/p^m Z)$$

where $H^1_{\text{ét}}$ means étale cohomology. Compare [Ka-L].

We must therefore show that the χ-component of $H^1_{\text{ét}}(X_n, Z/p^m Z)$ is free over $Z/p^m Z[\Gamma/\Gamma_n]$ for every m and $n \geq 1$.

Fix n, m and set $X = X_n$, $S = S_n$, $R = Z/p^m Z$, $G = \Gamma/\Gamma_n$.

Let $H^r_c(X - S, R)$ denote r-dimensional étale cohomology with compact supports, with coefficients in the ring R. By Proposition 1.2 of [C1] or of [C2] there is a perfect complex $K^\cdot$ of $R[G]$-modules such that

$$H^r(K^\cdot) = H^r_c(X - S, R)$$

for all r. See also SGA 4 1/2 Rapport 4.9. For background in perfect complexes, see SGA 6 I.

Using the fact that Δ acts trivially on S, that S is nonempty, and that χ is a nontrivial character of Δ, one sees that:

$$H^r_c(X - S, R) = 0 \quad \text{if} \quad r \neq 1, 2$$

and

$$H^1_c(X - S, R)^\chi = H^1(X, R)^\chi.$$

$$H^2_c(X - S, R)^\chi = 0,$$

where the superscript χ denotes χ-component.

Let $\hat{H}^s(G, \text{-})$ denote reduced cohomology of the cyclic group G. Then $\hat{H}^s(G, K^i) = 0$, for all p and all i, where K^i is the i-dimensional $R[G]$-module of the complex $K^\cdot$. Since the only nonvanishing cohomology groups $H^r(K^\cdot)$ are for $r = 1, 2$, an elementary cohomological calculation yields that $\hat{H}^{s+2}(G, H^1(K^\cdot))$ is canonically isomorphic to $\hat{H}^s(G, H^2(K^\cdot))$ for all s. Taking χ-components, and noting that the χ-component of $H^2(K^\cdot) = H^2_c(X - S, R)$ vanishes, we obtain that

$$\hat{H}^s(G, H^1(X, R)^\chi) = 0 \quad \text{for all } s.$$

But $H^1(X, R)^\chi$ is a free R-module, and Theorems 6, 7 of Chapter IX of [S2] apply to yield that $H^1(X, R)^\chi$ is free over $R[G]$.

Now let k be a finite field, and $\bar{k}$ an algebraic closure. Let $\varphi: \bar{k} \to \bar{k}$ denote the Frobenius automorphism ($x \mapsto x^{\mathrm{card}(k)}$).

If $\tau_{/k}$ is a tower over k, then φ induces an endomorphism Φ of the Λ-module $M(\bar{k}, \chi)$. If $r = r(\chi)$ is the rank of this module (which is free, by Proposition 2) then, upon making a choice of Λ-basis, we may view Φ as an $r \times r$ matrix with entries in Λ.

PROPOSITION 3. *The Λ-module $M(\tau, k, \chi) = M(k, \chi)$ admits a free Λ-resolution of the form*

$$0 \to M(\bar{k}, \chi) \xrightarrow{\Phi - 1} M(\bar{k}, \chi) \to M(k, \chi) \to 0.$$

Proof. For each $n \geq 1$ we have an exact sequence

$$0 \to J_n(k, \chi) \to J_n(\bar{k}, \chi) \xrightarrow{\Phi - 1} J_n(\bar{k}, \chi) \to 0$$

giving the exact sequence

$$0 \to M_n(\bar{k}, \chi) \xrightarrow{\Phi - 1} M_n(\bar{k}, \chi) \to M_n(k, \chi) \to 0$$

by Pontrjagin duality. Proposition 3 then follows from an elementary limit argument using Proposition 1.

