Invent. math. 93, 637–666 (1988)

Inventiones mathematicae

On the Shafarevich-Tate group of the jacobian of a quotient of the Fermat curve

William G. McCallum
M.S.R.I., Berkeley, Ca 94721, USA

Introduction

Let p be an odd prime number and let a, b, and c be integers such that $0<a$, $b<p$ and $a+b+c=0$. Let $F_{a,b,c}$ be the complete nonsingular curve over $\mathbb{Q}$ with affine equation

$$y^p = x^a(1-x)^b. \tag{0.1}$$

$F_{a,b,c}$ is a quotient of the Fermat curve $x^p+y^p=1$ by a cyclic automorphism group of order p. Let $J_{a,b,c}$ be the jacobian of $F_{a,b,c}$. Then $J_{a,b,c}$ has potential complex multiplication by the ring of integers $\mathbb{Z}[\mu_p]$ in the cyclotomic field of p-th roots of unity $\mathbb{Q}(\mu_p)$; if ζ is a p-th root of unity the action of ζ on $J_{a,b,c}$ is induced by

$$y \mapsto \zeta y.$$

If K is a number field, we denote by $Ш(J_{a,b,c}, K)$ the Shafarevich-Tate group of $J_{a,b,c}$ over K. In this paper we find systematically occurring non-trivial elements in $Ш(J_{a,b,c}, \mathbb{Q}(\mu_p))$. For a rational number x let $q(x)=(x^{p-1}-1)/p$.

Theorem. *Suppose* $p \equiv 1 \pmod 4$, $p \nmid B_{(p-1)/2}B_{(p+3)/2}$, and $-2abcq(a^ab^bc^c)$ *is congruent to a non-zero square modulo p. Then* $Ш(J_{a,b,c}, \mathbb{Q}(\mu_p))$ *contains a subgroup isomorphic to* $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$.

Here B_i denotes the i-th Bernoulli number. The congruence condition in the hypothesis has a geometric interpretation in terms of the reduction type of the minimal model of $F_{a,b,c}$ over $\mathbb{Z}_p[\mu_p]$. We will recall this interpretation in §3. Heuristically about half the quotients of the Fermat curve satisfy the congruence condition.

The theorem is proved by calculating the restriction of the Cassels-Tate pairing on $Ш(J_{a,b,c}, \mathbb{Q}(\mu_p))$ to its $(1-\zeta)$-torsion subgroup. In fact we give a general formula for the pairing between the $(1-\zeta)$-torsion and the $(1-\zeta)^n$-torsion of $Ш(J_{a,b,c}, K)$, provided $n \leqq p-2$ and all $(1-\zeta)^{n+1}$-torsion points on $J_{a,b,c}$ are rational over K. We are able to apply this to the case $n=1$, $K=\mathbb{Q}(\mu_p)$, by

Current address: Department of Mathematics, University of Arizona, Tucson, AZ 85721, USA

virtue of a result of Greenberg [7] stating that all $(1-\zeta)^3$-torsion points on $J_{a,b,c}$ are rational over $\mathbb{Q}(\mu_p)$.

In order to apply this formula directly, it would be necessary to find a function f defined over K whose divisor is p times a divisor which represents a $(1-\zeta)^2$-torsion point on $J_{a,b,c}$. Such functions are hard to find explicitly. We are able to avoid doing this by finding a p-adic approximation to the function in §4. The technique for this p-adic approximation was inspired by ideas of Robert Coleman.

In §1 we show how to express the Cassels-Tate pairing as a sum of local pairings when a certain hypothesis is satisfied, and in §2 we give a formula for the local pairing in terms of functions evaluated on divisors. In §3 we recall various results on curves over discrete valuations rings and duality theory. In §4 we recall the necessary information on the geometry of a minimal model for $F_{a,b,c}$. In §5 we find the p-adic approximation. In §6 we compute the local pairing, and in §7 we deduce the main theorem.

The author would like to thank Robert Coleman for many useful discussions. An earlier version of this work formed the author's Ph.D. thesis, under the supervision of Barry Mazur, to whom the author owes a great debt of gratitude for his advice and support. The author would also like to thank the referee for many helpful suggestions and corrections.

§ 1. The Cassels-Tate pairing

Let A be an abelian variety over a number field K. Let M_K be a complete set of non-equivalent valuations of K. The Shafarevich-Tate group is defined by the exactness of

$$0 \to Ш(K, A) \to H^1(K, A) \to \prod_{v \in M_K} H^1(K_v, A),$$

where the cohomology groups are Galois cohomology groups. Let $\hat{A}$ be the dual abelian variety. The Cassels-Tate pairing is a pairing

$$\langle , \rangle : Ш(K, A) \times Ш(K, \hat{A}) \to \mathbb{Q}/\mathbb{Z}$$

which is non-degenerate modulo the divisible subgroup. It was defined by Cassels for elliptic curves and by Tate in general. We give Tate's definition in the special case needed here, as expounded in [17] I.6.9. Let ϕ, ψ be isogenies of A over K, and let $\hat{\phi}, \hat{\psi}$ be the dual isogenies of $\hat{A}$. Denote the induced endomorphisms of $Ш(K, A)$ and $Ш(K, \hat{A})$ by the same letters. If $f: G \to G'$ is a morphism denote its kernel by G_f. We will define the restriction of the Cassels-Tate pairing to the kernels of ϕ and $\hat{\psi}$:

$$\langle , \rangle : Ш(K, A)_\phi \times Ш(K, \hat{A})_{\hat{\psi}} \to \mathbb{Q}/\mathbb{Z}.$$

We will make use of various maps between cohomology groups, all coming from the cohomology of one of the following types of sequence:

$$0 \to A_\psi(\bar{K}) \to A_{\phi\psi}(\bar{K}) \xrightarrow{\psi} A_\phi(\bar{K}) \to 0$$

or

$$0 \to A_\phi(\bar{K}) \to A(\bar{K}) \xrightarrow{\phi} A(\bar{K}) \to 0.$$

If $*$ is a global cohomology class, cocycle, or cochain, we write $*_v$ for the corresponding local object. Let $a \in Ш(K, A)_\phi$ and $a' \in Ш(K, \hat{A})_{\hat{\psi}}$. Choose elements b and b' of $H^1(K, A_\phi)$ and $H^1(K, \hat{A}_{\hat{\psi}})$ mapping to a and a' respectively. For each v, a maps to zero in $H^1(K_v, A)$, and so it is obvious from the diagram

$$\begin{array}{ccccc} A(K_v) & \longrightarrow & H^1(K_v, A_\phi) & \longrightarrow & H^1(K_v, A) \\ \| & & \uparrow & & \\ A(K_v) & \longrightarrow & H^1(K_v, A_{\phi\psi}) & & \end{array}$$

that we can lift b_v to an element $b_{v,1} \in H^1(K_v, A_{\phi\psi})$ that is in the image of $A(K_v)$. Suppose that a is divisible by ψ in $H^1(K, A)$, say $a = \psi a_1$, and choose an element $b_1 \in H^1(K, A_{\phi\psi})$ mapping to a_1. Then $b_{v,1} - b_{1,v}$ maps to zero under $H^1(K_v, A_{\phi\psi}) \to H^1(K_v, A_\phi)$, and so it is the image of an element c_v in $H^1(K_v, A_\psi)$. Then

$$\langle a, a' \rangle = \sum_{v \in M_K} \mathrm{inv}_v(c_v \cup b'_v), \tag{1.1}$$

where the cup-product is induced by the Weil pairing

$$e_\psi : A_\psi \times \hat{A}_{\hat{\psi}} \to \mathbb{G}_m,$$

and inv_v is the canonical isomorphism $H^2(K_v, \mathbb{G}_m) \to \mathbb{Q}/\mathbb{Z}$ (see [4], Ch. VI, §1). For the definition when a does not lift to an a_1 we direct the reader to [17] I.6.9.

Now suppose the following hypothesis holds

$(H_{\phi,\psi})$ the map of Galois modules $\psi : A_{\phi\psi}(\bar{K}) \to A_\phi(\bar{K})$ has a section $s : A_\phi(\bar{K}) \to A_{\phi\psi}(\bar{K})$.

Then we can take $a_1 = s_* a$. Further, we can express the Cassels pairing as a sum of local pairings. Write $Ш = Ш(K, A)$, $Ш' = Ш(K, \hat{A})$, and let S_ϕ be the ϕ-Selmer group, i.e., $S_\phi \subseteq H^1(K, A_\phi)$ and

$$0 \to A(K)/\phi A(K) \to S_\phi \to Ш_\phi \to 0$$

is exact. Let $S_{\hat{\psi}}$ be the $\hat{\psi}$-Selmer group. Denote the lifting of the Cassels-Tate pairing to $S_\phi \times S_{\hat{\psi}}$ by $\langle\ ,\ \rangle$ also. Fix a valuation $v \in M_K$. By the definition of Ш the third vertical map in

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(K)/\phi A(K) & \longrightarrow & S_\phi & \longrightarrow & Ш & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A(K_v)/\phi A(K_v) & \longrightarrow & H^1(K_v, A_\phi) & \longrightarrow & H^1(K_v, A)_\phi & \longrightarrow & 0 \end{array}$$

is 0. Hence we get a map

$$l_{v,\phi}: S_\phi \to A(K_v)/\phi A(K_v).$$

We will define a pairing

$$\langle\ ,\ \rangle_v^{\phi,\psi}: A(K_v)/\phi A(K_v) \times \hat{A}(K_v)/\hat{\psi}\hat{A}(K_v) \to \mathbb{Q}/\mathbb{Z}$$

such that for $b \in S_\phi$ and $b' \in S'_{\hat{\psi}}$

$$\langle b, b' \rangle = \sum_{v \in M_K} \langle l_{v,\phi}(b), l_{v,\hat{\psi}}(b') \rangle_v^{\phi,\psi}.$$

Let $G = \mathrm{Gal}(\bar{K}/K)$. Denote the map $A(K_v)/\phi A(K_v) \to H^1(K_v, A_\phi)$ by ι_ϕ. Consider the diagram

$$\begin{array}{ccccc} & & & & A_\phi(K_v)/\psi A_{\phi\psi}(K_v) \\ & & & \swarrow & \downarrow \\ & & A(K_v)/\psi A(K_v) & \xrightarrow{\iota_\psi} & H^1(K_v, A_\psi) \\ & & \downarrow \phi & & \downarrow \\ 0 & \longrightarrow & A(K_v)/\phi\psi A(K_v) & \xrightarrow{\iota_{\phi\psi}} & H^1(K_v, A_{\phi\psi}) \\ & & \downarrow & & \downarrow \psi \\ 0 & \longrightarrow & A(K_v)/\phi A(K_v) & \xrightarrow{\iota_\phi} & H^1(K_v, A_\phi) \end{array}$$

Let $x \in A(K_v)/\phi A(K_v)$, $x' \in \hat{A}(K_v)/\hat{\psi}\hat{A}(K_v)$. Let x_1 be a lifting of x to $A(K_v)/\phi\psi A(K_v)$. Then $i_{\phi\psi}(x_1)$ and $s_* i_\phi(x)$ both have the same image in $H^1(K_v, A_\phi)$, hence $(i_{\phi\psi}(x_1) - s_* i_\phi(x))$ is the image of an element $c_v \in H^1(K_v, A_\psi)$. Define

$$\langle x, x' \rangle_v^{\phi,\psi} = \mathrm{inv}_v[c_v \cup i_{\hat{\psi}}(x')]. \tag{1.2}$$

(1.3) **Proposition.** *The map*

$$\langle\ ,\ \rangle_v^{\phi,\psi}: A(K_v)/\phi A(K_v) \times \hat{A}(K_v)/\hat{\psi}\hat{A}(K_v) \to \mathbb{Q}/\mathbb{Z}$$

is a bilinear pairing of abelian groups.

