Part 2

# Non-abelian Invariant Differentials*)

*) Mimeographed Note 1971
Part 1 was published later as "Schwarzian equations";
J.Fac.Sci. Univ. of Tokyo IA21(1974)
The section- and the theorem-numberings used in Part I
are basically kept unchanged in the published version.

Part 2A The Frobenius map $\sigma$, the associated differential $\omega$, and the $\sigma$-invariant S-operator

Part 2B Theory of $\omega$ in some cases of automorphic functions

Y. Ihara

## §5 Valued differential fields

§ 5-1 The valuation V We shall keep the notations and assumptio of §1-1. Suppose now that we are given:

v: a discrete valuation of k, additive and normalized;

V: a discrete valuation of K extending v, assumed to have the same value group as v;

$* \mapsto \bar{*}$ : the reduction map modulo V.

We assume that K and $\bar{K}$ have unequal characteristics, i.e.,

$$ch(K) = 0, \quad ch(\bar{K}) = p > 0;$$

and that the differentiation $d: K \mapsto D(K)$ is V-continuous, i.e., continuous with respect to the V-adic topology of K and that induce on D(K).

Since d is V-continuous, the constant field k is closed in K, not only algebraically, but also topologically.

Let $\mathcal{O}$ be the valuation ring of V, and $\mathfrak{p}$, the maximal ideal of $\mathcal{O}$. Since multiplications of elements of $k^{\times}$ commute with d, the V-continuity of d implies that the $\mathcal{O}$-submodule of D(K) genera by its subset $\{dx \mid x \in \mathcal{O}\}$ must be a free $\mathcal{O}$-module of rank one.. ~~Call this~~ $\mathcal{O}$-module $D(\mathcal{O})$. It is generated by some (single) elemen of the form dx with $x \in \mathcal{O}$. Such an element x will be called regula Put $D^0(\mathcal{O}) = \mathcal{O}$, and for $h \geq 1$, $D^h(\mathcal{O}) = D(\mathcal{O}) \otimes \ldots \otimes D(\mathcal{O})$ (h copi over $\mathcal{O}$). Then each $D^h(\mathcal{O})$ is a free $\mathcal{O}$-module of rank one. Indee if x is a regular element, then $D^h(\mathcal{O}) = \mathcal{O}(dx)^h$. A differential

Let $\mathfrak{O}$ be the valuation ring of V, and $\mathfrak{P}$, the maximal ideal. Let $D(\mathfrak{O})$ denote the $\mathfrak{O}$-submodule of $D(K)$ generated by all elements of $D(K)$ of the form $dx$ with $x \in \mathfrak{O}$. Then $D(\mathfrak{O})$ is a free $\mathfrak{O}$-module of rank one. In fact, since every $\mathfrak{O}$-submodule of $D(K)$, other than $\{0\}$ and $D(K)$ itself, is a free $\mathfrak{O}$-module of rank one (because $D(K)$ is one dimensional over K, and $\mathfrak{O}$ is the valuation ring of a discrete valuation of K), it suffices to check $D(\mathfrak{O}) \neq \{0\}$, $\neq D(K)$. First, since $d \neq 0$, there is some $z \in K^{\times}$ with $dz \neq 0$. But since $V(K^{\times}) = v(k^{\times})$, there is some $c \in k^{\times}$ with $cz \in \mathfrak{O}$, and $d(cz) = c.dz \neq 0$; hence $D(\mathfrak{O}) \neq \{0\}$. Secondly, take any $\xi \in D(K)^{\times}$. Then since $d$ is V-continuous and $V(K^{\times}) = v(k^{\times})$, there is some $c \in k^{\times}$ such that $V(dz) \in \mathfrak{O}\cdot\xi$ for all $z \in c.\mathfrak{O}$. But then, $dx \in c^{-1}\mathfrak{O}\,\xi$ for all $x \in \mathfrak{O}$; hence $D(\mathfrak{O}) \neq D(K)$, and accordingly, $D(\mathfrak{O})$ is a free $\mathfrak{O}$-module of rank one.

An element $x \in \mathfrak{O}$ is called <u>regular</u> if $dx$ generates $D(\mathfrak{O})$, i.e., if $D(\mathfrak{O}) = \mathfrak{O}.dx$. Put $D^0(\mathfrak{O}) = \mathfrak{O}$, and for each $h \geq 1$, $D^h(\mathfrak{O}) = D(\mathfrak{O}) \otimes \ldots \otimes D(\mathfrak{O})$ ( h copies, over $\mathfrak{O}$ ). Then each $D^h(\mathfrak{O})$ is a free $\mathfrak{O}$-module of rank one. In fact, if $x$ is a regular element, then $D^h(\mathfrak{O}) = \mathfrak{O}.(dx)^h$. A differential

$\xi \in D^h(K)$ will be called V-<u>integral</u> if it belongs to $D^h(\mathcal{O})$.

We shall extend the valuation V of $K = D^0(K)$ to a $\mathbb{Z}^{\cup}(\infty)$-valued function on $\bigcup_{h\geq 0} D^h(K)$, by imposing the condition:

$$V(\xi \otimes \eta) = V(\xi) + V(\eta) \qquad \text{(for any } \xi, \eta \in \bigcup_{h\geq 0} D^h(K))$$

together with the normalization:

$$V(dx) = 0 \qquad \text{(for x: regular).}$$

It is clear that $\xi \in D^h(K)$ is V-integral if and only if $V(\xi) \geq 0$. Note that $V(dx) \geq V(x)$ holds for any $x \in K$. Indeed, since $V(K^\times) = v(k^\times)$, we may assume $V(x) = 0$. But then, $V(dx) \geq 0$, since dx is V-integral. It is also clear that $x \in K$ is regular if and only if $V(x) = V(dx) = 0$.

Put $D^h(\mathfrak{p}) = \mathfrak{p} \cdot D^h(\mathcal{O})$ $(h \geq 0)$. Then $D^h(\mathcal{O})/D^h(\mathfrak{p})$ is a one-dimensional vector space over $\bar{K} = \mathcal{O}/\mathfrak{p}$. Call it $D^h(\bar{K})$, and put $D(\bar{K}) = D^1(\bar{K})$. Then $D^0(\bar{K}) = \bar{K}$, and $D^h(\bar{K})$ $(h \geq 1)$ can be identified naturally with $D(\bar{K}) \otimes \ldots \otimes D(\bar{K})$ (h copies, over $\bar{K}$). For each $\xi \in D^h(\mathcal{O})$, let $\bar{\xi}$ denote its residue class modulo $D^h(\mathfrak{p})$. Then $\bar{x} \mapsto \overline{dx}$ $(x \in \mathcal{O})$ defines a differentiation $\bar{K} \longrightarrow D(\bar{K})$, which will be denoted by $\bar{d}$. The constant field of $\bar{d}$ contains $\bar{k} \cdot \bar{K}^p$, and is strictly smaller than $\bar{K}$, since $\overline{dx} \neq 0$ for x: regular.

§ <u>5-2</u> <u>Field extensions</u> (I) <u>Effect of completion</u> Let $K_V$ be the completion of K with respect to V. Then the differentials and the differentiation of K can be extended to those of $K_V$ in a natural manner. First, define $D(K_V)$ by $D(K) \otimes_K K_V$. Then, $d_V$ is defined to be the unique V-continuous differentiation $K_V \longrightarrow D(K_V)$ that extends d. Clearly, a regular element of K is also regular in $K_V$. Hence $D^h(\mathcal{O}_V) = D^h(\mathcal{O}) \otimes_{\mathcal{O}} \mathcal{O}_V$, $\mathcal{O}_V$ being the valuation ring of V in $K_V$. The constant field $k_V$ of $K_V$ contains the V-adic closure of k in $K_V$. But they do not coincide in general. In any case, it is obvious that $V(K_V^\times) = V(k_V^\times)$, since $k_V$ contains k.

(II) Effect of unramified extensions Let L be a separably algebraic extension of K. Then we know that d can be uniquely extended to $d_L : L \longmapsto D(L) = D(K) \otimes_K L$, and that the constant field of $d_L$ is the algebraic closure of k in L, denoted by $\mathcal{l}$ (§ 1-4). Now, let $V_L$ be a valuation of L extending V. By definition, $V_L/V$ is unramified if $V_L(L^\times) = V(K^\times)$ and if the residue field extension $\bar{L}/\bar{K}$ is also separable. Suppose that $V_L/V$ is unramified. Then, it is clear that $V_L(L^\times) = V_L(\mathcal{l}^\times)$, i.e., the condition of § 5-1 on the value groups is preserved. We shall show that:

Proposition 8 The differential $d_L$ is $V_L$-continuous, and regular elements of K are also regular in L; hence

$$D^h(\mathcal{O}_L) = D^h(\mathcal{O}) \otimes_{\mathcal{O}} \mathcal{O}_L \qquad (h \geq 0),$$

$\mathcal{O}_L$ being the valuation ring of $V_L$.