COROLLARY. *The Λ-module $M(k, \chi)$ is a finitely generated Λ-torsion module, possessing no finite Λ-submodules. The characteristic ideal of $M(k, \chi)$ is equal to its Λ-Fitting ideal, which is the principle ideal generated by the determinant of the $r \times r$ matrix $\Phi - 1$.*

Definition. *The characteristic element* of the tower $\tau_{/k}$ and χ is

$$D(k, \chi) = D(\tau, k, \chi) \overset{\text{defn}}{=} \det_\Lambda \Phi \in \Lambda.$$

As in Section 1, denote by $D(k, \chi, s)$ the Iwasawa function associated to $D(k, \chi) \in \Lambda$. We refer to $D(k, \chi, s)$ as the *characteristic function* of $\tau_{/k}$ and χ.

Remark. Ralph Greenberg has constructed examples of towers over

k and characters χ where the characteristic element $D(k, \chi)$ is divisible by p, i.e., where the μ-invariant is nontrivial.

PROPOSITION 4. *The characteristic element $D(k, \chi)$ is a proalgebraic element of Λ. If $r(\chi) = \operatorname{rank}_\Lambda M(\bar{k}, \chi)$ is equal to 1, then $D(k, \chi) + 1$ is a proalgebraic element of Weil type (cf. Section 1).*

Proof. Let Φ_n denote the Frobenius endomorphism of $M_n(\bar{k}, \chi)$ for each n. Then $\det_\Lambda(\Phi - 1)$ is the limit of $\det_{\Lambda_n}(\Phi_n - 1)$ as n tends to ∞. Since the characteristic polynomial of Φ_n has integral coefficients, the first assertion of our proposition easily follows. In case $r(\chi) = 1$, $D(k, \chi) + 1$ is equal to Φ; the second assertion is then immediate.

PROPOSITION 5 and DEFINITION. *The tower $\tau_{/k}$ is said to be* regular at χ *if equivalently*:

(a) *The characteristic element $D(k, \chi)$ is a unit in Λ.*

(b) $M(k, \chi) = 0$.

(c) *The χ-component of the p-primary component of $J_1(k)$ vanishes.*

Equivalence of (a) and (b) follows from the corollary. That (b) and (c) are equivalent follows from Proposition 1 and Nakayama's lemma.

3. Igusa Towers. Fix an odd prime number p, and set $k = \mathbf{F}_p$. For $n \geq 0$, let $X_{n/k}$ be the *Igusa curve of level p^n*. Thus X_n is a smooth, geometrically connected projective curve with the following property:

For $n \geq 1$, X_n contains an affine open subcurve which represents the moduli problem:

$$S \text{ (a scheme of characteristic } p) \dashrightarrow \begin{cases} \text{isomorphism classes of (ordinary)} \\ \text{elliptic curves } E \text{ over } S \\ \text{together with a point } P \text{ in } E^{(p^n)}(S) \\ \text{which generates the kernel of the} \\ n\text{-th iterate of Verschiebung} \\ V^n : E^{(p^n)} \to E. \end{cases}$$

For an exposition of Igusa curves, see [K-M] Chapter XII. One has a natural action of $(Z/p^nZ)^*/(\pm 1) = \Delta$ on X_n, the so-called diamond operators: If $a \in (Z/p^nZ)^*$ let $\langle a \rangle : X_n \to X_n$ be the automorphism which sends the isomorphism class (E, P) to $(E, a \cdot P)$. Define the base curve X_0 to be the quotient of X_1 by the action of the diamond operators. Then X_0 is a curve of genus zero, parametrized by the "elliptic modular function" j. For $m \geq$

n, there are natural mappings $X_m \to X_n$ given by $(E, P) \mapsto (E, V^{m-n}P)$, which identifies X_n with the quotient of X_m under the action of the subgroup of diamond operators in $(Z/p^mZ)^*$ consisting of those $\langle a \rangle$ such that $a \equiv 1 \bmod p^{m-n}$.