Proof. The pairing is well-defined, since if the lifting x_1 is modified by an element ϕt of $\phi A(K_v)/\phi\psi A(K_v)$, then the pairing changes by $i_\psi(t)\cup i_{\hat\psi}(x')$. It is well-known that the images of i_ψ and $i_{\hat\psi}$ annihilate each other (for lack of a precise reference, we prove this in Proposition 1.14 at the end of this section). Hence the pairing does not depend on the lifting. By a similar argument, the pairing does not depend on the choice of c_v and is linear in the first argument. It is obviously linear in the second. □

(1.4) **Theorem.** *The Cassels-Tate pairing on $S_\phi \times S'_{\hat\psi}$ may be expressed as a sum of local pairings*

$$\langle b, b'\rangle = \sum_{v\in M_K} \langle l_{v,\phi}(b), l_{v,\hat\psi}(b')\rangle_v^{\phi,\psi}.$$

Proof. It is clear that if $x = l_{v,\phi}(b)$ and $x' = l_{v,\hat\psi}(b')$, then $s_* i_\phi(x) = b_{1,v}$, $i_{\phi\psi}(x_1) = b_{v,1}$, and $i_{\hat\psi}(x') = b'_v$. Hence the c_v in (1.1) is the same as the c_v in (1.2). □

(1.5) **Lemma.** *If v is a complex archimedean valuation, or if v is non-archimedean, A has good reduction modulo the maximal ideal of v, and $v(\deg(\phi)\deg(\psi)) = 0$, then $\langle\ ,\ \rangle_v^{\phi,\psi}$ is trivial.*

Proof. The first statement is obvious, since in that case $\mathrm{inv}_v = 0$. Now suppose that v is non-archimedean. Under the hypotheses the cocycles in the definition of the pairing are unramified (see [14], Proposition 9). But unramified cocycles in $H^1(K_v, A_\psi)$ and $H^1(K_v, \hat A_{\hat\psi})$ pair trivially (see [17] I.2.6). □

Before proceeding further, we recall the definition and some properties of the Weil pairing. Let $a\in A_\phi$ and $a'\in \hat A_{\hat\phi}$ and let D be a divisor on $\hat A$ representing a. Let g be a function on $\hat A_{/K}$ with divisor $\hat\phi^{-1}D$. Then

$$e_\phi(a, a') = g(x + a')/g(x)$$

for any x for which the right hand side is defined.

The Weil pairing is skew symmetric,

$$e_\phi(a, a') = e_{\hat\phi}(a', a)^{-1} \quad \text{for all } a\in A_\phi,\ a'\in \hat A_{\hat\phi}. \tag{1.6}$$

If $a\in A_{\phi\psi}$ and $a'\in A_{\hat\phi}$ then

$$e_{\phi\psi}(a, a') = e_\phi(\psi a, a'), \tag{1.7}$$

and if $a\in A_\psi$ and $a'\in A_{\hat\psi\hat\phi}$ then

$$e_{\phi\psi}(a, a') = e_\psi(a, \hat\phi a'). \tag{1.8}$$

The latter two properties are immediate from the definition. Skew symmetry follows from the general duality theory of abelian varieties [19], §20.

The definition of $\langle\ ,\ \rangle_v^{\phi,\psi}$ depends on the choice of a section s, which may not be unique. However, once s has been chosen, there is a natural choice of section s': $\hat{A}_\psi(\bar{K}) \to \hat{A}_{\hat{\psi}\hat{\phi}}(\bar{K})$ for $\hat{\phi}$, namely, the one determined by the condition

$$e_{\phi\psi}(sa, s'a') = 0 \quad \text{for all } a \in A_\phi(\bar{K}),\ a' \in \hat{A}_{\hat{\psi}}(\bar{K}). \tag{1.9}$$

This is the choice we make in what follows. The following lemma is natural in view of the skew symmetry of the Cassels-Tate pairing.

(1.10) **Lemma.** *For all* $x \in A(K_v)/\phi A(K_v)$, $x' \in \hat{A}(K_v)/\hat{\psi}\hat{A}(K_v)$,

$$\langle x, x'\rangle_v^{\phi,\psi} = -\langle x', x\rangle_v^{\hat{\psi},\hat{\phi}}.$$

Proof. The skew symmetry of the Weil pairing (1.6) implies that the cup product pairing between $H^1(K, A_\phi)$ and $H^1(K, \hat{A}_{\hat{\phi}})$ is symmetric, i.e.,

$$a \cup a' = a' \cup a \quad \text{for all } a \in H^1(K_v, A_\phi) \quad \text{and} \quad a' \in H^1(K_v, \hat{A}_{\hat{\phi}}), \tag{1.11}$$

where the first cup is with respect to e_ϕ and the second with respect to $e_{\hat{\phi}}$. This follows from the general symmetry properties of the cup product (see [4], Ch, V, §7, Prop. 9(ii)). Now let $x \in A(K_v)/\phi A(K_v)$, $x' \in \hat{A}(K_v)/\hat{\psi}\hat{A}(K_v)$, and let x_1 and x_1' be liftings of x and x' to $A(K_v)/\phi\psi A(K_v)$ and $\hat{A}(K_v)/\hat{\psi}\hat{\phi}\hat{A}(K_v)$, respectively. Write

$$a = i_{\phi\psi}(x_1) - s_* i_\phi(x) \quad \text{and} \quad a' = i_{\hat{\psi}\hat{\phi}}(x_1') - s_*' i_{\hat{\psi}}(x').$$

Then a is the image of an element $c \in H^1(K_v, A_\psi)$, a' is the image of an element $c' \in H^1(K_v, \hat{A}_{\hat{\phi}})$, and by definition

$$\langle x, x'\rangle_v^{\phi,\psi} = c \cup i_{\hat{\psi}}(x') \quad \text{and} \quad \langle x', x\rangle_v^{\hat{\psi},\hat{\phi}} = c' \cup i_\phi(x). \tag{1.12}$$

By Proposition 1.14

$$\begin{aligned} 0 &= i_{\phi\psi}(x_1) \cup i_{\hat{\psi}\hat{\phi}}(x_1') \\ &= a \cup a' + a \cup s_*' i_{\hat{\psi}}(x') + s_* i_\phi(x) \cup a' + s_* i_\phi(x) \cup s_*' i_{\hat{\psi}}(x'). \end{aligned} \tag{1.13}$$

Now $s_* i_\phi(x) \cup s_*' i_{\hat{\psi}}(x') = 0$ by (1.9). From (1.7) and (1.8) it follows that $a \cup a' = 0 \cup c' = 0$, $s_* i_\phi(x) \cup a' = i_\phi(x) \cup c'$ and $a \cup s_*' i_{\hat{\psi}}(x') = c \cup i_{\hat{\psi}}(x')$. Hence (1.13) implies

$$c \cup i_{\hat{\psi}}(x') + i_\phi(x) \cup c' = 0.$$

The lemma now follows from (1.11) and (1.12). □

It remains to prove that the images of i_ϕ and $i_{\hat{\phi}}$ annihilate each other.

(1.14) **Proposition.** *Let ϕ be an isogeny of A. The images of the maps*

$$i_\phi\colon A(K_v)/\phi A(K_v) \to H^1(K_v, A_\phi) \quad \text{and} \quad i_{\hat{\phi}}\colon \hat{A}(K_v)/\hat{\phi}\hat{A}(K_v) \to H^1(K_v, \hat{A}_{\hat{\phi}})$$

annihilate each other under the cup product pairing

$$H^1(K_v, A_\phi) \times H^1(K_v, \hat{A}_{\hat{\phi}}) \to \mathbb{Q}/\mathbb{Z}.$$

Proof. Let $a=i_\phi(x)$ and $a'=i_{\hat\phi}(x')$. Then $a_\sigma=y^\sigma-y$ for some $y\in A(\bar K_v)$ such that $\phi y=x$, and $a'_\sigma=y'^\sigma-y'$ for some $y'\in A(\bar K_v)$ such that $\hat\phi y'=x'$. Let D be a divisor on $\hat A$ representing y and such that y'^σ and $\mathrm{supp}(D^\tau)$ never meet for $\sigma,\tau\in \mathrm{Gal}(\bar K/K)$, and let g_σ be a function with divisor $\hat\phi^{-1}(D^\sigma-D)$. Define a cochain b with values in $\bar K_v^*$ by

$$b_\sigma=g_\sigma(y'^\sigma).$$

By checking divisors we see that $g_{\sigma\tau}\equiv g_\sigma g_\tau^\sigma(\mathrm{mod}\,\bar K_v^*)$. Thus

$$\begin{aligned}(\delta b)_{\sigma,\tau}&=g_{\sigma\tau}(y'^{\sigma\tau})/g_\sigma(y'^\sigma)\,g_\tau(y'^\tau)^\sigma=g_\sigma((y'^{\sigma\tau})-(y'^\sigma))\\&=e_\phi(a_\sigma,a_\tau'^\sigma)=(a\cup a')_{\sigma,\tau}.\end{aligned}$$

Hence the cup product of a and a' is a coboundary, which is what we wanted to show. □

§ 2. A formula for the local pairing when $A_\psi\approx A_{\hat\psi}\approx\mathbb{Z}/m\mathbb{Z}$

In this section we will find a formula for the local pairing in terms of the Hilbert norm residue symbol of the values of certain functions. Until further notice, K is any field. If $f,g\in K(A)^*$ and H is a subgroup of $K(A)^*$, we say $f\equiv g(\mathrm{mod}\,H)$ if $f/g\in H$. Let ϕ be an isogeny of degree m. Suppose that there is a non-zero $P\in\hat A_{\hat\phi}\cap\hat A(K)$. Let D_P be a divisor on A over K which represents P and let $f_P\in K(F_{a,b,c})$ be a function satisfying

$$(f_P)=mD_P.$$

(2.1) **Lemma.** *Let $\mathfrak{a}$ be a zero-cycle of degree zero on A defined over K and not meeting the support of D_P.*

(i) *We have $f_P(\phi\mathfrak{a})\in K^{*m}$.*

(ii) *If $\Sigma\mathfrak{a}=0$ then $f_P(\mathfrak{a})\in K^{*m}$.*

(iii) *If D'_P is defined over K and linearly equivalent to D_P, and $f'_P\in K(A)$ is such that $(f'_P)=mD'_P$, then $f_P\equiv f'_P g^p(\mathrm{mod}\,K^*)$ for some $g\in K(A)$.*

Proof. (i) Let g be a function with divisor $\phi^{-1}D$. Then $f_P\circ\phi\equiv g^m(\mathrm{mod}\,K^*)$.

(ii) Since the divisor of f_P is divisible by m, this follows from Lang's reciprocity law [13].

(iii) Obvious. □

It follows from (i) and (ii) of Lemma 2.1 that by evaluating f_P on zero-cycles we get a well-defined map

$$\iota_P\colon A(K)/\phi A(K)\to K^*/K^{*m}.$$

It follows from (iii) that this map depends only on P, not on the divisor chosen to represent it. On the other hand, since P is rational over K, we have a Galois map

$$A_\phi\to\mu_m,\qquad a\mapsto e_\phi(a,P),$$

which induces a map

$$j_P: H^1(K, A_\phi) \to H^1(K, \mu_m) = K^*/K^{*m},$$

where the equality is the canonical map from Kummer theory. Recall the map $i_\phi: A(K)/\phi A(K) \to H^1(K, A_\phi)$ from the previous section.

(2.2) **Lemma.** *We have* $j_P \circ i_\phi = \iota_P$.

Proof. In what follows we identify $H^1(K, \mu_m)$ and K^*/K^{*m} via the canonical isomorphism from Kummer theory. Let $x \in A(K)/\phi A(K)$. Then $i_\phi(x)$ is represented by the galois cocycle $\sigma \mapsto a_\sigma = (\sigma - 1)y$, where $\phi y = x$, $y \in A(\bar{K})$, and $j_P \circ i_\phi(x)$ is represented by the cocycle $e_\phi(a_\sigma, P)$. On the other hand, $\iota_P(x)$ is represented by the cocycle $\sigma \mapsto t^{\sigma - 1}$, where $t^m = f_P(\mathfrak{a})$, for $\mathfrak{a}$ a zero-cycle of degree zero defined over K summing to x. Choose $\mathfrak{a} = (x) - (0)$, and choose D so that its support does not contain x, 0, or y. Let g be a function with divisor $\phi^{-1}D$. Then $f_P \circ \phi \equiv g^m \pmod{K^*}$. Hence we may choose $t = g((y) - (0))$. Then $t^{\sigma - 1} = g((\sigma y) - (y)) = g((y + a_\sigma) - (y)) = e_\phi(a_\sigma, P)$. □

Now let ϕ and ψ be isogenies satisfying $H_{\phi, \psi}$, and suppose further that

$$A_\psi \approx \mathbb{Z}/m\mathbb{Z} \quad \text{and} \quad \hat{A}_{\hat{\psi}} \approx \mathbb{Z}/m\mathbb{Z} \quad \text{for some } m \in \mathbb{Z}. \tag{2.3}$$

Let P and P' be generators of A_ψ and $A_{\hat{\psi}}$, respectively, and let $Q = s'P'$, where s' is the section dual to s, as in §1. Let K be a number field. Let v be a valuation of K, and let K_v be the completion of K at v. Let

$$\begin{aligned} (\ ,\ )_m: K_v^*/K_v^{*m} \times K_v^*/K_v^{*m} &\to \mu_m \\ (x, y) &\mapsto (x^{1/m})^{([\bar{y}, K_v] - 1)} \end{aligned}$$

be the Hilbert norm residue symbol. Here $\bar{y}$ is any element of K^* mapping to y, and $[\bar{y}, K_v]$ denotes the Artin symbol. If $\zeta, \zeta' \in \mu_m$, ζ a generator, let $\mathrm{Ind}_\zeta(\zeta')$ be the unique element u of $\frac{1}{m}\mathbb{Z}/\mathbb{Z}$ such that $\zeta^{mu} = \zeta'$. We have canonical isomorphisms

$$H^1(K_v, \mu_m) = K_v^*/K_v^{*m} \tag{2.4}$$

and

$$H^2(K_v, \mu_m \otimes \mu_m) = H^2(K_v, \mu_m) \otimes \mu_m = (m^{-1}\mathbb{Z}/\mathbb{Z}) \otimes \mu_m = \mu_m. \tag{2.5}$$

It follows easily from the discussion in [22] Ch. XIV, §2 that under the identifications (2.4) and (2.5), the Hilbert norm residue symbol may be identified with the cup product pairing

$$H^1(K_v, \mu_m) \times H^1(K_v, \mu_m) \to H^2(K_v, \mu_m \otimes \mu_m).$$

(2.6) **Theorem.** *Let* $x \in A(K_v)/\phi A(K_v)$, $y \in \hat{A}(K_v)/\hat{\psi}\hat{A}(K_v)$. *We have*

$$\langle x, y\rangle_v^{\phi,\psi} = \mathrm{Ind}_{e_\psi(P',P)}[(\iota_Q(x_1), \iota_P(y))_m],$$

where x_1 *is any lifting of* x *to* $A(K_v)/\phi\psi A(K_v)$.