Proof It is enough to check (the two assertions) when [L:K] is finite. Let $\mathcal{O}^i$ be the integral closure of $\mathcal{O}$ in L. Then $\mathcal{O}^i$ is the intersection of all valuation rings of L containing $\mathcal{O}$ (hence $\mathcal{O}_L \supset \mathcal{O}^i$). Let $y \in \mathcal{O}_L$. Take such $\alpha \in L$ that satisfy $V_L(\alpha) = 0$ and also $V_L'(\alpha)$, $V_L'(\alpha y) \geq 0$, for all other extensions $V_L'$ of V to L. This is possible by the approximation theorem on distinct discrete valuations. Put $y = \beta/\alpha$. Then $\alpha, \beta \in \mathcal{O}^i$, and $V_L(\alpha) = 0$. Now, since L/K is a finite separable extension, $\mathcal{O}^i$ is a finite $\mathcal{O}$-module; $\mathcal{O}^i = \sum_i \mathcal{O} z_i$. Therefore, if x is a regular element of K and $z \in \mathcal{O}^i$, we have $V_L(d_L z/dx) \geq \operatorname{Min}_i V(d_L z_i/dx)$; hence the set $\{V_L(d_L z/dx) \mid z \in \mathcal{O}^i\}$ is bounded from below. By using the above expression $y = \beta/\alpha$ for $y \in \mathcal{O}_L$, we see immediately that the set $\{V_L(d_L y/dx) \mid y \in \mathcal{O}_L\}$ is also bounded from below. Therefore, $d_L$ is $V_L$-continuous. Now we shall check that x is also regular in L. Suppose it were not. Then, the restriction of $\overline{d}_L$ to $\overline{K}$ must vanish identically, which is impossible since $\overline{L}/\overline{K}$ is separable and $\overline{d}_L \neq 0$. Q.E.D.

Corollary The notations and assumptions being as above, if there is a V-preserving isomorphism $\varphi$ of L into the completion $K_V$ of K, which is identical on K, then,

$$\varphi_* \circ d_L = d_V \circ \varphi$$

holds, where $\varphi_*$ is the canonical embedding $D(L) \hookrightarrow D(K_V)$ induced by $\varphi : L \hookrightarrow K_V$.

## § 6 The Frobenius map $\sigma$ and the associated differential $\omega$

§ 6-1 The q-th Frobenius map $\sigma$. As assumed in § 5-1, let $p = ch(\bar{K}) > 0$, and let $q = p^f$ be a fixed positive power of p. Let $K_V$ be the completion of K with respect to V. We shall always consider K as a subfield of $K_V$, identifying in particular the residue field of $K_V$ with that of K. Now, an injective isomorphism

$$\sigma : K \longmapsto K_V$$

will be called a q-th Frobenius map of K, if the following two conditions are satisfied:

($\sigma$1) $\sigma$ is V-preserving, and induces the q-th power map $\bar{x} \rightarrow \bar{x}^q$ of the residue field.

($\sigma$2) $\sigma$ commutes with the differentiation, i.e., $k^\sigma \subset k$, $(K - k)^\sigma \subset K - k$, and

$$\left(\frac{dy}{dx}\right)^\sigma = \frac{d_V(y^\sigma)}{d_V(x^\sigma)}$$

holds for all $x, y \in K$ with $x \notin k$. (Here, as in § 5-2(I), $d_V$ is the canonical extension of d to $K_V$.)

For each $h \geq 0$, $D^h(K)$ is canonically embedded into $D^h(K_V)$. On the other hand, $\sigma$ induces a map $D^h(K) \longmapsto D^h(K_V)$, which maps $y(dx)^h$ to $y^\sigma\{d_V(x^\sigma)\}^h$. This is well-defined by ($\sigma$2). In the following, we shall write d instead of $d_V$, for the simplicity of notations.

Proposition 9 Let $\sigma$ be a q-th Frobenius map of K. Then there is a positive integer $\nu = \nu(\sigma)$ such that

$$V(\xi^\sigma) = V(\xi) + h\nu$$

holds for all $\xi \in D^h(K)$, $\xi \neq 0$, $h \geq 0$.

Proof Let x be a regular element of K, and put $\nu = V(dx^\sigma)$. Let $\xi = y(dx)^h$ $(y \in K^\times)$. Then $V(\xi^\sigma) - V(\xi) = V(y^\sigma/y) + h \cdot V(dx^\sigma/dx) = h \cdot V(dx^\sigma) = h\nu$. On the other hand, let $\pi$ be a prime element of v, and put $x^\sigma = x^q + \pi z$ $(z \in \mathcal{O})$. Then we have $dx^\sigma = qx^{q-1}dx + \pi dz$; hence $\nu > 0$. Q.E.D.

Corollary Let $\eta \in D^h(K)$, with $h \geq 1$. Then the equation $\eta = \xi - \xi^\sigma$ has at most a unique solution $\xi \in D^h(K)$. If K is complete, then such a solution exists.

Proof The uniqueness follows immediately from the Proposition. The solution $\xi$ for the complete case is given by $\xi = \sum_{n=0}^{\infty} \eta^{\sigma^n}$ (which is convergent by the Proposition). Q.E.D.

§ 6-2 The associated differential $\omega$. Let $\sigma$ be a q-th Frobenius map of K. A differential $\omega \in D(K)^\times$ will be called a differential associated with $\sigma$, if

$$\omega^\sigma / \omega \in k^\times$$

holds.

Theorem 2 Let $\sigma$ be a q-th Frobenius map of K. Then (i) the

associated differential $\omega$ is at most unique up to $k^{\times}$-multiples,
(ii) $\omega$ exists if $K$ is complete and $\bar{K}$ is separably closed.

Proof (i) If $\omega$ and $z\omega$ ($z \in K^{\times}$) are two associated differentials, then $z^{\sigma-1} \in k^{\times}$. Hence $dz/z$ is $\sigma$-invariant, contradicting Proposition 9 unless $dz = 0$. (ii) Let $c$ be any element of $k^{\times}$ with $v(c) = \nu$ (see Proposition 9 for the symbol $\nu$). We shall show that there exists $\omega = y \cdot dx \in D(K)^{\times}$ with $\omega^{\sigma}/\omega = c$. Put $U = c \cdot (dx^{\sigma}/dx)^{-1}$, which is a V-unit in K. It is enough to show that the equation $y^{\sigma-1} = U$ has a solution $y$ in $K^{\times}$. This can be shown by a standard type argument, as follows. First, since $\bar{K}$ is separably closed, $\bar{U}$ has a $(q-1)$-th root $\bar{U}_1$ in $\bar{K}$ ($U_1 \in K$). Replacing $y$ by $yU_1$, we may assume from the beginning that $\bar{U} = 1$. Let $\pi$ be a prime element of $v$. It is enough to find a sequence $\{y_n\}_1^{\infty}$ of V-units of K, such that $y_{n+1} \equiv y_n \pmod{\pi^n}$ and that $y_n^{\sigma-1} \equiv U \pmod{\pi^n}$. Put $y_1 = 1$, and suppose that $y_1, \dots y_n$ are already found. Put $y_n^{\sigma-1} = U + \pi^n A_n$, and $y_{n+1} = y_n(1 + \pi^n B_n)$ ($A_n, B_n \in \mathcal{O}$). Then,

$$y_{n+1}^{\sigma-1} \equiv (U + \pi^n A_n)\{1 + \pi^n(B_n^q - B_n)\} \pmod{\pi^{n+1}};$$

hence it is enough to solve the Artin-Schreier equation $\bar{B}_n^q - \bar{B}_n = -\bar{U}^{-1}\bar{A}_n$ in $\bar{K}$, which is possible since $\bar{K}$ is assumed to be separably closed. Q.E.D.

The following Proposition will be needed later.

Proposition 10 Let $\sigma$ be a q-th Frobenius map of K, and suppose that an associated differential $\omega \in D(K)^{\times}$ exists. Assume that $\bar{k}^{1/p} \cap \bar{K} = \bar{k}$. Then $\omega$ is non-exact in K.

Proof Suppose that $\omega$ were exact; $\omega = dy$ $(y \in K)$. Since $\omega \neq 0$, we have $y \notin k$. Hence y cannot be approximated by elements of k. Among all elements of k, let a be one of the nearest to y. Choose $b \in k^{\times}$ in such a way that $y_1 = b(y - a)$ is a V-unit. Then $\bar{y}_1 \notin \bar{k}$. Since $\omega^{\sigma} = c\omega$ with $c \in k^{\times}$, we have $y_1^{\sigma} = cy_1 + e$ $(e \in k)$. But $v(c) = \nu > 0$; hence e is also a v-unit, and $y_1^{\sigma} \equiv e \pmod{\mathfrak{P}}$; hence $\bar{y}_1^{q} = \bar{e} \in \bar{k}^{\times}$. But since it is assumed that $\bar{k}^{1/p} \cap \bar{K} = \bar{k}$, we deduce that $\bar{y}_1 \in \bar{k}^{\times}$, which is a contradiction. Therefore, $\omega$ must be non-exact. Q.E.D.

§ 6-3 Extending K to the field of $\omega$ (I) Extending $\sigma$ to $K_V$.

In general, an associated differential $\omega$ may not exist in the given field K. But Theorem 2 (ii) suggests that such an $\omega$ should exist in the completion of a certain unramified extension of K. To fix this, it is necessary to study the extensions of a Frobenius map $\sigma$ to the completion and unramified extensions of K. To begin with, we see that a q-th Frobenius map $\sigma$ of K can be uniquely extended to that of the completion $K_V$. Indeed, it can be extended uniquely to an injective isomorphism $\sigma_V$ of $K_V$ into itself that satisfies

($\sigma 1$) of § 6-1. The only point to be checked is that if $x \in K_V$, then $d_V(x) = 0$ and $d_V(x^{\sigma_V}) = 0$ are equivalent. To check this, let $\{x_n\}_1^\infty$ be a sequence in K converging to x. Then since $V(dx_n^\sigma) = V(dx_n) + \nu$ (Proposition 9), $\{dx_n\}_1^\infty$ is a null sequence if and only if $\{dx_n^\sigma\}_1^\infty$ is so; hence our assertion.