The sequence

$$\tau_{/\mathbf{F}_p}: \cdots \to X_{n+1} \to X_n \to \cdots \to X_0$$

forms a tower over $\mathbf{F}_p$ in the sense of Section 2; we shall call it the *Igusa tower*. The subset $S_n \subset X_n(\bar{k})$ is the set of supersingular points of X_n. These points are rational over $\mathbf{F}_{p^2}$. For Atkin's table of supersingular values of j, see [Mod-F].

The covering $X_1 \to X_0$ is a cyclic covering of degree $(p-1)/2$, totally ramified at the supersingular points, possessing at most two other points of ramification:

$j = 0$: If $j = 0$ is not supersingular, then its ramification index is 3.

$j = 1728$: If $j = 1728$ is not supersingular, then its ramification index is 2.

Examples. 1. The smallest prime p for which X_1 is of positive genus is $p = 13$. For $p = 13$, X_1 is an elliptic curve an affine equation for which is given by Serre in the form $6X^3 + 8Y^2 = 1$ where the point at ∞ is the unique supersingular point; the six cusps are obtained by letting X run through the cube roots of 1 in $\mathbf{F}_{13}$, and $Y = \pm 1$; the diamond operator $\langle a \rangle$ acting on (X, Y) is: $\langle a \rangle \cdot (x, Y) = (a^4X, a^6Y)$; the mapping to X_0 is given by $6X^3/(Y^2 - 1)$. The group of rational points of X_1 over $\mathbf{F}_{13}$ is of order 19, generated by the cusps.

2. If $p = 37$, then X_1 is a cyclic covering of P^1 of degree 18 totally ramified at the three supersingular points, which are solutions of

$$(j - 8)(j^2 - 6j - 6) = 0;$$

it is ramified at $j = 0$ with ramification index 3, and at $j = 1728$, with ramification index two; it is unramified elsewhere.

Now let $\chi = \omega^i$ for i an even integer not congruent to 0 mod $p - 1$ and let k be the even integer in the range $4 \le k \le p - 1$ such that $i \equiv k - 2 \bmod p - 1$.

Let us say that the pair (p, χ) is *Igusa-regular* if the Igusa tower is regular at χ (see Proposition 5 above).

PROPOSITION 6. *The pair (p, χ) is Igusa-regular if and only if the Atkin operator U (equivalently: the Hecke operator T_p) has no fixed non-trivial vectors (i.e., no eigenvalue 1) in the space of $SL_2(Z)$ modular forms modulo p, of weight congruent to k mod $p-1$.*

Proof. By Proposition 10 of Section 11 of [S1] we have a canonical isomorphism

$$J_1(\mathbf{F}_p)[p] \underset{\cong}{\to} H^0(X_{1/\mathbf{F}_p}, \Omega^1)[\text{C-1}]$$

where $[p]$ denotes the kernel of multiplication by p and [C-1] denotes the kernel of C-1, where C is the "operation of Cartier and Tate" (loc. cit. Section 10).

By Theorem 12.8.8 of [K-M] (this has also appeared in an unpublished letter from Serre to Fontaine) $H^0(X_{1/\mathbf{F}_p}, \Omega^1)$ can be identified with $\oplus_{k=2}^{p-1} S_k$ where S_k is the $\mathbf{F}_p$-vector space of cusp forms of weight k mod p over $SL_2(\mathbf{Z})$ (cf. [S3] 1.2). Under this identification, the operation C of "Cartier and Tate" may be identified with Atkin's operator U (or with T_p) whose effect on Fourier expansions is given by $\Sigma_{n=0}^{\infty} a_n q^n \mapsto \Sigma_{n=0}^{\infty} a_{pn} q^n$. The identifications are compatible with the action of diamond operators, giving an isomorphism

$$J_1(\mathbf{F}_p)[p](\chi) \cong S_k[U-1] \tag{4}$$

where $\chi = \omega^i$ and $i \equiv k-2 \bmod p-1$, and $[U-1]$ denotes the kernel of the endomorphism $U-1$.