For the proof we need a lemma.

(2.7) **Lemma.** *The following diagram commutes.*

$$\begin{array}{ccccc} \mathrm{cup}: H^1(K_v, A_\psi) & \times & H^1(K_v, \hat{A}_{\hat{\psi}}) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle j_{P'}} & & \downarrow{\scriptstyle j_P} & & \downarrow \\ \mathrm{Ind}_{e_\psi(P',P)} \circ (\ ,\ )_m: K_v^*/K_v^{*m} & \times & K_v^*/K_v^{*m} & \longrightarrow & \mathbb{Q}/\mathbb{Z} \end{array}$$

Proof. Let $\alpha \in H^1(K_v, A_\psi)$, $\beta \in H^1(K_v, \hat{A}_{\hat{\psi}})$ be represented by the cocycles $n_\sigma P$ and $m_\sigma P'$ respectively. Let $\varepsilon = e_{\hat{\psi}}(P', P)$. Then by (1.6), $e_\psi(P, P') = \varepsilon^{-1}$. Thus $\alpha \cup \beta$ is

$$e_\psi(n_\sigma P, m_\tau P') = \varepsilon^{-n_\sigma m_\tau}.$$

On the other hand, $j_{P'}(\alpha)$ and $j_P(\beta)$ are represented by the cocycles ε^{-n_σ} and ε^{m_σ} respectively, and pair via the Hilbert norm residue symbol to $(\varepsilon \otimes \varepsilon)^{-n_\sigma m_\tau}$. Thus we have a commutative diagram

$$\begin{array}{ccccc} \mathrm{cup}: H^1(K_v, A_\psi) & \times & H^1(K_v, \hat{A}_{\hat{\psi}}) & \longrightarrow & H^2(K_v, \mu_m) \\ \downarrow{\scriptstyle j_{P'}} & & \downarrow{\scriptstyle j_P} & & \downarrow{\scriptstyle \otimes\varepsilon} \\ (\ ,\ )_m: K_v^*/K_v^{*m} & \times & K_v^*/K_v^{*m} & \longrightarrow & H^2(K_v, \mu_m \otimes \mu_m). \end{array}$$

The theorem now follows from the fact that the composition of maps

$$\begin{aligned} m^{-1}\mathbb{Z}/\mathbb{Z} &\xrightarrow{\mathrm{inv}^{-1}} H^2(K_v, \mu_m) \xrightarrow{\otimes\varepsilon} H^2(K_v, \mu_m \otimes \mu_m) \to H^2(K_v, \mu_m) \otimes \mu_m \\ &\xrightarrow{\mathrm{inv}\otimes 1} m^{-1}\mathbb{Z}/\mathbb{Z} \otimes \mu_m \to \mu_m \end{aligned}$$

is simply $a \mapsto \varepsilon^{ma}$. □

Proof of Theorem (2.6). Let $x \in A(K_v)/\phi A(K_v)$, $x' \in \hat{A}(K_v)/\hat{\psi}\hat{A}(K_v)$. Let x_1 be a lifting of x to $A(K_v)/\phi\psi A(K_v)$. Then $(i_{\phi\psi}(x_1) - s_* i_\phi(x)) = (1 - s_*\psi_*)(i_{\phi\psi}(x_1))$. For any $d \in H^1(K_v, A_{\phi\psi})$, $(1 - s_*\psi_*)(d)$ is the image of an element $c \in H^1(K_v, A_\psi)$, and it follows from (1.8) and (1.9) that $j_{P'}(c) = j_Q(d)$. The theorem now follows from the Lemmas 2.2 and 2.7. □

Note that if A is the jacobian of a curve C, then the zero cycles in the definition of the maps ι_P and ι_Q may be taken to be divisors on C. Further,

in defining the functions f_P and f_Q, instead of taking divisors on $\hat{A}$ and A representing P and Q, we may take divisors on C, and let f_P and f_Q be functions on C. All this follows from the autoduality of the jacobian and the natural divisorial correspondence between C and J (see [18], Ch. VI, § 5).

Theorem 2.6 applies in the following case. Let A be the jacobian J of the curve $F_{a,b,c}$. Then J is canonically isomorphic to $\hat{J}$ and the involution $\phi \mapsto \hat{\phi}$ of $\mathrm{End}(J) = \mathbb{Z}[\mu_p]$ is that induced by $\zeta \mapsto \zeta^{-1}$. Choose a primitive p-th root of unity ζ, and let $\lambda = 1 - \zeta$. Then $\deg(\lambda) = p$. Let $Ш = Ш(K, J)$. Let $1 \leqq n \leqq p-2$ be an integer and let K be a number field such that the complex multiplication is defined over K and $J_{\lambda^{n+1}} \subseteq J(K)$. Then, since λ^{n+1} divides p and $\lambda/\hat{\lambda}$ is a unit in $Z[\zeta]$, $J_{\lambda^k} = J_{\hat{\lambda}^k} \approx (\mathbb{Z}/p\mathbb{Z})^k$ as a $\mathrm{Gal}(\bar{K}/K)$-module for $1 \leqq k \leqq n+1$. Hypothesis $H_{\lambda^n, \hat{\lambda}}$ is satisfied, since all the groups in the sequence

$$0 \to J_{\hat{\lambda}}(\bar{K}) \to J_{\lambda^n \hat{\lambda}}(\bar{K}) \to J_{\lambda^n}(\bar{K}) \to 0$$

are abelian groups of exponent p and with trivial $\mathrm{Gal}(\bar{K}/K)$-action. Further, (2.3) is satisfied, since the divisor $(0, 0) - \infty$ represents a non-trivial λ and $\hat{\lambda}$-torsion point on J. Thus we may apply Theorem 2.6 with $\phi = \lambda^n$, $\psi = \hat{\lambda}$. In this paper we will consider only the case $n = 1$. Since, by [7], $J[\lambda^2] \subseteq J(\mathbb{Q}(\mu_p))$, we may take K to be $\mathbb{Q}(\mu_p)$ in that case. If we choose P to be the λ-torsion point represented by the divisor $(0, 0) - \infty$ then $f_P = x$. Let Q be a λ^2-torsion point. The function $f = f_Q$ is difficult to find explicitly, and we will have to use an approximation method. First, we recall some facts about curves over discrete valuation rings.

§ 3. Curves over discrete valuation rings

Let R be a discrete valuation ring with field of fractions K and residue field k. Let π be a uniformiser for R. By a curve over a field F we mean a separated scheme of finite type over F and of dimension one. By a curve over R we mean a connected normal scheme C with a morphism $f: C \to R$ which is flat and of finite type over R, and whose fibres are curves. We let $C_\eta = C \times_R K$ and $C_0 = C \times_R k$, and call these the generic and special fibres of C, respectively. We sometimes say that C is a model for C_η. If f is proper, we say C is *complete*. If C is a regular scheme, we say C is a *regular curve*. It is proved in [15] 2.8 that a complete regular curve over R is projective over R. It follows from [10], III.9.10 that the arithmetic genus of C_η is equal to the arithmetic genus of C_0; we call this number the genus of C. Denote the set of closed points of a scheme S by $S^\dagger$. By the valuative criterion for properness, any $P \in C_\eta^\dagger$ can be extended to a divisor $\bar{P}$ on C; we let $P_0 = \bar{P} \cdot C_0$. The map $P \mapsto P_0$ is called the reduction map.

For Theorem 3.7 below we need to recall some facts about the relative dualizing sheaf on a curve over R. We do this in some detail, since although it is all in [11] and [21] in some form, we could not find a precise reference for the statements we wanted.

Let A be R, K, or k. If $f\colon Y\to A$ is a scheme of finite type over A we denote by $\Omega_{Y/A}$ the relative dualizing complex for Y over A; specifically, in the notation of [11]

$$\Omega_{Y/A}=f^!(A).$$

Let $j\colon C_\eta\hookrightarrow C$ and $i\colon C_0\hookrightarrow C$ be the immersions of the generic and special fibres.

(3.1) **Theorem.** *Let C be a regular curve over R. Then $\Omega_{C/R}$ is an invertible sheaf on C. Further, $\Omega_{C/R}|_{C_\eta}=\Omega_{C_\eta/K}$ and $\Omega_{C/R}|_{C_0}=\Omega_{C_0/k}$.*

Proof. This is in [11]; for the convenience of the reader, we provide a guided tour of the relevant sections. It is shown in [11] that $f^!$ takes dualizing complexes to dualizing complexes [V, 2.4 for finite morphisms, 8.3 for smooth morphisms, VI and VII in general]. Any regular local ring is a dualizing complex for itself [11], §9. Thus $f^!(R)$ is a dualizing complex for C. On the other hand, since all the local rings of C are regular, it follows from [11] V, Corollary 2.3 that $\mathcal{O}_C$ is a dualizing complex. The first statement of the theorem now follows from the fact that dualizing complexes are unique up to tensoring by an invertible sheaf [11] V, 3.1.

That $\Omega_{C/R}|_{C_\eta}=\Omega_{C_\eta/K}$ follows immediately from the fact that $j^!=j^*$ [11] III, §1–2 and $(fj)^!=j^!f^!$ [11] III, 8.7. To see $\Omega_{C/R}|_{C_0}=\Omega_{C_0/k}$, consider the diagram

$$\begin{array}{ccc} C_0 & \xrightarrow{i} & C \\ {\scriptstyle f_0}\downarrow & & \downarrow{\scriptstyle f} \\ k & \xrightarrow[i_0]{} & R \end{array}$$

Using $(fi)^!=i^!f^!$, we get $\Omega_{C_0/R}=i^!\Omega_{C/R}$. By [11] III, 7.3 and definition (b) after 1.3 of the same reference this means

$$\Omega_{C_0/R}=\Omega_{C/R}|_{C_0}\otimes(I/I^2)^{-1}, \tag{3.2}$$

where I is the sheaf of ideals on C_0. The same reference implies that $(i_0)^!(R)=k\otimes((\pi)/(\pi^2))^{-1}$. Going the other way around the diagram, we get

$$\Omega_{C_0/R}=(f_0)^!(i_0)^!(R)=(f_0)^!(k\otimes((\pi)/(\pi^2))^{-1})=\Omega_{C_0/k}\otimes f_0^*((\pi)/(\pi^2))^{-1}.$$

The last equality follows from the fact that f_0 is Gorenstein, since C is regular (cf. [11], Ch. III, remark at end of §1). But $f_0^*((\pi)/(\pi^2))=I/I^2$, since C_0 is the divisor of π. Hence $\Omega_{C_0/R}=\Omega_{C_0/k}\otimes(I/I^2)^{-1}$. Comparing this with (3.2) gives the result. □

To apply Theorem 3.1 we need to identify $\Omega_{C/k}$ in a concrete form. Let

$$i\colon C_{\mathrm{red}}\to C$$

be the closed immersion of C with its reduced induced subscheme structure. The duality theorem for finite morphisms [11] III, 6.7 implies that for a coherent sheaf $\mathscr{F}$ on C_{red}

$$\text{Hom}_{C_{\text{red}}}(\mathscr{F}, \Omega_{C_{\text{red}}/k}) = \text{Hom}_C(i_*\mathscr{F}, \Omega_{C/k}).$$

Taking $\mathscr{F} = \Omega_{C_{\text{red}}/k}$ we get a canonical map

$$i_*\Omega_{C_{\text{red}}/k} \to \Omega_{C/k} \tag{3.3}$$

which is injective since Hom is left exact and i_* is fully faithful.