(II) <u>Complete unramified extension</u> L. Now we assume that K is complete. Then, unramified extensions of K and separable extensions of $\bar{K}$ correspond in a one-to-one manner (by $L \longmapsto \bar{L}$). By a <u>complete unramified</u> extension of K, we mean the completion of a (possibly infinite) unramified extension L of K. Let L be an unramified normal extension of K, and let $G = \mathrm{Aut}_K L$ be the Krull's Galois group. Let $g \in G$. Then g can be extended uniquely to a V-continuous automorphism $g_V$ of $L_V$. The group $G_V = \{g_V \mid g \in G\}$ consists of all V-continuous automorphisms of $L_V$ over K. We shall call $G_V$ the Galois group of $L_V$ over K. Sometimes, the two groups $G_V$ and G will be identified with each other. The completion of a normal (unramified) extension will also be called normal. We note that <u>the fixed field of</u> $G_V$ <u>in</u> $L_V$ <u>is</u> K. Let us briefly recall the proof. Let $\mathcal{O}_L$ be the ring of integers in L, and put $\mathfrak{P}_L = \mathfrak{P} \cdot \mathcal{O}_L$. It is enough to construct a G-<u>invariant</u> complete set of representative $\mathfrak{M}_L$ of $\mathcal{O}_L$ mod $\mathfrak{P}_L$. In fact, our assertion then follows immediately by using V-adic expansions with coefficients in $\mathfrak{M}_L$. Let $\mathfrak{M} \ni 0, 1$ be a complete set of representatives of $\mathcal{O}$ mod $\mathfrak{P}$. Let $\bar{\alpha} \in \bar{L}$, and let $x^n + \bar{a}_1 x^{n-1} + \ldots + \bar{a}_n = 0$ be the monic irreducible equation for $\bar{\alpha}$ over $\bar{K}$. For each i, let $a_i$ be the unique lifting of $\bar{a}_i$ in $\mathfrak{M}$. Then there exists a unique lifting $\alpha \in L$ of $\bar{\alpha}$ satisfying $\alpha^n + a_1\alpha^{n-1} + \ldots + a_n = 0$. The set $\mathfrak{M}_L = \{\alpha \mid \bar{\alpha} \in \bar{L}\}$ is a required G-invariant complete set of representatives.

By this (applied to any complete intermediate fields in place of K), we see that the Galois theory holds between closed subgroups H of $G_V$ and complete intermediate fields $M_V$ of $L_V/K$. If M is the fixed field of H in L, then $M_V$ coincides with its completion. By §§ 1-4, 5-2, the space of differentials, the differentiation d, and the valuation V can be extended uniquely to any complete unramified extension L of K. They preserve the conditions of § 5-1, and also $D^h(\mathcal{O}_L) = D^h(\mathcal{O}) \underset{\mathcal{O}}{\otimes} \mathcal{O}_L$. Let $\omega \in D^h(L)$, and put $\omega = y \cdot \xi$ with $y \in L$, $\xi \in D^h(K)$, $\xi \neq 0$. Then the smallest complete field containing K and y is independent of the above expression of $\omega$. We shall call this field <u>the field obtained by adjoining</u> $\omega$ <u>to</u> K, and denote it by $K(\omega)$.

(III) <u>Extending</u> $\sigma$ <u>to</u> L.

<u>Proposition 11</u> <u>Let</u> $\sigma$ <u>be a</u> q-th <u>Frobenius map of a complete field</u> K, <u>and let</u> L <u>be either an unramified extension of</u> K, <u>or the completion of an unramified extension of</u> K. <u>Then</u> $\sigma$ <u>can be extended uniquely to a</u> q-th <u>Frobenius map</u> $\sigma_L$ <u>of</u> L <u>into itself</u>. <u>Moreover</u>, <u>if</u> L/K <u>is normal</u>, <u>then</u> $\sigma_L$ <u>commutes with each element of the Galois</u>

group $\mathrm{Aut}_K L$.

Proof We may assume that $L/K$ is finite and normal. Take $x \in L$ such that $\bar{L} = \bar{K}(\bar{x})$. Then $L = K(x)$. Let $f(X) = \sum_{i=0}^{n} a_i X^i = 0$ be the monic irreducible equation for $x$ over $K$, and let $x = x_1, \ldots, x_n$ be the zeros of $f(X)$. Choose the subscripts of the zeros $y = y_1, \ldots, y_n$ of $f^{\sigma}(X)$ in such a way that $\bar{y}_i = \bar{x}_i^q$ holds for all $i$. If $\sigma_L$ is any extension of $\sigma$ to an isomorphism of $L$, then $\sigma_L(x)$ must be one of the $y_i$. Since $\bar{x}_i$ $(1 \le i \le n)$, and hence also $\bar{y}_i$ $(1 \le i \le n)$, are all mutually distinct, $\sigma_L$ cannot be a q-th Frobenius map unless $\sigma_L(x) = y$; hence the uniqueness. Now let $\sigma_L$ be the isomorphism of $L$ that extends $\sigma$ and that maps $x$ to $y$. The $\sigma_L$ preserves the valuation $V$, and the reduced map $\bar{\sigma}_L$ coincides with the q-th power map on $\bar{K}$ and also on $\bar{x}$; hence on $\bar{L}$. Since $\bar{L} = \bar{K}(\bar{x})$ and $\bar{L}/\bar{K}$ is separable, we have $\bar{L} = \bar{K}(\bar{y})$. Therefore, if we put $L' = K(y)$, then $n \ge [L':K] \ge [\bar{L}':\bar{K}] \ge [\bar{K}(\bar{y}):\bar{K}] = n$; hence $[L':K] = [\bar{L}':\bar{K}] = n$, and $\bar{L}' = \bar{L}$. Therefore, $L'/K$ is unramified, and $\bar{L}' = \bar{L}$; hence $L' = L$; i.e., $L = K(y)$. Therefore, $\sigma_L(L) \subset L$. That $\sigma_L$ commutes with the differentiation follows immediately. If $\varepsilon \in \mathrm{Aut}_K L$, then $\varepsilon \sigma_L \varepsilon^{-1}$ is also a q-th Frobenius map of $L$ extending $\sigma$; hence it coincides with $\sigma_L$. Q.E.D.

(IV) The differential $\omega$ in the general case Let $\sigma$ be a q-th Frobenius map of $K$. In general, $K$ may or may not contain the associated differential $\omega$. We shall extend the definition of $\omega$ to the general cases simply by considering the differentials in the bigger fields. Namely, in such cases, we take the maximum complete unramified extension L of the completion of K. Then $\sigma$ is uniquely extended to a q-th Frobenius map $\sigma_L$ of L, and L satisfies the assumption of Theorem 2A(ii). Hence $D(L)^{\times}$ contains a differential $\omega$ associated with $\sigma_L$. We call $\omega$ also the differential associated with $\sigma$. Then $\omega$ is a differential of L determined up to the non-zero multiples of elements of the constant field $\ell$ of L. On the other hand, the proof of Theorem 2A(ii) shows that $\omega^{\sigma}/\omega = c$ has a solution $\omega$ for any $c \in \ell^{\times}$ with $v(c) = \nu$. So, there exists some $\omega$ such that $\omega^{\sigma}/\omega \in k^{\times}$. To give a finer definition of $\omega$, we shall impose the conditions that $\omega^{\sigma}/\omega \in k^{\times}$ ( and not merely $\in \ell^{\times}$). Then, $\omega$ is determined up to such constant multiples $a \in \ell^{\times}$ that $a^{\sigma-1} \in k^{\times}$.

We note that the iterates $\sigma^n$ of $\sigma$ (defined in an obvious sense) associate the same differential $\omega$ as $\sigma$.

(V) <u>The field</u> $K(\omega)$ Suppose that K is complete. Let $\sigma$ be a q-th Frobenius map of K, and let c be an element of $k^{\times}$ with $v(c) = \nu$. Let $\omega$ be an associated differential, normalized by $\omega^{\sigma}/\omega = c$, in the completion L of the maximum unramified extension of K. Let $K(\omega)$ be the complete field obtained by adjoining $\omega$ to K (see (II)). Then we have the following:

Theorem 3 Assume that k is so large as to contain the fixed field of $\sigma|_{\ell}$, $\ell$ being the constant field of L. Then $K(\omega)$ is a complete unramified extension of K whose Galois group is abelian and topologically isomorphic to a subgroup of the v-unit group of k. The field $K(\omega)$ depends only on the Frobenius map $\sigma$ and the normalizing constant c.