We contrast the above Proposition with the following much deeper result which collects work of Kummer, Ribet, Iwasawa, and Kubota-Leopoldt: Let ζ_N denote a primitive N-th root of unity in an algebraic closure of Q.

PROPOSITION 7. *These are equivalent:*

(a) *The numerator of the k-th Bernoulli number is prime to p.*

(b) *The ω^{1-k}-component of the p-primary component of the ideal class group of $Q(\zeta_p)$ vanishes.*

(c) *The ω^{1-k}-component of the p-primary component of the ideal class group of $Q(\zeta_{p^n})$ vanishes, for any $n \geq 0$.*

(d) *The Kubota-Leopoldt p-adic L function $L_p(\omega^k, s)$ has no zeroes in the extended s-disc.*

Definition. If the equivalent conditions of Proposition 7 hold, then we say that (p, χ) is *classically regular*, where $\chi = \omega^{k-2}$.

A preliminary connection between the notions of classical and Igusa regularity is given by

PROPOSITION 8. *If (p, χ) is classically irregular, then it is Igusa irregular.*

Proof. If (p, χ) is classically irregular, then p divides the numerator of the Bernoulli number B_k. It follows that the Eisenstein series G_k with Fourier expansion

$$-B_k/2k + \sum_{n \geq 1} \sum_{d|n} d^{k-1} q^n$$

is a cuspform mod p. Compare [R] Section 3. Since this cuspform mod p is fixed under U, the vector space $S_k[U - 1]$ is nontrivial, and our Proposition follows from Proposition 6.

Let $\tau_{/\mathbf{F}_p}$ denote the Igusa tower, and $D_p(\chi) = D_p(\tau, \mathbf{F}_p, \chi)$ its characteristic element. Let $D_p(\chi, s)$ be the Iwasawa function associated to $D_p(\chi)$.

Example. If $p = 13$, and χ is either character of Δ of order 6, $r(\chi) = 1$. Consequently, $D_p(\chi) + 1$ is a proalgebraic element of Weil type (Proposition 4).

Our main result is the following connection between the zeroes of the Kubota-Leopoldt p-adic L function and those of $D_p(\chi, s)$.

PROPOSITION 9. *Let χ be different from the trivial character and from ω^{-2}. The Iwasawa function $L_p(\chi\omega^2, -1 - s)$ divides $D_p(\chi, s)$ in Iwasawa's ring Λ.*

Remark. Thus if θ is a zero of $L_p(\chi\omega^2, s)$ in the extended s-disc, occurring with multiplicity m, then $-1 - \theta$ is a zero of $D_p(\chi, s)$ with multiplicity $\geq m$.

Proof. We use the characteristic p version of Kubert-Lang theory [K-L] developed in chapter 4 of [M-W].

For each $n \geq 1$, a subgroup of the χ-component of the p primary component of $J_n(\mathbf{F}_p)$ was constructed in chapter 4 of [M-W]; we shall denote it $C^{(n)}(\chi)$ here, although in [M-W] it was called $C^{(n)}_{\mathfrak{m}}$ where $\mathfrak{m}$ is the maximal ideal in $Z_p[(Z/pZ)^*]$ generated by $(p, [a] - \chi(a)$ for $a \in (Z/pZ)^*)$. The subgroup $C^{(n)}(\chi)$ is stable under the action of the diamond operators and as Λ-module it is cyclic, with annihilator ideal generated by the image of

Γ_n and the element in Λ corresponding to the Iwasawa function $L_p(\chi\omega^2, -1-s)$. Consequently the Λ-Fitting ideal (cf. [M-W] Appendix) of $M(\tau, \mathbf{F}_p, \chi)$ is contained in the ideal generated by the image of Γ_n and $L_p(\chi\omega^2, -1-s)$. Since this is true for all n, the proposition follows.

What are the zeroes of the quotient

$$D_p(\chi, s)/L_p(\chi\omega^2, -1-s) \in \Lambda?$$

Can the μ-invariant of $D_p(\chi, s)$ be nonzero? How often is (p, χ) Igusa irregular, yet classically regular?