Now suppose that C is reduced and let $n: C' \to C$ be the normalization of C. We define the sheaf of regular differentials Ω_C^{reg} on C as follows. If U is an open subset of C, then $\Omega_C^{\text{reg}}(U)$ is the set of rational Kahler differentials ω on U such that

$$\sum_{x \in n^{-1}(U')} \text{res}_x(n^*(f\omega)) = 0 \quad \text{for all } f \in \mathscr{O}_C(U). \tag{3.4}$$

For example, there is only a simple pole at an ordinary double point and the residues on each branch cancel. If C is smooth then the sheaf of regular differentials is just the sheaf of Kahler differentials Ω_C^1.

(3.5) **Theorem.** *Suppose C is reduced and Cohen-Macaulay. Then $\Omega_{C/k}$ is canonically isomorphic to Ω_C^{reg}.*

Proof. We remark that for a curve, Cohen-Macaulay is equivalent to having no embedded components. Since C is Cohen-Macaulay, the dualizing complex $\Omega_{C/k}$ is a flat sheaf (cf. [1] IV, 5.6; III, 5.22). Let Ω denote either $\Omega_{C/k}$ or Ω_C^{reg}. Then there is a residue map

$$\eta: H^1(C, \omega) \to k$$

such that the induced pairing

$$H^1(C, F) \times \text{Hom}(F, \omega) \to k$$

is non-degenerate for any coherent sheaf F. For $\Omega_{C/k}$ this is the duality theorem [11]; for Ω_C^{reg} it is proved in [21]. In particular, the residue map for $\Omega_{C/k}$ induces a map $\Omega_{C/k} \to \Omega_C^{\text{reg}}$, and vice versa, and these maps must be inverses. □

(3.6) **Lemma.** *Let C be a regular, complete curve over a discrete valuation ring R. Suppose that C has a section $s: R \to C$. Then $H^0(C, \Omega_{C/R})$ is a free R-module and $H^0(C, \Omega_{C/R}) \otimes K = H^0(C_\eta, \Omega_{C_\eta/K})$ and $H^0(C, \Omega_{C/R}) \otimes k = H^0(C_0, \Omega_{C_0/k})$.*

Proof. Since C is projective over R, it suffices by Grauert's theorem [10] III, 12.9 to show that $\dim H^i(C_\eta, \Omega_{C/R}|_{C_\eta}) = \dim H^i(C_0, \Omega_{C/R}|_{C_0})$ for $i = 0, 1$. Since C has a section, at least one of the components of C_0 has multiplicity 1. It follows from [20] 8.2.1 that $f: C \to R$ is cohomologically flat (see [20] 1.4) which implies that $\dim_K H^0(C_\eta, \mathscr{O}_{C_\eta}) = \dim_k H^0(C_0, \mathscr{O}_{C_0}) = 1$. Since f is flat, it follows from [9]

7.9.4 that $\chi(\mathcal{O}_{C_\eta})=\chi(\mathcal{O}_{C_0})$, hence $\dim_K H^1(C_\eta, \mathcal{O}_{C_\eta})=\dim_k H^1(C_0, \mathcal{O}_{C_0})$. By Theorem 3.1 and the duality theorem for curves over fields [1] VIII, §1,

$$\dim_K H^i(C_\eta, \Omega_{C/R}|_{C_\eta})=\dim_K H^{1-i}(C_\eta, \mathcal{O}_{C_\eta}),$$

and

$$\dim_k H^i(C_0, \Omega_{C/R}|_{C_0})=\dim_k H^{1-i}(C_0, \mathcal{O}_{C_\eta}), \quad i=0, 1. \quad \square$$

It follows that we may regard $H^0(C, \Omega_{C/R})$ as an R-submodule of $H^0(C_\eta, \Omega^1_{C_\eta})$. If $\omega \in H^0(C_\eta, \Omega^1_{C_\eta})$ lies in $H^0(C, \Omega_{C/R})$ and maps to

$$\omega \in H^0(C_0, \Omega_{C_0/k})=H^0(C, \Omega_{C/R})\otimes k,$$

we say that ω reduces to ω_0.

(3.7) **Theorem.** *Let C be a regular, complete curve over a discrete valuation ring R. Let ω_0 be a regular differential on $C_{0,\mathrm{red}}$. Then there is a holomorphic differential ω on C_η that reduces to ω_0.*

Proof. Follows immediately from Theorem 3.5, Lemma 3.6, and the inclusion (3.3). $\square$

Let C be a complete, regular curve over R, and let $\mathcal{I}$ be the set of irreducible components of C_0, with their reduced induced subscheme structure. We refer the reader to [15] for the following basic facts. An irreducible (Weil) divisor on C is on of two types:

(i) horizontal, i.e., the image of a morphism $\mathrm{spec}(R')\to C$ for some finite extension R' of R

(ii) vertical, i.e., an element of $\mathcal{I}$.

A linear combination of horizontal (vertical) divisors will be called horizontal (vertical). Any divisor D on C can be written uniquely in the form D_h+D_v, where D_h is horizontal and D_v is vertical. Since C is regular, every invertible sheaf $\mathcal{L}$ is isomorphic to $\mathcal{O}(D)$ for some divisor D. We have $\deg(\mathcal{L}|_{C_\eta})=\deg(D\cap C_\eta)$ and $\deg(\mathcal{L}|_{C_0})=\deg(D\cdot C_0)$. Here $\cdot$ denotes the intersection product. Since $X\cdot C_0=0$ for all $X\in\mathcal{I}$, the two degrees are the same; we call their common value the degree of $\mathcal{L}$.

(3.8) **Proposition.** *Let C be a regular complete curve over R, of genus g, and let $\mathcal{L}$ be an invertible sheaf on C. Suppose that $\deg(\mathcal{L})>2g-2$. Then $H^0(C, \mathcal{L})$ is a free R-module of rank $\deg(\mathcal{L})-g+1$. Further,*

$$H^0(C, \mathcal{L})\otimes_R K=H^0(C_\eta, \mathcal{L}_\eta) \quad \textit{and} \quad H^0(C, \mathcal{L})\otimes_R k=H^0(C_0, \mathcal{L}_0).$$

Proof. By the Riemann-Roch theorem for curves over a field ([1] VIII, §1) $H^1(C_\eta, \mathcal{L}_\eta)=0$ and $H^1(C_0, \mathcal{L}_0)=0$, and $\dim_k H^0(C_0, \mathcal{L}_0)=\dim_K H^0(C_\eta, \mathcal{L}_\eta)=\deg(\mathcal{L})-g+1$. The proposition now follows from Grauert's theorem [10] III, 12.9. $\square$

If S is a set of closed points of C_η we denote by S_0 the image of S under the reduction map.

(3.9) **Lemma.** *Let C be a regular complete curve over R. Let S be a finite set of closed points of C_η. Let D be a divisor on C, and let E be an effective horizontal divisor whose support does not meet $\bar{P}$ for $P \in S$. Then for large enough n there is a function f such that*

$$(f)+nE \geqq D \quad \text{and} \quad f(P)=1 \quad \text{for all } P \in S.$$

Proof. Choose n such that the invertible sheaf associated with the divisor

$$F = nE - D - \sum_{P \in S} \bar{P}$$

satisfies the conditions of Proposition 3.8. Let $P \in S$, and let $F' = F + \bar{P}$. Then $\mathscr{L}_{F'}$ also satisfies the conditions of Proposition 3.8, and $\deg(\mathscr{L}^{F'}) = \deg(\mathscr{L}_F)+1$, so there is a function $f_P \in H^0(C, \mathscr{L}^{F'})$ but not in $H^0(C, \mathscr{L}_F)$. Hence

$$(f_P)+nE \geqq D, \quad f_P(P')=0 \quad \text{for all } P' \neq P \in S, \quad \text{and} \quad f_P(P) \neq 0.$$

Multiplying by a suitable constant we may assume that $f_P(P)=1$. Then

$$f = \sum_{P \in S} f_P$$

is the function we seek. □

§ 4. The local geometry of $F_{a,b,c}$

In this section we recall from [16] some facts about the minimal regular model for $F_{a,b,c}$ over the ring of integers in $\mathbb{Q}_p(\zeta_p)$, where ζ_p is a primitive p-th root of unity. This model is one of three types, according to what its special fibre looks like:

(i) Wild type

(a) Split

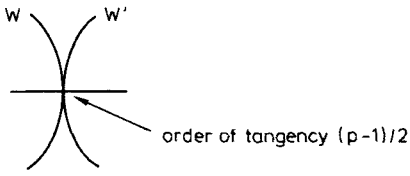

Fig. 1. All components are curves of genus zero defined over $\mathbb{F}_p$ and have multiplicity 1

(b) Non-split.

Same picture as for the split type, except that the two tangent curves are not individually defined over $\mathbb{F}_p$, but are conjugate over the unique quadratic extension of $\mathbb{F}_p$.

(ii) Tame type

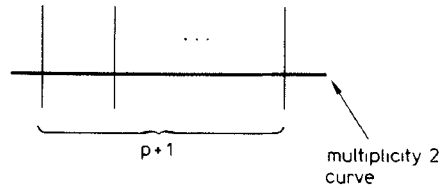

Fig. 2. All components are curves of genus zero defined over $\mathbb{F}_p$. All vertical components have multiplicity 1

The types are distinguished as follows. Recall that for a rational number x

$$q(x)=(x^{p-1}-1)/p.$$

Then $F_{a,b,c}$ is

tame	if $q(a^a b^b c^c)\equiv 0 \pmod p$	
wild split	if $q(a^a b^b c^c)\not\equiv 0 \pmod p$,	$-2abcq(a^a b^b c^c)\in \mathbb{F}_p^{*2}$
wild non-split	if $q(a^a b^b c^c)\not\equiv 0 \pmod p$,	$-2abcq(a^a b^b c^c)\notin \mathbb{F}_p^{*2}$.

§ 5. Approximation of f in the wild split case

We now return to the situation discussed at the end of §2. Thus $\phi=\lambda$, $\psi=\hat{\lambda}$, $K=\mathbb{Q}(\mu_p)$, $P=P'$ is the point on J corresponding to the divisor $(0,0)-\infty$, $f_P=x$, and Q is a λ^2-torsion point such that $\hat{\lambda}Q=P$. There is only one valuation v such that $v(p)\neq 0$. By Lemma 1.5, this is the only valuation such that $\langle\ ,\ \rangle_v^{\lambda,\hat{\lambda}}$ is non-trivial, since K is totally complex, $F_{a,b,c}$ has good reduction outside v and $\deg(\lambda)=\deg(\hat{\lambda})=p$. In order to apply the formula for the local pairing in the wild split case we need to approximate the function f on $F_{a,b,c}$ whose divisor is p times a divisor representing Q. To carry out this approximation we need to know the structure of certain affinoids contained in $F_{a,b,c}$. So assume that $F_{a,b,c}$ is wild split and denote it simply by F. We refer the reader to [3] for general facts about rigid analysis.

The closed unit disk, $\{x\in\bar{K}: |x|\leqq 1\}$, has a natural affinoid structure defined over K. The open unit disk, $\{x\in\bar{K}: |x|<1\}$, has a natural structure of rigid analytic space defined over K. By a closed (resp. open) disc over R we mean an affinoid (resp. rigid analytic space) conformal to the closed (resp. open) unit disc in R; by a parameter on a closed (resp. open) disc we mean an isomorphism from it to the closed (resp. open) unit disc. Let C be a curve over a complete discrete valuation ring R. For any subscheme $S\subseteq C_0$, the subset $\mathrm{red}^{-1}(S^\dagger)$ of $C_\eta^\dagger$ has a natural structure of rigid analytic space, which we denote by $\bar{S}$. If S is a Zariski open affine subset we call $\bar{S}$ a *Zariski open affinoid* in C_η. If $S=\{P\}$ where P is a closed point of C_0 then we call $\bar{S}$ the residue class of P.