Proof Let $\varepsilon \in G(L/K)$. Then $\varepsilon\sigma = \sigma\varepsilon$ (Proposition 11); hence $(\omega^{\varepsilon})^{\sigma} = c\,\omega^{\varepsilon}$. Therefore, by the uniqueness of $\omega$, $\omega^{\varepsilon}/\omega$ belongs to $\ell^{\times}$, and moreover is invariant by $\sigma$. Hence $\omega^{\varepsilon}/\omega \in k^{\times}$. Put $\chi(\varepsilon) = \omega^{\varepsilon}/\omega$. Then $\chi$ is a continuous homomorphism of G(L/K) into $\mathfrak{U}$, the v-unit group of k. But $K(\omega)$ is the fixed field of the kernel of $\chi$. (In fact, if we put $\omega = w\cdot\xi$ ($\xi \in D(K)^{\times}$), then $\omega^{\varepsilon} = \omega$ if and only if $w^{\varepsilon} = w$, and $K(\omega)$ is the complete field generated by K and w.) Therefore, $K(\omega)/K$ is a Galois extension, its Galois group being isomorphic to $\mathrm{Aut}_K L/\mathrm{Ker}\chi$. Since $\mathrm{Aut}_K L$ is compact, the induced map $\mathrm{Aut}_K L/\mathrm{Ker}\chi \rightarrow \mathrm{Image}(\chi)$ is a topological isomorphism. The last assertion follows immediately, since the fixed field of $\sigma|_{\ell}$ is contained in k. Q.E.D.

(VI) The fields $K(\omega)_n$. Assumptions being as in (V), put $G = \mathrm{Aut}_K K(\omega)$. Then $\chi: G \longrightarrow \chi(G) \subset \mathfrak{U}$ is a topological isomorphism. For each $n \geq 1$, put $\mathfrak{U}_n = \{u \in \mathfrak{U} \mid u \equiv 1 \pmod{\pi^n}\}$ ($\pi$: a prime element of v), and $G_n = \chi^{-1}(\mathfrak{U}_n)$. Then since $G_n$ is open, $G/G_n$ is finite. Let $K(\omega)_n$ be the fixed field of $G_n$, so that $K(\omega)_n/K$ is finite and abelian. Then it is easy to prove, by using the V-adic expansions with respect to the representatives $\mathcal{M}_L$ of (II), the following:

Proposition 12 Let the assumptions be as in (V) and as immediately above. Then $K(\omega)_n$ is the smallest unramified extension of K containing a differential $\omega_n$ satisfying $V(\omega_n) = 0$ and $c^{-1}\omega_n^{\sigma} \equiv \omega_n \pmod{\pi^n}$. Such $\omega_n$ is unique up to $\mathcal{U}\cdot\{1 + \pi^n \mathcal{O}_L\}$ multiples.

6-4 The reduced differential $\overline{\omega}$. Here, K is not assumed to be complete. Let $\sigma$ be a q-th Frobenius map of K. Fix $c \in k^{\times}$ with $v(c) = \nu$ ; $\nu = \nu(\sigma)$ being as in §6-1. Take any $\xi \in D(K)^{\times}$ with $V(\xi) = 0$, and put

$$\omega_* = c \cdot \xi^q / \xi^{\sigma} \qquad (\xi^q = \xi \otimes \cdots \otimes \xi \text{ ; q copies})$$

Then $\overline{\omega_*}$, which is a non-zero differential of $\overline{K}$ of degree q-1, is independent of $\xi$. Indeed, let z be any V-unit of K, and replace $\xi$ by $z \cdot \xi$. Then $\omega_*$ is simply multiplied by $z^q/z$ ; but since $\sigma$ is a q-th Frobenius map, we have $\overline{(z^q/z^{\sigma})} = 1$. Therefore, $\overline{\omega_*}$ remains unchanged.

On the other hand, we have defined a differential $\omega$ associated with $\sigma$. Normalize $\omega$ by the two conditions $\omega^{\sigma}/\omega = c$ and

$V(\omega) = 0$. Then, with the notations of §6-3 (IV), $\omega$ is determined up to multiples of such element $a \in \ell^{\times}$ that $a^{\sigma-1} = 1$ and $V(a) = 0$. Therefore, the reduction $\bar{\omega}$ of $\omega$ is determined up to multiples of elements of $\mathbb{F}_q^{\times}$. Hence its $(q-1)$-th power $\bar{\omega}^{q-1}$ is a (non-zero) differential of L of degree $q-1$, which is determined uniquely. Now we claim that

<u>Theorem 4</u> $$\bar{\omega}^{q-1} = \bar{\omega}_*.$$

(This shows in particular that $\bar{\omega}^{q-1}$ belongs to $\bar{K}$.)

The proof is immediate. In fact, put $\omega = y \cdot \xi$ ($y \in L^{\times}$, $\xi \in D(K)^{\times}$, $V(y) = V(\xi) = 0$. Then $\overline{\omega_*} = \overline{c \cdot \xi^q/\xi^{\sigma}} = \overline{c \cdot \omega^q/\omega^{\sigma}}$ $= \overline{\omega^{q-1}} = \bar{\omega}^{q-1}$.

<u>Thus</u>, $\bar{\omega}^{q-1}$ <u>is directly defined by Theorem 4, without looking at big extensions of</u> K, <u>and</u> $\bar{\omega}$ <u>is obtained by taking its</u> $(q-1)$-th <u>root in a finite separable extension of</u> $\bar{K}$. As can be checked immediately, <u>the field</u> $\bar{K}(\bar{\omega})$ <u>is nothing but the residue field of</u> $K(\omega)_1$.

Of course, $\bar{\omega}$ depends on the choice of the normalizing constant c. If c is unfixed, then $\bar{\omega}$ (resp. $\bar{\omega}^{q-1}$) is determined <u>up to</u> $\bar{k}^{\times 1/(q-1)}$-<u>multiples</u> (<u>resp</u>. $\bar{k}^{\times}$-<u>multiples</u>).

## §7 The $\sigma$-invariant S-operator and the differential $\omega$.

§7-1 V-integral S-operators We shall now consider some V-adic properties of S-operators of K. (See §1 for the definition and basic properties of the symbol $\langle\ ,\ \rangle$ and the S-operators.)

Proposition 13 $\langle \eta , \xi \rangle$ is V-integral for any $\xi, \eta \in D(K)^{\times}$.

Proof By Proposition 2 (§1-2), $\langle \eta , \xi \rangle$ remains unaltered if we replace $\eta$ or $\xi$ by their $k^{\times}$-multiples. So, we can assume $V(\eta) = V(\xi) = 0$. But then, $V(\eta/\xi) = 0$. Since $V(dx) \geq V(x)$ for any $x \in K$, our assertion follows immediately from the definition of $\langle \eta, \xi \rangle$. Q.E.D.

Corollary 1 Let S be an S-operator of K. Then $S\langle \xi \rangle$ is V-integral for all $\xi$ if and only if it is so for one $\xi$.

Proof $S\langle \eta \rangle - S\langle \xi \rangle = \langle \eta , \xi \rangle$, and Proposition 13. Q.E.D.

An S-operator S will be called V-integral if $S\langle \xi \rangle$ is so. All inner S-operators are V-integral.

Corollary 2 Let S be a V-integral S-operator of K, and let $\xi, \eta$ be V-integral differentials of K, with $\overline{\xi} = \overline{\eta} \neq 0$. Then $\overline{S\langle \xi \rangle} = \overline{S\langle \eta \rangle}$.

Proof Immediate, since $\overline{\langle \eta , \xi \rangle} = \langle \overline{\eta}, \overline{\xi} \rangle = 0$. Q.E.D.

Let S be a V-integral S-operator of K. Then its reduction $\overline{S}$, which is an S-operator of $\overline{K}$, will be defined by $\overline{S}\langle \overline{\xi} \rangle = \overline{S\langle \xi \rangle}$ (for any $\xi \in D(K)$ with $V(\xi) = 0$).

§7-2 The $\sigma$-invariant S-operator (I) Let $\sigma$ be a q-th Frobenius map of K. An S-operator S of K is said to be $\sigma$-invariant if $S\langle\xi\rangle^{\sigma} = S\langle\xi^{\sigma}\rangle$ holds for all (or equivalently, one) $\xi \in D(K)^{\times}$.

Theorem 5 Let $\sigma$ be a q-th Frobenius map of K. Then, (i) a $\sigma$-invariant S-operator S of K is at most unique, (ii) S is V-integral, (iii) S exists if K is complete.

Proof Take any $\zeta \in D(K)^{\times}$. Then, the S-operators of K are of the form $S\langle\xi\rangle = \langle\xi, \zeta\rangle + C$, C being an arbitrary constant of $D^2(K)$. With this expression, S is $\sigma$-invariant if and only if $\langle\zeta, \zeta^{\sigma}\rangle = C - C^{\sigma}$. Hence (i) and (iii) are immediate consequences of the Corollary of Proposition 9 (§6-1). To check (ii), let x be a regular element of K, and put $S\langle dx\rangle = y(dx)^2$ $(y \in K)$. If $y = 0$, then there is no problem; so assume $y \neq 0$. We have $S\langle dx\rangle^{\sigma} - S\langle dx\rangle = S\langle dx^{\sigma}\rangle - S\langle dx\rangle = \langle dx^{\sigma}, dx\rangle$; hence by Proposition 13, this differential is V-integral; hence $y^{\sigma}(dx^{\sigma}/dx)^2 - y$ is V-integral. But $V(y^{\sigma}) = V(y)$ and $V(dx^{\sigma}/dx) = \nu > 0$ (Proposition 9); hence y must be V-integral. This settles (ii). Q.E.D.