As Serre pointed out to us, there is another source of Igusa irregularity:

PROPOSITION 10. *Let p be a prime number such that $p \equiv -1 \bmod 4$ and such that the class number of $Q(\sqrt{-p})$ is greater than one. Then if $\chi = \omega^{(p-3)/2}$, the pair (p, χ) is Igusa irregular, yet classically regular.*

Proof. Let h be an ideal class of $Q(\sqrt{-p})$ and consider the q-expansion

$$\theta_h = \sum_{\mathfrak{a} \in h} q^{N\mathfrak{a}}$$

where $\mathfrak{a}$ runs through all ideals in the ring of integers of $Q(\sqrt{-p})$ which are members of the class h; $N\mathfrak{a}$ means the norm of $\mathfrak{a}$. Then if h is a nontrivial ideal class, $\theta_h - \theta_1$ represents a cuspform mod p of weight $k = (p+1)/2$, fixed under Atkin's U operator. Therefore, (p, χ) is Igusa-irregular for $\chi = \omega^i$, where $i = k - 2$. The pair (p, χ) is classically regular since p never divides the class number of $Q(\sqrt{-p})$.

Call a pair (p, χ) satisfying the hypotheses of Proposition 10 *θ-irregular*. Consequently, $D_p(\chi, s)$ has zeroes in the extended s-disc for $p \equiv -1 \bmod 4$, $p \geq 23$, $p \neq 43, 67$, and 163 and $\chi = \omega^{(p-3)/2}$. Can one say more about these zeroes? What do they signify?

As for other examples of Igusa irregular pairs, Atkin has provided us with the following data. In the range $24 \leq k \leq 82$ and $k < p < 181$, (p, ω^{k-2}) is Igusa irregular if it is classically, or θ-irregular, or if (p, k) take these eight values:

p	47	83	89	101	103	131	157	167
k	30	74	56	52	66	78	70	42

4. Hecke algebras of Krull dimension two. We keep the notation and assumptions of the previous section. Thus J_n is the jacobian of the Igusa curve of level n. If Φ is the Frobenius endomorphism of the Z_p-module $J_n(\bar{k}, \chi)$, let $J_n(\bar{k}, \chi)_0 \subset J_n(\bar{k}, \chi)$ denote the union of the kernels of $(\Phi - 1)^r$ for $r = 1, 2, \ldots$. Let $M_n(\bar{k}, \chi)_0$ be the Pontrjagin dual of $J_n(\bar{k}, \chi)_0$. We have that $M_n(\bar{k}, \chi)_0$ is a direct summand of the free Λ_n-module $M_n(\bar{k}, \chi)$ and is therefore also free over Λ_n, of rank, say, $r_0(\chi)$. One easily sees that

$$M_n(\bar{k}, \chi)_0 = \varprojlim_r M_n(\bar{k}, \chi)/(\Phi - 1)^r \cdot M_n(\bar{k}, \chi)$$

and that the sequence

$$0 \to M_n(\bar{k}, \chi)_0 \xrightarrow{\Phi - 1} M_n(\bar{k}, \chi)_0 \to M_n(k, \chi) \to 0$$

is exact.

Let $M(\bar{k}, \chi)_0$ denote the Λ-module $\varprojlim_n M_n(\bar{k}, \chi)_0$. Then $M(\bar{k}, \chi)_0$ is free of rank $r_0(\chi)$ over Λ.

Let $\mathbf{T}_n(\chi)$ denote the Z_p-subalgebra of the endomorphism ring of $J_n(\bar{k}, \chi)_0$ (or of $M_n(\bar{k}, \chi)_0$) generated by the Hecke operators T_l ($l \neq p$), Φ, and the diamond operators.