If V is a K-vector space, then a *lattice* in V is an R-submodule V^0 such that $V^0\otimes_R K=V$. If X is an affinoid over K, let $A(X)$ be the ring of rigid

analytic functions on X, let $M(X)$ be the quotient field of $A(X)$, and let $D(X)$ be the module of Kahler differentials of $M(X)$. Define lattices

$$A^0(X)=\{f\in A(X): |f(x)|\leqq 1 \quad \text{for all} \quad x\in X\},$$
$$M^0(X)=\{f/g: f\in A^0(X),\ g\in A^0(X)-\pi A^0(X)\},$$

and

$$D^0(X)=\{\sum f_i dg_i: f_i,\ g_i\in M^0(X)\}.$$

If $f, g\in M(X)$, $\omega, \eta\in D(X)$, and $h\in A^0(X)$, we say $f\equiv g(\mathrm{mod}_X h)$ if $f-g\in hM^0(X)$, and we say $\omega\equiv\eta(\mathrm{mod}_X h)$ if $\omega-\eta\in hD^0(X)$. We will also write these congruences $f=g+O(h)$ and $\omega=\eta+O(h)$. If P is a closed point in C_η and ω is a differential on C then we define $\mathrm{res}_P(\omega)$ to be the residue of $\omega|_{C_\eta}$ at P. We denote by ω_0 be the restriction of ω to C_0, and by $n: C_0'\to C_0$ the normalization of the reduced subscheme of C_0. Let $(\omega)_\infty$ denote the polar divisor of ω, i.e., smallest divisor such that $(\omega)+(\omega)_\infty\geqq 0$, and let $(\omega)_{\infty,v}$ denote the vertical part of the polar divisor.

(5.1) **Theorem.** *Let C be a curve over R with a section s: $\mathrm{spec}(R)\to C$. Let ω be a rational differential on C. Let P_0 be a closed point at which C is regular which does not meet the support of $(\omega)_{\infty,v}$. Let Z be the residue class of P_0. Then*

$$\sum_{Q\in Z}\mathrm{res}_Q(\omega)\equiv\sum_{Q_0\in n^{-1}(P_0)}\mathrm{res}_{Q_0}(\omega_0)\quad(\mathrm{mod}\,\pi).$$

Proof. Step 1. We may suppose that C is regular. For if not, we may, by blowing up, obtain a regular curve C' and a morphism f: $C'\to C$ which is an isomorphism on a neighbourhood of P_0 [15]. Replace C by C' and ω by $f^*\omega$.

Step 2. We may suppose that $(\omega)_{\infty,v}=0$. Let X be the union of all irreducible components of C_0 containing P_0. Let $S=\{\text{poles of } \omega \text{ in } Z\}$, $D=(\omega)_{\infty,v}$, and $E=\bar{U}$, where $U\notin Z$. Choose f as in Lemma 3.9. Then $(f\omega)_{\infty,v}=0$ and $\mathrm{res}_P(f\omega)=\mathrm{res}_P(\omega)$ for all $P\in Z$. Further, $f(P_0)=1$ since f has no poles in Z and takes the value 1 at points of S_0. Hence $\mathrm{res}_{Q_0}((f\omega)_0)=\mathrm{res}_{Q_0}((\omega)_0)$ for all $Q_0\in n^{-1}(P_0)$. Thus it suffices to prove the theorem for $f\omega$.

Step 3. Suppose that C_0 is smooth at P_0. In that case Z is conformal to an open disc [2] 2.2. There exists a rigid analytic function t on a Zariski open affinoid neighbourhood of Z which restricts to a parameter on Z and which reduces to a uniformiser at P_0. Then ω has a formal Laurent expansion in t, and the coefficient a_{-1} of t^{-1} in this expansion reduces to the residue of ω_0 at P_0. The formula now follows from [6] I.3.3, which states that the sum of the residues of ω in Z is equal to a_{-1}. In fact it is proved there only for closed discs, but may be deduced here by choosing a large enough closed disc in Z; a_{-1} does not change when t is multiplied by a constant.

Step 4. If C_0 is not smooth at P_0, choose a point U not in Z at which ω does not have a pole, and such that C_0 is smooth at U_0. Indeed, there exists at least one component X of C_0 which is reduced, namely the component through which the section s passes. Any smooth point on $X-\{P_0\}$ not in the

support of $(\omega)_\infty$ will do. Choose a rational function f on C satisfying the conclusion of Lemma 3.9 with $S=(\omega)_\infty \cap Z$, $E=(U)$, and $D=(\omega)_\infty \cap (C-Z)$. Then the only poles of $f\omega$ are in Z and at U. By the same argument as in Step 2, $\mathrm{res}_P(f\omega) = \mathrm{res}_P(\omega)$ for all $P \in Z$ and $\mathrm{res}_{Q_0}((f\omega)_0) = \mathrm{res}_{Q_0}((\omega)_0)$ for all $Q_0 \in n^{-1}(P_0)$. We have already proven in Step 3 that $\mathrm{res}_U(f\omega) \equiv \mathrm{res}_{U_0}(f_0\omega_0) \pmod{\pi}$. The formula now follows from the fact that the sum of the residues of a differential on C_η or $n^{-1}(C_0)$ is zero. □

(5.2) **Theorem.** *Let C_η be a curve over K, and let Y be a Zariski open affinoid in C_η with reduced reduction. Let f be a function on C_η whose divisor is divisible by p. Then there exists a holomorphic differential ω on C such that $df/f|_Y \equiv \omega|_Y \pmod{_Y p}$.*

Proof. Choose a model C for C_η such that $Y=\bar{X}$ for some Zariski open affine X in C_0 and such that C_0 is reduced. (For example, start with any model such that $Y=\bar{X}$ for some Zariski open affine X in C_0, blow it up to become regular, choose a horizontal divisor D that is very ample on the generic fibre, very ample on each component of C_0 contained in the completion of X, and of negative degree on each other component, and take image of the corresponding map to projective space.) Then π has multiplicity one along each irreducible component of the special fibre; hence on each component, there is some $c=\pi^n$ such that cf is neither identically zero nor identically infinity on that component. Thus since $d(cf)/cf = df/f$, df/f is defined on each component. All its residues are multiples of p, hence by Theorem 5.1 its reduction is a regular differential, so by Theorem 3.7 there is a holomorphic differential ω_1 whose reduction is the same as that of df/f. Hence $(df/f-\omega_1)$ vanishes on C_0, and so $\eta_1 = (df/f-\omega_1)/\pi$ is defined on each component. In particular its restriction to Y is in $D^0(Y)$. If p/π is a unit we are finished. Otherwise let e be the ramification index of π. Since all the residues of η_1 are multiples of π^{e-1}, there is a holomorphic differential ω_2 whose reduction is the same η_1. Let $\eta_2=(\eta_1-\omega_2)/\pi$ and repeat the argument above. Continuing in this way we construct η_i and ω_i for $i=1, \ldots, e$ such that $\eta_i|_X \in D^0(X)$, ω_i is holomorphic,

$$df/f = \omega_1 + \pi\eta_1$$
$$\eta_i = \omega_{i+1} + \pi\eta_{i+1}, \qquad i=1, \ldots, e-1.$$

Thus $df/f = \omega_1 + \pi\omega_2 + \ldots + \pi^{e-1}\omega_e + \pi^e\eta_e$. □

Let W and W' be the two mutually tangent components of F_0 (see Fig. 1), and let $W^0 = W - W \cap W'$, $W'^0 = W' - W \cap W$. Let

$$X = \overline{W^0} \quad \text{and} \quad X' = \overline{W'^0}.$$

Set

(5.3) $$x = -a/c(1+\pi^{(p-1)/2}s)$$

(5.4) $$y = a^a b^b c^c (1+\pi t).$$

(5.5) **Lemma.** *X and X' are isomorphic to closed discs. The function t restricts to a parameter on each of them.*

Proof. It is shown in [16] that on the model for $F_{a,b,c}$ defined by the equation (0.1), the point on the closed fibre defined by the ideal $(\pi, x+a/c,\ y-a^a b^b c^c)$ is a non-regular point which blows up to give the two components W and W'. It is also shown that $P \in X(K) \cup X'(K) \Leftrightarrow x(P) \equiv -a/c \pmod{\pi}$, and that then in fact $x(P) \equiv -a/c \pmod{\pi^{(p-1)/2}}$ and $y(P) \equiv f(-a/c) \equiv a^a b^b c^c \pmod{\pi}$. Thus $X(K) \cup X'(K) = \{P \in F_\eta(K): |t(P)| \leqq 1, |s(P)| \leqq 1\}$. Substituting (5.3) and (5.4) into (0.1) we obtain

$$(a^a b^b c^c)^{p-1}(1+\pi t)^p = (1+\pi^{(p-1)/2}s)^a\left(1-\frac{a}{b}\pi^{(p-1)/2}s\right)^b.$$

Expanding both sides gives

$$(1+pq(a^a b^b c^c))(1-p\pi(t^p-t)+O(p\pi^2)) = 1-\frac{ac}{2b}ps^2+O(p\pi^{(p-1)/2}),$$

hence

$$s^2 = \frac{-q(a^a b^b c^c)\,2b}{ac} + \frac{\pi 2b}{ac}(t^p-t)+O(\pi^2). \tag{5.6}$$

It follows from [16] that the two square roots of the right hand side of this equation separate X from X'. Thus

$$X = \{P: |t(P)| \leqq 1 \quad \text{and} \quad |s(P)-\alpha| \leqq \pi\},$$

where α is one of the square roots of $\dfrac{-q(a^a b^b c^c)\,2b}{ac}$. It follows that $A(X) = K\{\{u, t\}\}$ (cf. [6] III.1), where $u=(s-\alpha)/\pi$. From (5.6) we have $u(2\alpha+\pi u) \in tR\{\{t\}\}$, hence $u \in R\{\{t\}\}$, so $A(X) = K\{\{t\}\}$. This proves the lemma for X. The proof for X' is the same, replacing α with $-\alpha$. □

Now choose $\Pi \in \mathfrak{O}_p$ satisfying $\Pi^p = \pi$ and let $S = R[\Pi]$. Let L be the field of fractions of S. Then the substitution

$$t = u/\Pi \tag{5.7}$$

transforms (5.6) into

$$s^2 = -\frac{2b}{ac}q(a^a b^b c^c) + \frac{2b}{ac}(u^p - \Pi^{p-1}u) + O(\pi\Pi). \tag{5.8}$$

The error term is $O(\pi\Pi)$ because the highest power of t in the $O(\pi^2)$ error term of (5.6) is t^{p-1}. Let $Y = \{P \in F_\eta \times_K L: |s(P)| \leqq 1, |u(P)| \leqq 1\}$. Then Y is a Zariski open affinoid in $F_\eta \times_K L$. Indeed, the completion of the affine scheme over R defined by (5.8) is a model for $F_\eta \times_K L$, and its special fibre contains the reduction of Y as a Zariski open subset. The reduction of Y is just the affine scheme over k defined by (5.8) mod π; in particular, it is reduced, so we may apply

Theorem 5.2. Let $X_L = X \times_K L$, $X'_L = X' \times_K L$. Then it is clear from the defining equations that

$$Y \supseteq X_L \cup X'_L. \tag{5.9}$$

We are now ready to find the approximation for f. We will find two properties of f that are sufficient to approximate it on Y.

(5.10) **Proposition.** *The function f satisfies the following:*

(i) $f/f \circ \zeta \equiv x \pmod{K(F_{a,b,c})^{*p}}$.

(ii) *There is a holomorphic differential ω on $F_{a,b,c}$* such that $df/f \equiv \omega \pmod{_Y p}$.

Proof. Let D be a divisor representing Q. Then, since $\hat{\lambda}Q = P$, $(1-\zeta^{-1})D$ is linearly equivalent to $(0,0)-\infty$. Let g be a function with divisor $(0,0)-\infty-(1-\zeta^{-1})D$. Then $(f/f\circ\zeta) = p(1-\zeta^{-1})D = (x)-p(g)$. Thus $f/f\circ\zeta = cx/g^p$ for some constant c. Evaluating at the point $(1,0)$, which is fixed by ζ, we see that $c \in K^{*p}$. This proves (i). Property (ii) follows immediately from Theorem 5.2. □

To apply this proposition we need to know the holomorphic differentials on $F_{a,b,c}$. If $z \in \mathbb{Q}$, let $[z]$ denote the integer part of z. Let

$$H_{a,b,c} = \left\{k: 1 \leqq k \leqq p-1, \left[\frac{ka}{p}\right] + \left[\frac{kb}{p}\right] + \left[\frac{kc}{p}\right] = -2\right\}.$$

For $k \in H_{a,b,c}$, let

$$\omega_k = \frac{X^{\left[\frac{ka}{p}\right]}(1-X)^{\left[\frac{kb}{p}\right]}}{Y^k}\,dX. \tag{5.11}$$

Lemma. *The set $\{\omega_k: k \in H_{a,b,c}\}$ is a basis for $H^0(F_{a,b,c}, \Omega^1)$. Also $\omega_k \circ \zeta = \zeta^{-k}\omega_k$.*

Proof. The second statement is obvious from the definitions. First we show that ω_k is holomorphic if $k \in H_{a,b,c}$. The only possible poles are at $(0,0)$, $(1,0)$, and ∞. If $m \in \mathbb{Z}$, let $r(m)$ denote the unique integer such that $0 \leqq r(m) \leqq p-1$ and $m \equiv r(m) \pmod{p}$. Note that $m - p[m/p] = r(m)$. The following table gives the orders of x, $1-x$, y and dx at these points.