(II) Here, we note that <u>an</u> S-<u>operator of</u> K <u>can be extended uniquely to that of</u> L, <u>where</u> L <u>is either a separable extension or the completion of</u> K. The first case is already explained in §1-4, and the same argument applies to the second case. Indeed, let S be an S operator of K, and take any $\xi \in D(L)^{\times}$ and $\zeta \in D(K)^{\times}$. Then, the formula $S_L\langle\xi\rangle = \langle\xi, \zeta\rangle + S\langle\zeta\rangle$ defines an S operator $S_L$ of L (independently of $\zeta$). It is clear that $S_L$ is the unique S operator of L which extends S.

So, an S-operator of K can be extended uniquely to that of the completion of K, an unramified extension of K, or the towers of such extensions (e.g., a complete unramified extension of the completion of K). Since each such extension of S is unique, we shall always identify it with S, and denote it also by S (instead of $S_L$). Note that the V-integrality and the $\sigma$-invariance properties of S are preserved by each of such extensions.

(III) If K contains an associated differential $\omega$, then the S-operator of K defined by

$$S\langle\omega\rangle = 0$$

is the (unique) $\sigma$-invariant S-operator of K. Indeed, $S\langle\xi\rangle = \langle\xi, \omega\rangle$ ($\xi \in D(K)^{\times}$), so that $S\langle\xi\rangle^{\sigma} - S\langle\xi^{\sigma}\rangle = \langle\omega^{\sigma}, \omega\rangle = \langle c\omega, \omega\rangle = 0$. Let us look at this very simple fact from the reverse side, since we are often given a $\sigma$-invariant S-operator without knowing $\omega$. Thus, it is somewhat useful to state the following theorem.

Theorem 6 *Let $\sigma$ be a q-th Frobenius map of a complete field K, and let S be the unique $\sigma$-invariant S-operator of K. Then the equation $S\langle\omega\rangle = 0$ has a solution $\omega$ in a certain complete unramified extension $K(\omega)$ of K. Let L be the maximum complete unramified extension of K and let $\ell$ be the algebraic closure of k in L. Then if $\bar{k}$ is perfect, $\omega$ is a unique solution of $S\langle\omega\rangle = 0$ in $D(L)^{\times}$, up to $\ell^{\times}$-multiples.*

Proof It is enough to take the associated differential $\omega$ in L (see §6-3(IV)). The uniqueness is a direct consequence of Propostion 2 (ii) (§1-2) and Proposition 10 (§6-2). Q.E.D.

Remark The V-integrality of a $\sigma$-invariant S-operator S (Theorem 5(ii)) can also be deduced immediately from the fact that S is inner with respect to $\omega$, But then, we must use big field extensions. This is why an alternative proof is given.

Remark Let S be a $\sigma$-invariant S-operator. Then the solution of $S\langle\omega\rangle = 0$ generally exists only in a big extension of K. On the other hand, the equation $S\langle\zeta_n\rangle \equiv 0 \pmod{\pi^n}$ has a solution

$\zeta_n \in D(K)^\times$ for any n. Indeed, take any $\zeta \in D(K)^\times$ and put $\zeta_n = a_n \cdot \zeta^{\sigma^n}$ ($a_n \in k^\times$). Then $S\langle \zeta_n \rangle = S\langle \zeta \rangle^{\sigma^n} \equiv 0 \pmod{\pi^{2\nu n}}$ by Proposition 9 (and by the V-integrality of S). Note that one may choose $a_n$ in such a way that $V(\zeta_n) = 0$. The point is that, in general, such "partial solutions" $\zeta_n$ cannot be chosen to be convergent (even if K is complete). In any case, $\overline{S}$ must always be an inner S-operator of $\overline{K}$, which, as a necessary condition for the $\sigma$-invariance of S, is not totally useless.

7-3 Digression; the Cartier operator $\gamma$. In §7-3, and only in this section, we are released from the previous notations and assumptions. Here, $\overline{k}$ will denote any perfect field of characteristic $p > 0$, and $\overline{K}$ will denote any (finitely or infinitely generated) dimensional regular extension of $\overline{k}$, i.e., such an extension as that satisfying $\dim_{\overline{k}}(\overline{K}) = 1$, $\overline{k}$ : algebraically closed in $\overline{K}$, and $\overline{K}/\overline{k}$ : separably generated. Let $D(\overline{K})$ be a one-dimensional vector space over $\overline{K}$. A differentiation $\overline{d} : \overline{K} \longrightarrow D(\overline{K})$ (see §1-1) will be called a differentiation of $\overline{K}/\overline{k}$, if it is trivial on $\overline{k}$, i.e., if its constant field $\{\alpha \in \overline{K} \mid \overline{d}\alpha\} = 0$ contains $\overline{k}$. It follows easily from our assumptions that the differentiations $\overline{d}$ of $\overline{K}/\overline{k}$ form a one dimensional vector space over $\overline{K}$, and that if $\overline{d} \neq 0$, then its constant field coincides with $\overline{K}^p$.

Now, fix any non-zero differentiation $\bar{d}$ of $\bar{K}/\bar{k}$. Then <u>the Cartier operator of</u> $\bar{K}/\bar{k}$ <u>with respect to</u> $\bar{d}$ is the unique map $\gamma$ of $D(\bar{K})$ into itself, satisfying the following conditions ($\gamma 1$)$\sim$($\gamma 3$):

($\gamma 1$) $\gamma$ is <u>semi-linear</u>, i.e.,

$$\gamma(\xi + \eta) = \gamma(\xi) + \gamma(\eta)$$

<u>and</u>

$$\gamma(\alpha^{p} \cdot \xi) = \alpha \cdot \gamma(\xi)$$

<u>for any</u> $\xi, \eta \in D(\bar{K})$, $\alpha \in \bar{K}$.

($\gamma 2$) $\gamma(\xi) = 0$ <u>if</u> $\xi$ <u>is exact</u>, <u>i.e.</u>, <u>if</u> $\xi = \bar{d}\alpha$ <u>with some</u> $\alpha \in \bar{K}$.

($\gamma 3$) $\gamma(\xi) = \xi$ <u>if</u> $\xi$ <u>is logarithmically exact</u>, <u>i.e., if</u> $\xi = \alpha^{-1}\bar{d}\alpha$ <u>with some</u> $\alpha \in \bar{K}^{\times}$.

The unique existence of $\gamma$ is proved in P. Cartier [ ]. It is also proved there that the converses of ($\gamma 2$) and ($\gamma 3$) are valid. Note that for $\alpha \in \bar{K}^{\times}$, the Cartier operator of $\bar{K}/\bar{k}$ with respect to $\alpha \cdot \bar{d}$ is given by $\alpha \cdot \gamma \cdot \alpha^{-1}$. Let $\bar{L}$ be any separable extension of $\bar{K}$, let $D(\bar{L}) = D(\bar{K}) \otimes_{\bar{K}} \bar{L}$, and let $\bar{d}_{\bar{L}} : \bar{L} \to D(\bar{L})$ be the unique extension of $\bar{d}$ to $\bar{L}$ (see §1-4). Let $\bar{\ell}$ be the algebraic closure of $\bar{k}$ in $\bar{L}$, so that $\bar{\ell}$ is perfect, and $\bar{L}/\bar{\ell}$ is also one-dimensional and regular. Clearly, $\bar{d}_{\bar{L}}$ is a differentiation of $\bar{L}/\bar{\ell}$. Let $\gamma_{\bar{L}}$ be the Cartier operator of $\bar{L}/\bar{\ell}$ with respect to $\bar{d}_{\bar{L}}$. Then it can be checked immediately that $\gamma_{\bar{L}}$ coincides with $\gamma$ on $D(\bar{K})$.

Lemma 2 Let $\alpha \in \bar{K}^{\times}$, and $r \geq 0$. Then

$$\gamma(\alpha^{p^r - 1}\bar{d}\alpha) = \alpha^{p^{r-1}-1}\bar{d}\alpha \qquad \ldots \quad r \geq 1,$$

$$= 0 \qquad \ldots \quad r = 0.$$

Proof Immediate, by ($\gamma$2), ($\gamma$3). Q.E.D.

Corollary Let $\alpha_1, \cdots, \alpha_n$ be elements of $\bar{K}$ not contained in $\bar{K}^p$, and let $r_1 > \cdots > r_n \geq 0$. Then the differentials $\alpha_i^{p^{r_i}-1}\bar{d}\alpha_i$ are linearly independent over $\bar{k}$.

Proof This follows immediately from the lemma, by using the iterates of $\gamma$. Q.E.D.

§7-4 A characterization of $\bar{\omega}$ by $\bar{S}$ and $\gamma$. (I) Now we come back to the notations and assumptions of §§1-1, 5-1. But now, we assume further; namely that $\bar{K}/\bar{k}$ is one-dimensional, that $\bar{k}$ is perfect, and that $\bar{k}$ is algebraically closed in $\bar{K}$. It follows from our assumptions that $\bar{K}/\bar{k}$ is separably generated. In fact, let x be a regular element of K (see § 5-1). Then $\bar{d}\bar{x} \neq 0$; hence $\bar{x} \notin \bar{k}$, which implies that $\bar{x}$ is transcendental over $\bar{k}$. But then, $\bar{K}/\bar{k}(\bar{x})$ is algebraic. Since $\bar{d}\bar{x} \neq 0$, we conclude that $\bar{K}/\bar{k}(\bar{x})$ must be separable. Therefore, $\bar{K}/\bar{k}$ is separably generated. Note that this is not a consequence of the perfectness assumption of $\bar{k}$, since $\bar{K}/\bar{k}$ may be infinitely generated. At any rate, $\overline{K}/\overline{k}$ satisfies the assumptions of §7-3.