PROPOSITION 11. *The module $M_n(\bar{k}, \chi)_0$ is free of rank one over $\mathbf{T}_n(\chi)$. The Λ_n-algebra $\mathbf{T}_n(\chi)$ is finite and flat of rank $r_0(\chi)$.*

Proof. Let P be any maximal ideal in $\mathbf{T}_n(\chi)$. By the corollary to Proposition 1 of [M-W] Chapter 2 Section 10 (which is, in effect, an application of the "q-expansion principle" mod p), the kernel of P in $J_n(\bar{k}, \chi)_0$ is a vector space of dimension ≤ 1 over the residue field $k_P = \mathbf{T}_n(\chi)/P$.

Since $\mathbf{T}_n(\chi)$ acts faithfully on $J_n(\bar{k}, \chi)_0$, the kernel of P must be of dimension equal to 1. Since $\mathbf{T}_n(\chi)$ is a complete semi-local ring it follows from Nakayama's lemma that $M_n(\bar{k}, \chi)_0$ is a cyclic $\mathbf{T}_n(\chi)$-module. Since $M_n(\bar{k}, \chi)_0$ is a faithful $\mathbf{T}_n(\chi)$-module, it is free of rank 1.

The second assertion of our proposition then follows from Proposition 2. Let $\mathbf{T}(\chi)$ denote the projective limit of the algebras $\mathbf{T}_n(\chi)$, compiled by the natural mappings $\mathbf{T}_{n+1}(\chi) \to \mathbf{T}_n(\chi)$. Then Proposition 11 gives

COROLLARY 1. *$M(\bar{k}, \chi)_0$ is a free $\mathbf{T}(\chi)$-module of rank 1; $\mathbf{T}(\chi)$ is a finite flat Λ-module of rank $r_0(\chi)$.*

It follows that $\mathbf{T}(\chi)$ is a Cohen-Macaulay (semi-local) ring of dimension 2. It would be interesting to know more about its structure. Can it be nonregular? Non-normal? What is its "discriminant locus"?

For any prime number $l \neq p$, the Hecke operator T_l gives rise to an element in $\mathbf{T}(\chi)$. The characteristic polynomial of T_l over Λ has coefficients which are pro-algebraic elements of Λ.

COROLLARY 2. *The $\mathbf{T}(\chi)$-module $M(k, \chi)$ is isomorphic to $\mathbf{T}(\chi)/(\Phi - 1)$; the canonical generator $D(k, \chi)$ is equal to $N_{\mathbf{T}(\chi)/\Lambda}(\Phi - 1)$ times a unit in Λ.*

The cuspidal group $C^{(n)}(\chi)$ is left stable by the action of $\mathbf{T}_n(\chi)$ on $J_n(k, \chi)$. Define the *Eisenstein ideal* $I_n(\chi)$ to be the annihilator ideal of the $\mathbf{T}_n(\chi)$-module $C^{(n)}(\chi)$. Let $I(\chi) \subset \mathbf{T}(\chi)$ be the projective limit of the Eisenstein ideals $I_n(\chi)$. We have the ring-isomorphism

$$\Lambda/(L_p(\chi\omega^2, -1 - s)) \cong \mathbf{T}(\chi)/I(\chi).$$

Since $C^{(n)}(\chi)$ is in $J_n(k, \chi)$, $\Phi - 1$ is contained in the Eisenstein ideal $I(\chi)$.

Let $\mathbf{T}(\chi)^{\text{Eis}}$ denote the $I(\chi)$-adic completion of the ring $\mathbf{T}(\chi)$. Then $\mathbf{T}(\chi)^{\text{Eis}}$ is a local ring occurring as a direct product factor in $\mathbf{T}(\chi)$:

$$\mathbf{T}(\chi) = \mathbf{T}(\chi)^{\text{Eis}} \times \mathbf{T}(\chi)^0,$$

where $\mathbf{T}(\chi)^0$ denotes the complementary factor. This direct product decomposition yields a corresponding direct product decomposition in the modules $M(\bar{k}, \chi)_0$ and $M(k, \chi)$:

$$M(\bar{k}, \chi)_0 = M(\bar{k}, \chi)^{\text{Eis}} \times M(\bar{k}, \chi)^0$$

$$M(k, \chi) = M(k, \chi)^{\text{Eis}} \times M(k, \chi)^0$$

and the direct product decomposition of $M(k, \chi)$ gives a factorisation of $D_p(\chi, s)$:

$$D_p(\chi, s) = D_p(\chi, s)^{\text{Eis}} \cdot D_p(\chi, s)^0 \cdot (\text{unit in } \Lambda).$$