Order at	$(0,0)$	$(1,0)$	∞
x	p	0	$-p$
$1-x$	0	p	$-p$
y	a	b	c
dx	$p-1$	$p-1$	$-p-1$

Thus

$$\mathrm{ord}_{(0,0)}(\omega_k)=p-1-r(ka)\geqq 0, \qquad \mathrm{ord}_{(0,1)}(\omega_k)=p-1-r(kb)\geqq 0,$$

and

$$\mathrm{ord}_{\infty}(\omega_k)=-p\left(\left[\frac{ka}{p}\right]+\left[\frac{kb}{p}\right]+\left[\frac{kc}{p}\right]\right)-p-1-r(kc).$$

Now $\left[\frac{ka}{p}\right]+\left[\frac{kb}{p}\right]+\left[\frac{kc}{p}\right]$ is -1 or -2, so $\mathrm{ord}_{\infty}(\omega_k)$ is non-negative if and only if the latter possibility occurs. Thus ω_k is holomorphic if $k\in H_{a,b,c}$. Now it is not hard to see that $H_{a,b,c} \pmod p$ is a set of representatives for $\mathbb{F}_p^*$ modulo $\langle \pm 1\rangle$. Thus

$$\# H_{a,b,c}=(p-1)/2=g(F_{a,b,c})=\dim_K H^0(F_{a,b,c}, \Omega^1).$$

Hence we need only show that the ω_k are linearly independent. This follows from the fact that they all have different eigenvalues for the action of ζ. □

By Lemma 5.5 X is isomorphic to the closed unit disc over K, and t is a parameter. Thus, since (f) is divisible by p, there is a rational function $g(t)$ on X such that $f|_X/g(t)^p$ has no poles or zeroes on X. Hence $f|_X/g(t)^p$ is an element of K^* times an element of $1+\pi tR\{\{t\}\}$. Write this element in the form $u(t)\,v(t^p)$ for some $u(t)$, $v(t)\in 1+\pi tR\{\{t\}\}$, such that the coefficient of t^k in $u(t)$ is zero whenever $p|k$. Thus we have

$$f|_X=C\,u(t)\,v(t^p)\,g(t)^p, \tag{5.12}$$

where $C\in K^*$, $g(t)\in K(t)$, $u(t)$ and $v(t)\in 1+\pi R\{\{t\}\}$. The following theorem is the key theorem in this paper. The rest of this section is devoted to its proof.

(5.13) **Theorem.** *The power series $u(t)$ in* (5.12) *satisfies*

$$u(t)=1+\pi^{(p-1)/2}\,Dt+O(\pi^{(p+1)/2}\,t), \qquad D\in R^*.$$

Proof. Since u has no p-th powers in its expansion, this is equivalent to showing that

$$\frac{du}{u}\equiv \pi^{(p-1)/2}\,D\,dt \qquad (\mathrm{mod}_X\,\pi^{(p+1)/2}),$$

for some $D\in R^*$. Now

$$\frac{df}{f}=p\,\frac{dg}{g}+p\,\frac{t^{p-1}\,v'(t^p)}{v(t)}\,dt+\frac{du}{u}\equiv\frac{du}{u} \qquad (\mathrm{mod}_X\,p),$$

so it suffices to show that

$$\frac{df}{f}\equiv \pi^{(p-1)/2}\,D\,dt \qquad (\mathrm{mod}_X\,\pi^{(p+1)/2}). \tag{5.14}$$

In fact we will show that

$$\frac{df}{f} \equiv \pi^{(p-1)/2} D' \frac{dt}{s} \quad (\mathrm{mod}_Y\, \pi^{(p-1)/2} \Pi), \tag{5.15}$$

for some $D' \in S^*$. Because of (5.9) this congruence will then also hold $\mathrm{mod}_X\, \pi^{(p-1)/2} \Pi$ (see note added in proof). Then choosing $D'' \in R^*$ such that $D'' \equiv D' \pmod{\Pi}$ (which is possible because S is totally ramified over R) we get

$$\frac{df}{f} \equiv \pi^{(p-1)/2} D'' \frac{dt}{s} \quad (\mathrm{mod}_Y\, \pi^{(p-1)/2} \Pi).$$

Since both sides of this congruence are in $A(X)$, it is a congruence $\mathrm{mod}_X\, \pi^{(p+1)/2}$. Finally, it follows from (5.6) that $s \equiv D'''$ $(\mathrm{mod}_X \pi)$ for some $D''' \in R^*$. Setting $D = D''/D'''$, we get (5.14).

By Theorem 5.2, there exist $a_k \in L$ such that

$$\frac{df}{f} \equiv \sum_{k \in H_{a,b,c}} a_k \omega_k \quad (\mathrm{mod}_Y\, p).$$

From (5.11), (5.3), and (5.4) we have

$$\omega_k \equiv \pi^{(p-1)/2} \frac{E_k\, ds}{(1+\pi t)^k} \quad (\mathrm{mod}_Y\, p),$$

for some $E_k \in R$. (Note: although $t \notin A^0(Y)$, it follows from (5.7) that $\Pi t \in A^0(Y)$.) Thus

$$\frac{df}{f} \equiv \pi^{(p-1)/2} \sum_{k \in H_{a,b,c}} \frac{a_k E_k\, ds}{(1+\pi t)^k} \quad (\mathrm{mod}_Y\, p). \tag{5.16}$$

From (5.7) and (5.8) it follows that

$$ds \equiv -\pi \frac{b}{ac} \frac{dt}{s} \quad (\mathrm{mod}_Y\, \pi \Pi).$$

Thus to deduce (5.15) from (5.16) it suffices to show that

$$\pi E_k a_k \in S \quad \text{for } k \in H_{a,b,c} \quad \text{and} \quad \pi \sum_{k \in H_{a,b,c}} a_k E_k \in S^*. \tag{5.17}$$

Using Proposition 5.10(i), (5.16), and the fact that $\omega_k \circ \zeta = \zeta^{-k}\omega_k$, we have

$$\frac{dX}{X} \equiv \pi^{(p-1)/2} \sum_{k \in H_{a,b,c}} \frac{b_k E_k}{(1+\pi t)^k} ds \quad (\mathrm{mod}_Y\, p), \tag{5.18}$$

where $b_k = (1-\zeta^{-k})\, a_k$. Since $\pi/(1-\zeta^{-k}) \equiv -1/k \pmod{\pi}$, we have $\pi a_k/b_k \equiv -1/k \pmod{\pi}$. Thus to show (5.17) it suffices to show

$$E_k b_k \in S \quad \text{for } k \in H_{a,b,c} \quad \text{and} \quad \sum_{k \in H_{a,b,c}} \frac{b_k E_k}{k} \in S^*. \tag{5.19}$$

Now from (5.3),

$$dX/X \equiv \pi^{(p-1)/2} F\, ds \quad (\mathrm{mod}_Y\, p)$$

for some $F \in R^*$. Thus (5.18) implies

$$\pi^{(p-1)/2} F\, ds \equiv \pi^{(p-1)/2} \sum_{k \in H_{a,b,c}} \frac{b_k E_k}{(1+\pi t)^k} ds \quad (\mathrm{mod}_Y\, p).$$

Now from (5.8), $ds \equiv 0 \ (\mathrm{mod}_Y \Pi^{p-1})$ and $ds \not\equiv 0 \ (\mathrm{mod}_Y \Pi^p)$. Thus, dividing both sides by $\pi^{(p-1)/2} ds$ we get

$$\sum_{k \in H_{a,b,c}} \frac{b_k E_k}{(1+\pi t)^k} \equiv F \quad (\mathrm{mod}_Y\, \Pi \pi^{(p-3)/2}).$$

It is to achieve this congruence that we introduced the affinoid Y. Working with X alone, one can only show that this congruence holds $\mathrm{mod}_X\, \pi^{(p-3)/2}$, which is not strong enough. Expanding and setting the coefficients of 1, $\pi t, \ldots, (\pi t)^{(p-3)/2}$ congruent mod Π, we obtain

$$\sum_{k \in H_{a,b,c}} b_k E_k \binom{-k}{i} \equiv \begin{cases} F & \text{if } i = 0 \\ 0 & \text{if } 1 \leqq i \leqq (p-3)/2 \end{cases} \pmod{\Pi}.$$

Expanding the binomial coefficients in powers of k we find inductively that

$$\sum_{k \in H_{a,b,c}} b_k E_k k^i \equiv \begin{cases} F & \text{if } i = 0 \\ 0 & \text{if } 1 \leqq i \leqq (p-3)/2 \end{cases} \pmod{\Pi}. \tag{5.20}$$

This is a system of $(p-1)/2$ linear congruences in the $(p-1)/2$ quantities $b_k E_k$, $k \in H_{a,b,c}$. Let

$$\Delta(x_1, \ldots, x_n) = \prod_{1 \leqq i < j \leqq n} (x_j - x_i).$$

The coefficient matrix M of the system is non-singular, since its entries are k^i, $0 \leqq i \leqq (p-3)/2$, $k \in H_{a,b,c}$, and thus its determinant is a van der Monde determinant

$$\det(M) = \Delta(k_1, \ldots, k_{(p-1)/2}),$$

where $\{k_1, \ldots, k_{(p-1)/2}\} = H_{a,b,c}$. Since $F \in R^*$, it follows from (5.20) that $b_k E_k \in S$ for all $k \in H_{a,b,c}$.

(5.21) **Lemma.** *Let*

$$M' = \begin{bmatrix} 1 & \cdots & \frac{1}{k_{\frac{p-1}{2}}} \\ k_1 & \cdots & k_{\frac{p-1}{2}} \\ \cdot & \cdots & \cdot \\ k_1^{\frac{p-3}{2}} & \cdots & k_{\frac{p-1}{2}}^{\frac{p-3}{2}} \end{bmatrix}.$$

Then

$$\sum_{k \in H_{a,b,c}} \frac{b_k E_k}{k} \equiv F \det(M')/\Delta(k_1, \ldots, k_{(p-1)/2}) \pmod{\Pi}.$$

Proof. This follows from (5.20) and elementary linear algebra. □

Thus to prove (5.19) it suffices to show that $\det(M') \not\equiv 0 \pmod{p}$. Let

$$\Gamma(x_1, \ldots, x_n) = \det \begin{bmatrix} 1 & \cdots & 1 \\ x_1^2 & \cdots & x_n^2 \\ x_1^3 & \cdots & x_n^3 \\ \cdot & \cdots & \cdot \\ x_1^n & \cdots & x_n^n \end{bmatrix}.$$

Then

$$\det(M') = (k_1 \ldots k_{(p-1)/2})^{-1} \Gamma(k_1, \ldots, k_{(p-1)/2}). \tag{5.22}$$

Let $s(x_1, \ldots, x_n)$ be the coefficient of x in $(x-x_1)(x-x_2)\ldots(x-x_n)$.

(5.23) **Lemma.** *We have* $\Gamma(x_1, \ldots, x_n) = \pm \Delta(x_1, \ldots, x_n)\, s(x_1, \ldots, x_n)$.

Proof. To prove this identity we work over an algebraically closed field of characteristic zero. The determinant defining $\Gamma(x_1, \ldots, x_n)$ vanishes if $x_i = x_j$ or if there is a polynomial $f(t)$ of degree n which vanishes on all the x_i and in which the coefficient of t is zero. Such a polynomial exists only if $s(x_1, \ldots, x_n) = 0$. Thus Γ vanishes if Δs vanishes. Thus every irreducible factor of Δs divides the determinant. Further, Δs has no multiple factors and its total degree is $(n(n-1))/2 + (n-1) = (n(n+1))/2 - 1$, which is the total degree of the determinant.

Thus Δs and the determinant differ by a constant factor. Finally, the coefficient of $x_2^2 x_3^3 \dots x_{n-1}^{n-1} x_n^n$ is ± 1 in both polynomials, so the constant factor is ± 1. □

From (5.22) and Lemma 5.23 we have

$$\begin{aligned}\det(M') &= \pm\Delta(k_1, \dots, k_{(p-1)/2})(k_1 \dots k_{(p-1)/2})^{-1} s(k_1, \dots, k_{(p-1)/2}) \\ &= \pm\Delta(k_1, \dots, k_{(p-1)/2})\left(\frac{1}{k_1} + \dots + \frac{1}{k_{(p-1)/2}}\right).\end{aligned}$$

Clearly $\Delta(k_1, \dots, k_{(p-1)/2}) \not\equiv 0 \pmod{p}$. To prove $\det(M') \not\equiv 0 \pmod{p}$ and finish the proof of Theorem 5.13, we have the following miraculous fact.