Let $\alpha \in \overline{K}$. Then $\bar{d}\alpha = 0$ if and only if $\alpha \in \overline{K}^p$. On the other hand, $\overline{K}/\overline{k}$ is separably generated. Therefore, any element $\alpha \in \overline{K}$ not contained in $\overline{k}$ can be expressed as $\alpha = \beta^{p^r}$ ($\beta \in \overline{K}$, $r \geq 0$) with $\bar{d}\beta \neq 0$. Let $K_V$ be the completion of K, and let $y \in K_V$. Then y has a V-adic expansion of the form

$$(*) \qquad y = \sum_{i\in I} y_i^{p^{r_i}} \pi^i + \sum_{j\in J} c_j \pi^j,$$

where $\pi$ is a prime element of v, I and J are disjoint sets of integers (containing only finitely many negative ones), $y_i$ are regular elements of K, $r_i \geq 0$, and $c_j$ are v-units of k. The following Proposition is somewhat noteworthy:

<u>Proposition 14</u> <u>The constant field of</u> $K_V$ <u>coincides with the</u> V-<u>adic closure of</u> k <u>in</u> $K_V$.

<u>Proof</u> Let $k_V$ and $k_V'$ be the constant field of $K_V$ and the V-adic closure of k in $K_V$, respectively. The inclusion $k_V' \subset k_V$ being trivial, we shall prove $k_V \subset k_V'$. Let $y \in k_V$, and let (*) (above) be its V-adic expansion. Suppose $I \neq \emptyset$. Put $e = v(p)$, $r = \operatorname{Min}_{i\in I}\{i + er_i\}$, and $I_0 = \{ i \in I \mid i + er_i = r\}$. Then we obtain, by differentiating (*),

$$\sum_{i\in I_0} \bar{a}_i \bar{y}_i^{p^{r_i}-1} \cdot \bar{d}\bar{y}_i = 0 \qquad (\bar{a}_i \in \bar{k}^\times),$$

which is a contradiction to the Corollary of Lemma 2 (§7-3), since $\overline{dy_i} \neq 0$ for $i \in I$. Therefore, $I = \emptyset$. But then $y \in k'_V$. <u>Q.E.D.</u>

(II) Now let $q = p^f$, and let $\sigma$ be a q-th Frobenius map of K. Take $c \in k^{\times}$ with $v(c) = \nu$ ($= \nu(\sigma)$; see §6-1), and let $\omega$ be an associated differential, normalized by the two conditions $\omega^{\sigma}/\omega = c$ and $V(\omega) = 0$. Let $\overline{\omega}$ be the reduction of $\omega$.

<u>Theorem 7</u> <u>We have</u>

$$\gamma^f(\overline{\omega}) = \overline{a}\cdot\overline{\omega},$$

<u>where</u> $\overline{a} = \overline{(qc^{-1})} \in \overline{k}$. <u>If</u> $q = p$ <u>and</u> $v(p) = 1$, <u>then</u> $\overline{a} \neq 0$.

<u>Proof</u> Let x be a regular element of K, and $\pi$ be a prime element of v. Then $x^{\sigma} \equiv x^q \pmod{\pi}$, and hence $x^{\sigma}$ has a following V-adic expansion (see (I) above):

$$x^{\sigma} = x^q + \sum_{i \in I} x_i^{p^{r_i}} \pi^i + \sum_{j \in J} c_j \pi^j,$$

where I and J are disjoint sets of positive integers, $x_i$ are regular elements of K, $r_i \geq 0$, and $c_j$ are v-units of k. By differentiating this, we obtain

$$dx^{\sigma} = qx^{q-1}dx + \sum_{i \in I} \pi^i p^{r_i} x_i^{p^{r_i}-1} dx_i .$$

Put $e = v(p)$, $r = \underset{i\in I}{\mathrm{Min}}\{i + er_i\}$, and $r_0 = \mathrm{Min}\{ef, r\}$. Take any $c_1 \in k^\times$ with $v(c_1) = r_0$, put $\xi = c_1^{-1}dx^\sigma$, and let $I_0$ be the finite subset of I consisting of all $i \in I$ such that $i + er_i = r_0$. Then $I_0 \neq \phi$ if and only if $r \leq ef$, and we have

$$(**) \qquad \bar{\xi} = \bar{a}\bar{x}^{q-1}\overline{dx} + \sum_{i\in I_0} \bar{a}_i \bar{x}_i^{p^{r_i}-1}\overline{dx}_i,$$

with $\bar{a}_i \in \bar{k}^\times$ and $\bar{a} = \overline{(qc_1^{-1})} \in \bar{k}$; hence $\bar{a} \neq 0$ if and only if $ef \leq r$. Since $\overline{dx}, \overline{dx}_i \neq 0$, we conclude by (**) with the use of the Corollary of Lemma 2 (§7-3) that $\bar{\xi} \neq 0$. Therefore, $r_0 = \nu$. On the other hand, by operating $\gamma^f$ on both sides of (**), we obtain by Lemma 2:

$$\gamma^f(\bar{\xi}) = \bar{a}\,\overline{dx}.$$

Since $r_0 = \nu$, we may now put $c_1 = c$. Then, $\bar{\omega}^{q-1} = (\overline{dx})^q/\bar{\xi}$ by Theorem 4(§6-4); hence $\bar{\omega} = (\bar{\xi}/\overline{dx})^{q/1-q} \cdot \bar{\xi}$. Hence $\gamma^f(\bar{\omega}) = (\bar{\xi}/\overline{dx})^{1/1-q} \cdot \gamma^f(\bar{\xi}) = \bar{a}\,(\bar{\xi}/\overline{dx})^{1/1-q} \cdot \overline{dx} = \bar{a}\,\bar{\omega}$. On the other hand, $\bar{a} = \overline{(qc^{-1})}$. If $q = p$ and $v(p) = 1$, then $ef = 1 \leq r$; hence $\bar{a} \neq 0$.

Q.E.D.

In the case where $q = p$ and $v(p) = 1$, we have $\nu(\sigma) = r_0 = 1$; hence <u>one may normalize</u> $\omega$ <u>further by imposing</u> $\omega^\sigma/\omega = p$. Then $\bar{\omega}$ is given by

$$(***) \qquad \bar{\omega} = \left(\overline{x^{p-1} + \frac{dR}{dx}}\right)^{\frac{-1}{p-1}} \cdot \overline{dx},$$

where R is a V-integer of K such that

$$x^{\sigma} \equiv x^{p} + pR \pmod{p^2}.$$

Since q = c = p, we have $\bar{a} = 1$ in this case; i.e.,

$$\gamma(\bar{\omega}) = \bar{\omega}.$$

(III) The proof of Theorem 7 tells us that $\bar{\omega}$ can be expressed explicitly by means of $x_i$ and $r_i$ for $i \in I_0$. Hence if one has a sufficient knowledge about the expansion of $x^{\sigma}$, then one is able to compute $\bar{\omega}$; for instance, by the above formula (***) in the case of q = p and v(p) = 1. But in the theoretically interesting cases, one does not have a sufficient knowledge about the expansion of $x^{\sigma}$. Instead, one is often provided with a good knowledge about the $\sigma$-invariant S-operator S. Recall that if S is a $\sigma$-invariant S-operator of K, then $S\langle\omega\rangle = 0$, S is V-integral, and hence also $\bar{S}\langle\bar{\omega}\rangle = 0$ (see §7-2). Thus, the following characterization of $\bar{\omega}$ is useful for its explicit calculations.

Theorem 8 Suppose that p is a prime element of v, and let $\sigma$ be a p-th Frobenius map of K. Let S be the $\sigma$-invariant S-operator of the completion $K_V$ of K, so that S is V-integral and $\bar{S}$ is an S-operator of $\bar{K}$ (§§7-1,2). Let $\omega$ be an associated differential (§6-3(IV)), normalized by the two conditions $\omega^{\sigma}/\omega = p$, $V(\omega) = 0$. Let $\bar{\omega}$ be the reduction of $\omega$, so that $\bar{\omega}$ is a *differential of a separable extension of* $\overline{K}$, *which is intrinsic up to* $\mathbb{F}_p^\times$*-multiples*. *Then* $\overline{\omega}$ *satisfies*

$$\text{(i)} \qquad \overline{S}\langle\overline{\omega}\rangle = 0,$$

*and*

$$\text{(ii)} \qquad \gamma(\overline{\omega}) = \overline{\omega},$$

$\gamma$ *being the Cartier operator*.

*Conversely, if* $\overline{L}$ *is the separable closure of* $\overline{K}$, *then the two equations* (i) *and* (ii) *for the differentials* $\overline{\omega} \in D(\overline{L})^\times$ *determine* $\overline{\omega}$ *uniquely up to* $\mathbb{F}_p^\times$*-multiples, and thus characterize the reduced associated differential*.

*Remark* The condition (ii) is equivalent to the logarithmical exactness of $\overline{\omega}$ (in $\overline{K}(\overline{\omega})$, and also in $\overline{L}$; see §7-3).