One can refine the proof of Proposition 9 to give that $L_p(\chi\omega^2, -1 - s)$ divides $D_p(\chi, s)^{\text{Eis}}$.

Are there examples where $\mathbf{T}(\chi)^{\text{Eis}}$ is of rank >1 over Λ? Can $D_p(\chi, s)^{\text{Eis}}/L_p(\chi\omega^2, -1 - s)$ have zeroes in the extended s-disc?

REFERENCES

[C1] Crew, R., *Slope characteristics in Crystalline cohomology,* Princeton PHD. Thesis, June 1981.

[C2] Crew, R., Etale p-covers in Characteristic p, submitted to *Compositio Math.*

[G-R] Galovich, S., and M. Rosen, The class number of cyclotomic function fields, *J. Number Theory*, **13** (1981), 363-376.

[G] Goss, D., The theory of totally-real function fields, preprint.

[H] Hayes, D., Analytic class number formulas in function fields, *Inventiones Math.* **65,** (1981), 49-70.

[I] Iwasawa, K., Analogies between number fields and function fields, preprint. Lecture given at the Yeshiva Science Conference.

[Ka-L] Katz, N., and S. Lang, Elementary finiteness theorems in geometric classfield theory, preprint, I.H.E.S., 1980.

[K-M] Katz, N., and B. Mazur, Arithmetic moduli of elliptic curves, preprint, Princeton, 1982.

[Ku-L] Kubert, D., and S. Lang, *Modular Units*, Springer-Verlag, New York, 1981.

[M-W] Mazur, B., and A. Wiles, Class fields of abelian extensions of Q, to be submitted for publication in *Inventiones Math.*

[R] Ribet, K., A modular construction of unramified p-extensions of $Q(\mu_p)$, *Inventiones Math.* **34**, (1976), 151-162.

[S1] Serre, J.-P, Sur la topologie des variétés algébriques en caractéristique p. Symposium Internacional de Topologia Algebraica. Published by La Universidad Nacional Autónoma de México and UNESCO, (1958), 24-53.

[S2] Serre, J.-P., *Corps Locaux.* Hermann, Paris, 1962.

[S3] Serre, J.-P., Formes modulaires et fonctions zêta p-adiques, Modular functions of one variable III. Proceedings of the International Summer School, University of Antwerp, RUCA, 1972, 191-268. Lecture Notes in Mathematics **350**. Springer-Verlag. Berlin-Heidelberg-New York, 1973.

[W] Weil, A., Sur l'analogie entre les corps de nombres algébriques et les corps de fonctions algébriques. Published in *André Weil, Oeuvres Scientifiques, Collected papers Volume* I, Springer-Verlag, New York, 1979, 236-240.

[Mod-F] *Modular functions of one variable* IV. Edited by B. J. Birch and W. Kuyk. Lecture Notes in Mathematics **476**. Springer-Verlag, Berlin-Heidelberg-New York, 1975.

[SGA 4 1/2] *Cohomologie Etale.* (by P. Deligne et al) *Lecture Notes in Mathematics* **569**. Springer-Verlag, Berlin-Heidelberg-New York, 1977.

[SGA 6] *Théorie des Intersections et Théorèmes de Riemann-Roch* (by P. Perthelot et al). Lecture Notes in Mathematics **225**. Springer-Verlag, Berlin-Heidelberg-New York, 1971.