(5.24) **Lemma.** $\displaystyle\sum_{k \in H_{a,b,c}} \frac{1}{k} \equiv -q(a^a b^b c^c) \pmod{p}.$

Proof. It follows easily from the definition that $q(uv) \equiv q(u) + q(v)$, $q(u^{-1}) \equiv -q(u)$, and $q(u) = q(|u|)$. Thus $q(a^a b^b c^c) \equiv aq(a) + bq(b) - |c|\, q(|c|)$. On the other hand, it is easy to deduce from the definition of $H_{a,b,c}$ that

$$-\sum_{k \in H_{a,b,c}} \frac{1}{k} = \sum_{k=1}^{p-1} \left\{\left[\frac{ka}{p}\right] + \left[\frac{kb}{p}\right] - \left[\frac{k|c|}{p}\right]\right\} \frac{1}{k}.$$

Thus it suffices to show that, for $1 \leqq s \leqq p-1$,

$$\sum_{k=1}^{p-1} \left[\frac{ks}{p}\right] \frac{1}{k} \equiv s q(s) \pmod{p}.$$

This follows easily from a formula of Vandiver [23] 17. □

Since the curve we are considering is wild split, $q(a^a b^b c^c) \not\equiv 0 \pmod{p}$, so $\det(M') \not\equiv 0 \pmod{p}$, and we are finished. □

§ 6. Computation of the local pairing

Let v be the valuation of $\mathbb{Q}(\mu_p)$ extending the p-adic valuation of $\mathbb{Q}$, and let K be the completion of $\mathbb{Q}(\mu_p)$ at v. Using Theorem 2.6, we will explicitly compute the local pairing

$$\langle\ ,\ \rangle = \langle\ ,\ \rangle_v^{\lambda,\hat{\lambda}} : J(K)/\lambda J(K) \times J(K)/\hat{\lambda} J(K) \to \mathbb{Q}/\mathbb{Z}.$$

Let $\Delta = \mathrm{Gal}(K/\mathbb{Q}_p)$, and let $\kappa : \Delta \to \mathbb{Z}_p^*$ be the cyclotomic character giving the action of Δ on the group of p-th roots of unity. Let $\pi \in K$ be the unique uniformiser such that $\pi^{p-1} = -p$ and $\pi/(1-\zeta) \equiv 1 \pmod{\pi}$. Let U^i denote the image

in K^*/K^{*p} of the group of units in K congruent to 1 (mod π^i). If M is a Δ-module, let $M(i)$ denote the κ^i eigenspace of M. Then

$$U(i) \text{ is generated by } \begin{cases} \exp(\pi^i) & 2 \leqq i \leqq p-2 \\ \zeta \text{ and } 1+\pi^p & i=1 \\ 1+\pi^{p-1} & i=0 \end{cases} \tag{6.1}$$

It is well known that $U(i)$ pairs non-trivially with $U(j)$ under the Hilbert norm residue symbol if and only if $i+j \equiv 1 \pmod{p-1}$.

(6.2) **Proposition** (Faddeev [5]). *The image of ι_P is $U((p-1)/2) \times U^{(p+3)/2}$ if $F_{a,b,c}$ is wild split, and is $U^{(p+1)/2}$ if $F_{a,b,c}$ is tame or wild non-split.*

Most of the computation of $\langle\ ,\ \rangle$ may be disposed of by the following proposition.

(6.3) **Proposition.** *Let $\delta \in \Delta$. Then*

$$\langle x^\delta, y^\delta \rangle = \langle x, y \rangle^{\kappa^2(\delta)}.$$

Proof. Since x is defined over $\mathbb{Q}_p$, ι_P is Δ-equivariant. Denote linear equivalence of divisors by $\sim$. Since $\hat{\lambda}Q = P$ and $\hat{\lambda}^\delta \equiv \kappa(\delta)\hat{\lambda} \pmod{\hat{\lambda}^2}$, we have $\hat{\lambda}(D_Q - \kappa(\delta) D_Q^\delta) \sim \hat{\lambda} D_Q - \hat{\lambda}^\delta D_Q^\delta \sim D_P - D_P^\delta = 0$, so $D_Q - \kappa(\delta) D_Q^\delta \sim n D_P$ for some $n \in \mathbb{Z}$, so $f \equiv f^{\delta\kappa(\delta)} x^n \pmod{K^* \cdot K(F)^{*p}}$. Thus $\iota_Q(x^\delta) \equiv \iota_Q(x)^{\delta\kappa(\delta)} \pmod{\operatorname{im}(\iota_P)}$. By Proposition 1.14 and Lemmas 2.2 and 2.7, the image of ι_P is isotropic for the Hilbert norm residue symbol. Also the Hilbert norm residue symbol is Galois equivariant, and hence $(\alpha^\delta, \beta^\delta)_p = (\alpha, \beta)_p^{\kappa(\delta)}$ for all $\delta \in \Delta$. Thus

$$(\iota_P(x^\delta), \iota_Q(y^\delta))_p = (\iota_P(x)^\delta, \iota_Q(y)^{\delta\kappa(\delta)})_p = (\iota_P(x), \iota_Q(y))_p^{\kappa^2(\delta)}.$$

The lemma follows from Theorem 2.6. □

(6.4) **Corollary.** *The local pairing $\langle\ ,\ \rangle$ is trivial in the tame and wild non-split cases. In the wild split case its restriction to the subgroup $\iota_P^{-1}(U^{((p+3)/2)})$ is trivial. This subgroup has index p.*

Proof. Since ι_P is a Δ-equivariant injection, it follows from Proposition 6.2 that $J(K)/\lambda J(K)$ has a basis of eigenvectors for Δ with characters $\kappa^{(p-1)/2}$ and κ^i, $(p+3)/2 \leqq i \leqq p$, if $F_{a,b,c}$ is wild split, and κ^i, $(p+1)/2 \leqq i \leqq p$, if $F_{a,b,c}$ is tame or wild non-split. From Lemma 6.3 we deduce that if two eigenvectors, with characters κ^{i_1} and κ^{i_2}, pair non-trivially, then $i_1 + i_2 \equiv 2 \pmod{p-1}$. In the tame and wild non-split cases, this leaves only the possibility of pairing the eigenvector for $\kappa^{(p+1)/2}$ with itself; however, the pairing is skew symmetric by Lemma 1.10, so it is trivial in this case. In the wild split case, the only two eigenvectors which can pair non-trivially are those with characters $\kappa^{(p-1)/2}$ and $\kappa^{(p+3)/2}$. In this case the pairing is trivial on $\iota_P^{-1}(U^{((p+3)/2)})$, which has index p in $J(K)/\lambda J(K)$ by Proposition 6.2. □

It remains to compute the pairing of the two eigenvectors which can pair non-trivially. To do this we need the following lemma. As we saw in §2, ι_P is computed by evaluating x on divisors.

(6.5) **Lemma.** *Suppose that $F_{a,b,c}$ is wild split. Let P_i be any point in $X(K)$ such that $t(P_i)\in\pi^i R^*$, let O be the point where $t(O)=0$, and let $D_i=P_i-O$. Then $x(D_i)\in U^{((p+1)/2)+i}-U^{((p+3)/2)+i}$.*

Proof. From (5.3) we have

$$x=-a/c(1+\pi^{(p-1)/2}s).$$

By Lemma 5.5, s has a power series expansion on X in terms of t which converges for $|t|\leqq 1$. From (5.6) that expansion has the form

$$s=a_0+\pi a_1(t^p-t)+O(\pi^2 t^2),$$

where $a_0, a_1\in R^*$. The result is now clear. □

Remark. If we let O' be the point where $t(O')=0$ in X' and set $D=O-O'$, then $x(D)\in U((p-1)/2) \pmod{U^{(p+3)/2}}$. In fact, the computation of the lemma, suitably modified for the wild non-split and tame cases, leads to a proof of Proposition 6.2. First one shows that the group given as the image of ι_P in the proposition is achieved by evaluating x on certain divisors. Then one proves that this is the full image by observing that it is a maximal isotropic subgroup for the Hilbert norm residue symbol, and one knows a priori from Proposition 1.14 and Lemma 2.7 that the image of ι_P must be isotropic.

(6.6) **Theorem.** *If $F_{a,b,c}$ is wild split then $\langle\ ,\ \rangle$ induces a non-trivial pairing between $(J(K)/\lambda J(K))((p-1)/2)$ and $(J(K)/\lambda J(K))((p+3)/2)$.*

Proof. Choose a point $P\in X(K)$ such that $t(P)\in\pi R^*$ and $P\notin\mathrm{supp}(f)$. Let $D=P-O$. Let $x\in J(K)/\lambda J(K)$ be the point represented by D. Then x has non-trivial image in $(J(K)/\lambda J(K))((p+3)/2)$, since by Lemma 6.5 $\iota_P(x)$ has non-trivial image in $(K^*/K^{*p})((p+3)/2)$. By Theorem 2.6 it suffices to show that $i_Q(x)$ pairs non-trivially under the Hilbert norm residue symbol with any element of $(K^*/K^{*p})((p-1)/2)$. Now $\iota_Q(x)=f(D)$, and by Theorem 5.13 $f(D)\in 1+\pi^{(p+1)/2}R^*$. Hence $\iota_Q(x)$ has non-trivial image in $(K^*/K^{*p})((p+1)/2)$. Since $(K^*/K^{*p})((p-1)/2)$ and $(K^*/K^{*p})((p+1)/2)$ pair non-trivially with respect to the Hilbert norm residue symbol, the theorem is proven. □

§ 7. The Shafarevich-Tate group

In this section K will denote the global field $\mathbb{Q}(\zeta_p)$. Having computed the local pairing, we can now compute the Cassels-Tate pairing on S_λ. If v is a valuation in M_K, denote by ι_v the map ι_P relative to K_v, and by i_v the map i_λ. Then the isomorphism j_P identifies S_λ with the subgroup

$$\{x\in K^*/K^{*p}\colon x\in\mathrm{im}(\iota_v) \text{ for all } v\in M_K\}$$

of K^*/K^{*p}. If $v(p)=0$ then $\mathrm{im}(i_v)$ is the group of unramified cocycles in $H^1(K_v, J_\lambda)$, so $\mathrm{im}(\iota_v)=\{x\in K_v^*: v(x)\equiv 0 \pmod p\}$. If $v(p)\neq 0$, then by Proposition 6.2, $\mathrm{im}(\iota_v)\subseteq\{x\in K_v^*: v(x)\equiv 0 \pmod p\}$. Thus if

$$U=\{x\in K^*/K^{*p}: v(x)\equiv 0 \pmod p \text{ for all } v\},$$

and if w is the unique valuation of K above p, then S_λ fits into the cartesian diagram

$$\begin{array}{ccc} S_\lambda & \xrightarrow{j_P} & U \\ {\scriptstyle \iota_w}\downarrow & & \downarrow \\ \mathrm{im}(\iota_w) & \longrightarrow & K_w^*/K_w^{*p}. \end{array}$$

Further, by Lemma 1.5, the Cassels-Tate pairing on S_λ factors through the local pairing on its image in K_w^*/K_w^{*p}. Thus, by Theorem 6.6, the pairing will be non-trivial if and only if there are elements x and y in U whose images in K_w^*/K_w^{*p} are non-trivial and in the $\kappa^{(p-1)/2}$ and $\kappa^{(p+3)/2}$ eigenspaces. This problem of determining the image of U in K_w^*/K_w^{*p} is a problem from the theory of cyclotomic integers which is not completely solved. We will summarize what is known about it here. Let $I=\{i\in\mathbb{Z}: i \text{ even}, 2\leqq i\leqq p-3\}$. If $i\in I$, denote by i' the complementary odd integer such that $i+i'=p$. Let $V=K_w^*/K_w^{*p}$.

(7.1) **Proposition.** *There exists a subset $S\subseteq I$ such that the image of U in V is*

$$\mu_p\cup\bigcup_{i\in S} V(i)\cup\bigcup_{i\in I-S} V(i').$$

Further, $S=I$ if p is regular, and more generally $i\in S$ if $p\nmid B_i$.

Proof. We have $\{0, 1, 2, \ldots, p-2\}=I\cup I'\cup\{0, 1\}$. First, $V(0)\cap\mathrm{im}(U)=\{1\}$. Indeed, it follows from the fact that $\#\mathrm{Gal}(K/\mathbb{Q})$ is prime to p that $(K^*/K^{*p})(0)=\mathbb{Q}^*/\mathbb{Q}^{*p}$, and obviously $\mathbb{Q}^*/\mathbb{Q}^{*p}\cap U=\{1\}$. Second, $V(1)\cap\mathrm{im}(U)=\mu_p$. Indeed, by (6.1), $V(1)=\mu_p\cup(1+\pi^pR_w^*)$. Suppose that there is an element $x\in U\cap(1+\pi^pR_w^*)$. Then $L=K(x^{1/p})$ is an extension of K which is unramified anywhere and which has a non-trivial residue field extension at $(1-\zeta)$. By class field theory there is no such extension, since $(1-\zeta)$ is principal.