*Proof* It remains to prove the converse. Take any $\overline{\omega}' \in D(\overline{L})^\times$ satisfying $\overline{S}\langle\overline{\omega}'\rangle = 0$ and $\gamma(\overline{\omega}') = \overline{\omega}'$. Put $\overline{\omega}' = \alpha\overline{\omega}$ ($\alpha \in \overline{L}$). We shall show that $\alpha \in \mathbb{F}_p^\times$. First, since $\gamma(\overline{\omega}) \neq 0$, $\overline{\omega}$ is non-exact in $\overline{L}$. On the other hand, $\langle\overline{\omega}',\overline{\omega}\rangle = S(\overline{\omega}') - S\langle\overline{\omega}\rangle = 0$. Therefore, by Proposition 2 (§1-1), we conclude $\overline{\omega}'/\overline{\omega} \in \mathrm{Ker}(\overline{d}) = \overline{L}^p$. Therefore, $\alpha = \beta^p$ ($\beta \in \overline{L}$). But then, $1 = \gamma(\overline{\omega}')/\overline{\omega}' = \beta^{1-p}\cdot\gamma(\overline{\omega})/\overline{\omega} = \beta^{1-p}$; hence $\beta^{p-1} = 1$. Therefore, $\alpha = \beta^p \in \mathbb{F}_p^\times$.

Q.E.D.

## §8 Theory of $\omega$ under the weak congruence relation

§8-1 The weak congruence relation (I) Let k be a field with a non-trivial discrete valuation v, additive and normalized. Let $\bar{k}$ be the residue field. We assume that $ch(k) = 0$, $ch(\bar{k}) = p > 0$, and that $\bar{k}$ is algebraic over the prime field $\mathbb{F}_p$.

Let $\mathcal{C}$ be a complete non-singular irreducible algebraic curve, and $\mathcal{X}$ be a closed irreducible algebraic curve on $\mathcal{C} \times \mathcal{C}$ considered as an algebraic correspondence of $\mathcal{C}$, both defined over k. Let $q = p^f$ be a positive power of p. We shall assume that:

(i) $\bar{\mathcal{C}}$ is a good reduction of $\mathcal{C}$;

(ii) (the weak congruence relation): $\bar{\mathcal{C}}^q = \bar{\mathcal{C}}$, and $\bar{\mathcal{X}}$ contai the q-th power correspondence

$$\Pi = \{ \zeta \times \zeta^q \mid \zeta \in \bar{\mathcal{C}} \}$$

as a simple component.

Here, in general, $\bar{*}$ denotes the reduction mod v of $*$. We say that $\bar{\mathcal{C}}$ is a good reduction of $\mathcal{C}$, if $\mathcal{C}$ has a structure of a v-variety and is v-simple in the sense of Shimura [ ].

(II) Here, we shall discuss some immediate consequences of our assumptions. Let K be the field of k-rational functions on $\mathcal{C}$. We shall show that the above assumptions give rise to a discrete valuation V of K satisfying the assumptions of §5-1, and a q-th

Frobenius map $\sigma$ of K. Let P and $\bar{P}$ be generic points of $\mathcal{C}$ and $\bar{\mathcal{C}}$ over k and $\bar{k}$, respectively. Take $Q \in \mathcal{C}$ such that $P \times Q \in \mathfrak{X}$. (By the weak congruence relation, $\mathfrak{X}$ cannot be of the form $P_0 \times \mathcal{C}$ (nor of $\mathcal{C} \times Q_0$); hence this is possible.) Then $P \times Q$ is a generic point of $\mathcal{C}$ over k. Let $\bar{P}^q$ denote the image of $\bar{P}$ under the q-th power correspondence $\Pi$, so that $\bar{P} \times \bar{P}^q$ is a generic point of $\Pi$ over $\bar{k}$. Put $L = k(P, Q)$, and identify K with k(P). Let $\mathcal{O}_L$ be the specialization ring of $P \times Q \to \bar{P} \times \bar{P}^q$. Then, since $\Pi$ is a simple component of $\bar{\mathfrak{X}}$, we conclude that $\mathcal{O}_L$ is a discrete valuation ring in L, and that the corresponding discrete valuation $V_L$ has the same group as $v = V_L|_k$. These are immediate consequences of [ ] (Th. 15, its Coroll. 2, and Prop. 5). Accordingly, the restriction V of $V_L$ to K satisfies the assumption of §5-1 on the value groups (i.e., $V(K^\times) = v(k^\times)$). Let D(K) be the space of differentials of K/k, and let $d : K \to D(K)$ be the usual differentiation. Then, since $\mathcal{C} \to \bar{\mathcal{C}}$ is a good reduction, d is V-continuous. Hence the assumptions of §5-1 are satisfied for K, V and d. Now, the residue fields of K and L coincide; indeed, $\bar{K} = \bar{L} = \bar{k}(\bar{P})$. Since V and $V_L$ have the same value groups, this implies that K is $V_L$-adically dense in L. Accordingly, L may be considered as a subfield of the V-adic completion $K_V$ of K. Since $\mathfrak{X}$ cannot be of the form $\mathcal{C} \times Q_0$, Q is also a generic point of $\mathcal{C}$ over k; hence there is a unique isomorphism of K into L (over k) that maps P to Q. Call it $\sigma$. Then $\sigma$ maps the specialization ring of $P \to \bar{P}$ to that of $Q \to \bar{P}^q$, and hence leaves $V_L$ invariant, and moreover induces the q-th power isomorphism of the residue field $\bar{K}$. On the other hand, $\sigma$ commutes with the differentiation d. Therefore, $\sigma$ is a q-th Frobenius map of K.

$$\begin{tikzcd}[column sep=small]
 & L = k(P, Q) \subset K_V \arrow[dl, dash] \arrow[dr, dash] & \\
K = k(P) \arrow[rr] \arrow[dr, dash] & & K^{\sigma} = k(Q) \arrow[dl, dash] \\
 & k &
\end{tikzcd}
\qquad\qquad
\begin{array}{c}
\bar{L} \\ \| \\ \bar{K} \\ | \\ \bar{K}^q \\ | \\ \bar{k}
\end{array}$$

Note that $\bar{k}$ is algebraically closed in $\bar{K}$, since $\bar{\mathcal{C}}$ is a good reduction of $\mathcal{C}$.

§8-2 <u>The ramification conditions</u>. (I) In addition to (i), (ii) ( §8-1), we shall assume the following condition (iii). It is in essence a condition on the ramifications of some covering maps related to $\mathcal{C}$ and $\mathcal{X}$ (see (II) below), but it can be formulated more simply by using fuchsian groups, as:

(iii) $\mathcal{C}$, $\mathcal{X}$ <u>are those obtained in</u> §3-1 (II).

Namely, we assume that k is embedded into $\mathbb{C}$, and that there is a fuchsian group of the first kind $\Delta$ and an element

$\varepsilon \in G_{\mathbb{R}} = PSL_2(\mathbb{R})$ with the following properties: $\Delta$ and $\varepsilon^{-1}\Delta\varepsilon$ are commensurable and generate a dense subgroup of $G_{\mathbb{R}}$, and $\mathcal{C}$, $\mathfrak{X}$ are algebraico-geometric models of $\Delta\backslash H$, $\Delta\cap\varepsilon^{-1}\Delta\varepsilon\backslash H$ respectively. The embedding of $\mathfrak{X}$ into $\mathcal{C}\times\mathcal{C}$ is the one defined by the embedding $\tau \to \tau \times \varepsilon\tau$ of $\Delta\cap\varepsilon^{-1}\Delta\varepsilon\backslash H$ into $\Delta\backslash H \times \Delta\backslash H$.

The condition (iii) is for the existence of a natural and sometimes calculable $\sigma$-invariant S-operator of K. Indeed, let S be the canonical S-operator of $\mathcal{C}$ with respect to $\Delta$. Then S is k-rational by the Corollary of Theorem 1A (§3-1). Hence it can be considered as an S-operator of K. Let $\xi \in D(K)^{\times}$. Then $S\langle\xi\rangle^{\sigma} - S\langle\xi\rangle = \langle d\tau, d\tau^{\varepsilon}\rangle = 0$, since $\tau^{\varepsilon}$ is a linear fractional function of $\tau$ (see Proposition 2, § 1-2). Therefore, S is $\sigma$-invariant (in the sense of §7-2).

We note here that the density condition for the subgroup of $G_{\mathbb{R}}$ generated by $\Delta$ and $\varepsilon^{-1}\Delta\varepsilon$ is actually superfluous. In fact, it follows automatically from the weak congruence relation. But we will not stop here for the verification.