Now let L be the maximal abelian unramified extension of K. Let A be the ideal class group of $\mathbb{Q}(\zeta_p)$. Then class field theory gives an isomorphism

$$A/pA\xrightarrow{\sim}\mathrm{Gal}(L/K).$$

Kummer theory gives an isomorphism

$$\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_p)\xrightarrow{\sim}\left\{\begin{array}{l}x\in K^*/K^{*p}: K_v(x^{1/p}) \text{ is unramified}\\ \text{over } K_v \text{ for all } v\end{array}\right\}.$$

If $v(p)=0$, then $K_v(x^{1/p})$ is unramified if and only if $v(x)\equiv 0 \pmod p$, and $K_w(x^{1/p})$ is unramified if and only if $x\in(1+\pi^p R_w)K_w^{*p}$. As we saw above, this latter condition implies that $x\in K_w^{*p}$. Hence we have an exact sequence

$$0\to \mathrm{Hom}(A/pA, \mu_p)\to U\to V. \tag{7.2}$$

Let E be the group of units in the ring of integers of K. If $x\in U$ is the image of $\bar{x}\in K^*$, then $(\bar{x})=\mathfrak{a}^p$ for some ideal $\mathfrak{a}$. The map $x\mapsto\mathfrak{a}$ is well defined modulo principle ideals. Its kernel is E/E^p, and its image is $A[p]$. Thus we get an exact sequence

$$0\to E/E^p\to U\to A[p]\to 0. \tag{7.3}$$

Let $i\in I$. Then $(E/E^p)(i)\approx\mathbb{Z}/p\mathbb{Z}$ and $(E/E^p)(i')=0$ (see [25] 8.10 and 8.13). Hence from (7.3) we have

$$\mathrm{rk}\,(A[p](i))+1=\mathrm{rk}\,(U(i)) \quad\text{and}\quad \mathrm{rk}\,(A[p](i'))=\mathrm{rk}\,(U(i')). \tag{7.4}$$

We claim that either $\mathrm{im}(U)\cap V(i)$ or $\mathrm{im}(U)\cap V(i')$ is non-trivial, but not both. Indeed, from (7.2) it follows that

$$\mathrm{im}(U)\cap V(i') \text{ is non-trivial} \Leftrightarrow \mathrm{rk}\,(U(i'))=\mathrm{rk}\,((A/pA)(i))+1,$$

(since $\mathrm{Hom}((A/pA), \mu_p)(i')=\mathrm{Hom}((A/pA)(i), \mu_p)$)

$$\begin{aligned}
&\Leftrightarrow \mathrm{rk}\,(A[p](i'))=\mathrm{rk}\,((A/pA)(i))+1 \quad \text{(by (7.4))}\\
&\Leftrightarrow \mathrm{rk}\,((A/pA)(i'))=\mathrm{rk}\,(A[p](i))+1\\
&\Leftrightarrow \mathrm{rk}\,(\mathrm{Hom}\,(A/pA, \mu_p)(i))=\mathrm{rk}\,(A[p](i))+1\\
&\Leftrightarrow \mathrm{rk}\,(\mathrm{Hom}\,(A/pA, \mu_p)(i))=\mathrm{rk}\,(U(i)) \quad \text{(by (7.4))}\\
&\Leftrightarrow \mathrm{im}(U)\cap V(i)=0 \quad \text{(by (7.2))}.
\end{aligned}$$

Since, for $i\in S$, $V(i)$ and $V(i')$ have rank 1 by (6.1), this proves the first statement. Finally, it follows from the theory of cyclotomic units that it is the i component that is non-trivial if $p\nmid B_i$ (see [25] 8.16). □

(7.5) **Theorem.** *If* $p\equiv 1 \pmod 4$, $p\nmid B_{(p-1)/2}B_{(p+3)/2}$, *and* $F_{a,b,c}$ *is wild split, then* $Ш[\lambda]$ *contains a subgroup isomorphic to* $\mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/p\mathbb{Z}$.

Proof. By Proposition 7.1 and Theorem 6.6, the conditions guarantee the existence of elements in U whose local pairing is non-trivial. □

Concluding remarks

1. Using the same methods and the fact that there is a non-trivial $\mathbb{Q}(\mu_p)$-rational λ^3-torsion point [7], one can compute the local pairing $\langle\ ,\ \rangle_v^{\lambda^2,\lambda}$ and see if there are any elements in $Ш(\mathbb{Q}(\mu_p), J)$ of exact order λ^2. It turns out that there are none if p is regular. However, if p satisfies a certain irregularity condition, then $Ш(\mathbb{Q}(\mu_p), J)$ contains a $\mathbb{Z}[\mu_p]$-submodule isomorphic to $(\mathbb{Z}[\mu_p]/(\lambda^2))^2$. Specifi-

cally, this occurs if F is wild split and the image of U is non-trivial in $V((p-1)/2)$ and $V((p+5)/2)$, or if F is wild non-split and the image of U is non-trivial in $V((p+1)/2)$ and $V((p+3)/2)$. For the condition to be satisfied, one of the following is necessary: in the wild split case, $p \equiv 1 \pmod 4$ and $p | B_{(p-5)/2}$, or $p \equiv 3 \pmod 4$ and $p | B_{(p+1)/2}$; in the wild non-split case, $p \equiv 1 \pmod 4$ and $p | B_{(p-1)/2}$, or $p \equiv 3 \pmod 4$ and $p | B_{(p-3)/2}$. These conditions are also sufficient if Vandiver's conjecture is true. However, the author knows of no primes satisfying these conditions. First, it is a well-known and elementary property of Bernoulli numbers that $p \nmid B_{(p+1)/2}$ when $p \equiv 3 \pmod 4$. Second, by inspection of the tables in [12] one finds that no prime less than 8,000 satisfies any of the conditions, and according to [24] the condition $p \equiv 1 \pmod 4$, $p | B_{(p-1)/2}$ is not satisfied for $p < 125{,}000$.

2. Faddeev's computation of S_λ enabled him to bound the rank of $J(K)$. Gross and Rohrlich [8] found a point on $J(K)$ which has infinite order except in certain cases. Combining this with Faddeev's bound, they determined the $\mathbb{Z}[\mu_p]$-rank of $J(K)$ for $p \leqq 13$ except in one case (see the table at the end of §4 of [8]). In each of these cases the rank was 0 or 1. Our results decrease Faddeev's bound by 2 whenever the conditions of Theorem 7.5 are satisfied. In the case $p = 17$, two of the three isomorphism classes of curves $F_{a,b,c}$ satisfy the conditions; thus we can deduce that the rank is 1 in those cases. The third isomorphism class, $F_{1,2,14}$, is wild non-split, and its rank should be 2 according to the conjecture of Birch and Swinnerton-Dyer.

3. On heuristic principles one expects plenty of pairs $(p, F_{a,b,c})$ to satisfy the conditions of Theorem 7.5 (in particular, infinitely many). However, since it is not even known if there are infinitely many primes not dividing $B_{(p-1)/2} B_{(p+3)/2}$, we cannot prove this. From the tables in [12] one finds that no $p \equiv 1 \pmod 4$ less than 8,000 divides $B_{(p-1)/2} B_{(p+3)/2}$, and for any such prime about half the curves $F_{a,b,c}$ are wild split.

References

1. Altman, A., Kleiman, S.: Introduction to Grothendieck duality theory. (Lecture Notes in Mathematics, Vol. 146). Berlin-Heidelberg-New York: Springer 1970
2. Bosch, S., Lütkebohmert, W.: Stable reduction and uniformization of abelian varieties I. Math. Ann. **270**, 349–379 (1985)
3. Bosch, S., Guntzer, U., Remmert, R.: Non-archimedean analysis. Berlin-Heidelberg-New York: Springer 1984
4. Cassels, J.W.S., Fröhlich, A.: Algebraic number theory. London: Academic Press 1967
5. Faddeev, D.K.: Invariants of divisor classes for the curves $x^k(1-x)=y^l$ in an l-adic cyclotomic field. Tr. Mat. Inst. Steklova **64**, 284–293 (1961)
6. Fresnel, J., Put, M., van der: Géometrie analytique rigide et applications. Boston: Birkhäuser 1981
7. Greenberg, R.: On the Jacobian variety of some algebraic curves. Compos. Math. **42**, 345–359 (1981)
8. Gross, B.H., Rohrlich, D.E.: Some results on the Mordell-Weil group of the jacobian of the Fermat curve. Invent. Math. **44**, 201–224 (1978)
9. Grothendieck, A., Dieudonné, J.: Eléments de Géometrie Algébrique III. Étude cohomologique des faisceaux cohérents. Publ. Math. Inst. Hautes Etud. Sci. **11** (1961); **17** (1963)
10. Hartshorne, R.: Algebraic geometry. Berlin-Heidelberg-New York: Springer 1977

11. Hartshorne, R.: Residues and duality. (Lecture Notes in Mathematics, Vol. 20). Berlin-Heidelberg-New York: Springer 1966
12. Johnson, W.: On the vanishing of the Iwasawa invariant μ for $p<8{,}000$. Math. Comp. **27**, 387–396 (1973)
13. Lang, S.: Reciprocity and correspondences. Am. J. Math. **80**, 431–440 (1958)
14. Lang, S., Tate, J.: Principal homogeneous spaces over abelian varieties. Am. J. Math. **80**, 659–685 (1958)
15. Lichtenbaum, S.: Curves over discrete valuation rings. Am. J. Math. **85**, 380–405 (1968)
16. McCallum, W.G.: The degenerate fiber of the Fermat curve. Number theory related to Fermat's last theorem, Neal Koblitz (ed.). Boston: Birkhäuser 1982
17. Milne, J.S.: Arithmetic duality theorems. London: Academic Press 1986
18. Milne, J.S.: Jacobian varieties. Arithmetic Geometry, Cornell, G., Silverman, J.H. (eds.). Berlin-Heidelberg-New York: Springer 1986
19. Mumford, D.: Abelian varieties. Oxford: Oxford University Press 1970
20. Raynaud, M.: Spécialisation du foncteur de Picard. Publ. Math., Inst. Hautes Etud. Sci. **38**, 27–76 (1970)
21. Serre, J-P.: Groupes algébriques et corps de classes. Paris: Hermann 1959
22. Serre, J-P.: Local fields. Translation of corps locaux. Paris: Hermann, 1959. Berlin-Heidelberg-New York: Springer 1979
23. Vandiver, H.S.: A property of cyclotomic integers and its relation to Fermat's last theorem. Ann. Math. **21**, 73–80 (1919–1920)
24. Wagstaff, S.: The irregular primes to 125,000. Math. Comp. **32**, 583–591 (1978)
25. Washington, L.C.: Introduction to cyclotomic fields. Berlin-Heidelberg-New York: Springer 1982

Oblatum 6-IX-1987 & 29-II-1988

Note added in proof

The step in the proof of Theorem 5.13 after (5.15) requires further justification. A congruence mod_Y does not always hold mod_X, since $D^0(Y) \subsetneq D^0(X)$. However, in this case we can argue as follows. The two residue classes R and $\bar{R}$ where $|u|<1$ on Y have u as a parameter, and contain the components W and $\bar{W}$ of X as the closed balls $|u| \leqq |\Pi|$. Note that from (5.8) s is congruent to a non-zero constant on each of R and $\bar{R}$. Let g be as in (5.15). Since g is a rational function in t, it may be regarded as a function on Y; further, since $cg \in A^0(Y) - \Pi A^0(Y)$ for some $c \in L^*$, $dg/g \in D^0(Y)$. Combining (5.15) and (5.12), we get

$$\frac{df}{f} = \pi^{(p-1)/2} D' \frac{dt}{s} + p \frac{dg}{g} + \pi^{(p-1)/2} \Pi \omega$$

where ω is in $D^0(Y)$ and regular on X. Furthermore, since s is a unit on $R \cup \bar{R}$, ω has only simple poles on $R \cup \bar{R}$. To show that the congruence (5.15) also holds mod_X, we must show that $\omega \in D^0(X)$. On each residue class R and $\bar{R}$ we can write

$$\omega = g(u)\, du + \text{terms of the form } a\, du/(u-b),\ a, b \in S,\ |\Pi| < |b| \leqq 1.$$

where $g(u)$ is a power series with integer coefficients. Expanding the polar terms in powers of u/b and setting $u = \Pi t$, we get something in $D^0(X)$.