(II) We shall give another formulation of (iii). Let $\mathcal{C}_0$ be a complete non-singular model of $\mathfrak{X}$ over k. For each i = 1, 2, let $pr_i : \mathcal{C}_0 \to \mathcal{C}$ be the covering map corresponding to the projection of $\mathfrak{X}$ to the i-th component of $\mathcal{C}\times\mathcal{C}$. Let g be the genus of $\mathcal{C}$, and let P run over all points of $\mathcal{C}$. For each $R \in \mathcal{C}_0$, let $\rho_i(R)$

denote the ramification index of the covering map $pr_i$ at R (i = 1, 2)

Then, (iii) is equivalent to:

(iii)' *there is a* $\mathbb{Z}^+ \cup (\infty)$-*valued function* e *on* $\mathcal{C}$ *such that* e(P) = 1 *for almost all* P, *that*

(#) $$2g - 2 + \sum_P (1 - 1/e(P)) > 0,$$

*and that the quotients*

($\flat$) $$e(pr_i(R))/\ \rho_i(R) \qquad (i = 1, 2)$$

*are independent of* i, *and are integral (if finite).* *Moreover, the two coverings* $pr_1$, $pr_2$ *are "essentially different," in the sense that there is no algebraic curve* $\mathcal{C}'$ *and rational maps* $f_i : \mathcal{C} \to \mathcal{C}'$ (i = 1, 2) *such that* $f_1 \circ pr_1 = f_2 \circ pr_2$.

This last condition corresponds to the density condition (in (iii)) of the subgroup of $G_{\mathbb{R}}$ generated by $\Delta$ and $\varepsilon^{-1} \Delta \varepsilon$. We shall leave the verification of the equivalence of (iii) and (iii)' to the readers. See § 2-2 for the one-to-one correspondence $\Delta \leftrightarrow \{\mathcal{C}, e\}$, and note that the assumptions of § 8-2 on the field k implies $\overline{\overline{k}} \leq \aleph$, and hence that k can be embedded into $\mathbb{C}$.

Finally, we note that the function e in (iii)' is actually unique. But this will not be used, and the proof will be omitted. It is reduced to some properties of a certain family of subgroups of a fuchsian group.

8-3 The Main Theorem 1. By applying our results of §§6~7 to the present case, we obtain the following Main Theorem 1. Our assumptions in this theorem are (i) (ii) (§8-1 (I)), and (iii) (§8-2 (I)). Before stating the theorem, we recall the following natations:

$K$ : the field of k-rational functions on $\mathcal{C}$;

$V$ : the (additive) discrete valuation of $K$ whose valuation ring is the specialization ring of the reduction $\mathcal{C} \to \overline{\mathcal{C}}$ ;

$K_V$ (resp. $k_v$) : the V-adic completion of $K$ (resp. the v-adic completion of k);

$K_V^\infty$ (resp. $k_v^\infty$) : the completion of the maximum unramified extension of $K_V$ (resp. $k_v$);

$* \to \overline{*}$ : the reduction mod $V$;

$D(*)^\times$ : the set of non-zero differentials of the field $*$;

$\gamma$ : the Cartier operator;

$S$ : the canonical S-operator of $\mathcal{C}$ w.r.t. $\Delta$.

Recall that $S$ is by definition the unique S-operator of $\mathcal{C}$ such that $S\langle d\tau\rangle = 0$, where $\tau$ is the inverse of the covering map $\mathbb{H} \to \Delta\backslash\mathbb{H} \cong \mathcal{C}$ (see §2).

Main Theorem 1 (i) The canonical S-operator S is k-rational. So, S will henceforth be considered as an S-operator of K.

(ii) S is moreover V-integral.

So, we can consider its reduction mod V, denoted by $\overline{S}$ (see §7-1).

(iii) The equation $S\langle\omega\rangle = 0$ has a V-adic solution $\omega$ in $D(K_V^{\infty})^{\times}$, which is unique up to $(k_V^{\infty})^{\times}$-multiples. This differential $\omega$ is non-exact in $K_V^{\infty}$.

(iv) If $\omega$ is suitably normalized and k is so taken that $\overline{k} \supset \mathbb{F}_q$, then the Galois group of $K_V(\omega)/K_V$, in the sense of §6-3, is abelian and is isomorphic to a closed subgroup of the v-unit group of $k_v$.

(v) Normalize $\omega$ to be a V-unit. Then, $\overline{\omega}^{q-1}$ is a non-zero differential (of degree q-1) of $\overline{K}$, intrinsic up to $\overline{k}^{\times}$-multiples; and $\overline{\omega}$ satisfies the two equations:

$$\overline{S}\langle\overline{\omega}\rangle = 0, \qquad \gamma^{f}(\overline{\omega}) = \overline{a}\,\overline{\omega} \qquad (\overline{a} \in \overline{k}).$$

(vi) If $f = 1$ (i.e., $q = p$) and $v(p) = 1$, we can normalize $\omega$ further in a certain manner (§7-4 (II)). This normalization determines $\overline{\omega}^{p-1}$ uniquely, and hence $\overline{\omega}$ up to $\mathbb{F}_p^{\times}$-multiples. The differential $\overline{\omega}$ satisfies the above two equations with $f = 1$, $\overline{a} = 1$, and is moreover characterized by these two equations.

Proof  We have checked (i) and the $\sigma$-invariance of S (§8-2(I)). Since $\sigma$ is a q-th Frobenius map (§8-1 (II)) of K, (ii) is a special case of Theorem 5 (ii) (§7-2). After extending the differentials, the differentiation d, the Frobenius map $\sigma$, and the S-operator S of K to $K_V$, and further to $K_V^{\infty}$ (see §§5-2, 6-3, 7-2 (II)), apply Theorem 6 (§7-2) to conclude (iii), and Theorem 3 (§6-3(V)) to conclude (iv). Here, note the following. By Proposition 14 (§7-4), the constant field of $K_V$ is $k_v$, and that of $K_V^{\infty}$ is $k_V^{\infty}$. On the other hand, if $\bar{k} \supset \mathbb{F}_q$, then the Galois group of $k_V^{\infty}/k_v$ is contained in the group topologically generated by $\sigma|_{k_V^{\infty}}$. Therefore, the $\sigma$-invariant elements of $k_V^{\infty}$ must belong to $k_V$ (cf. the argument of §6-3(II)), and hence the assumptions of Theorem 3 are satisfied. The assertions (v), (vi) follow immediately from Theorems 7, 8 (§7-4).  Q.E.D.

§8-4 V-integrality of S for the Morita's models. We shall keep the notations of §3-3 including those used in the proof of Theorem 10. The Shimura models $\mathcal{E}$ for $_{\Delta}\mathbb{H}$ are unique up to biregular morphisms over k ([ ]). It is probable that among the Shimura models $\mathcal{E}$, there exists such a nice model $\mathcal{E}^*$ as would satisfy the following conditions.

($\mathcal{C}^*1$) $\mathcal{C}^*$ has a good reduction $\overline{\mathcal{C}}^*$ at every prime divisor $\mathfrak{P}$ of $k = C(F, \mathfrak{t})$ not dividing $\mathfrak{t}\cdot D(B/F)$.

($\mathcal{C}^*2$) For each such $\mathfrak{P}$, let $\mathfrak{p}$ be its restriction to F, and let $\varepsilon$ be an element of $\Delta^{(\mathfrak{p})}$ such that $\eta_{\mathfrak{p}}(\varepsilon) \notin GL_2(\mathcal{O}_{\mathfrak{p}})$. Let $\mathfrak{X}$ be the algebraic correspondence of $\mathcal{C}^*$ defined with respect to this $\varepsilon$ (§3-1(II), §8-2(I)). Then the reduction $\overline{\mathfrak{X}}$ of $\mathfrak{X}$ modulo $\mathfrak{P}$ contains a $q^d$-th power correspondence of $\overline{\mathcal{C}}^*$ as a simple component, where $q = N_{k/\mathbb{Q}}(\mathfrak{P})$ and $d > 0$.

Y. Morita [ ] constructed such a nice model $\mathcal{C}^*$, when $F = \mathbb{Q}$. Therefore, by the Main Theorem 1 (ii), we conclude, for instance, that if $\mathbb{F} = \mathbb{Q}$ and $\mathfrak{t} = 1$, then the canonical S-operator of $\mathcal{C}^*$ is "p-integral" for all $p \nmid D(B/\mathbb{Q})$, i.e., $S\langle \xi \rangle$ is finite with respect to the reduction $\mathcal{C}^* \to \overline{\mathcal{C}}^*$ mod p, for any $\mathbb{Q}$-rational differential $\xi \neq 0$ of $\mathcal{C}^*$.

§8-5 Calculation of $\overline{\omega}$ in certain triangular cases (I) The Main Theorem 1 (vi) provides us with a principle of explicit calculations of $\overline{\omega}$ in the following special cases, where in addition to (i), (ii) (§8-1(I)) and (iii) (§8-2(I)), the following assumptions are fulfilled:

(iv) $\Delta$ is commensurable with a triangular fuchsian group (see §2-4);

(v) $q = p$, and $v(p) = 1$.

First, in view of the assumption (iv), we can compute the canonical S-operator S of $\mathcal{E}$ explicitly by combining the Corollary of Proposition 7 (§2-4) with Proposition 5' (§2-2). By the Main Theorem 1, S is k-rational, V-integral, and $\bar{\omega}$ satisfies $\bar{S}\langle\bar{\omega}\rangle = 0$. Solve the equation $\bar{S}\langle\zeta\rangle = 0$ in the separable closure $\bar{L}$ of field $\bar{K}$. It is equivalent to solving the corresponding linear differential equation of degree two (see §1-5)*). But $\bar{L}$ is a p-dimensional vector space over the constant field $\bar{\ell} = \bar{L}^p$, and the corresponding differential operator is an $\bar{\ell}$-linear map of $\bar{L}$. Hence it is the question of calculating some $p \times p$ matrices over $\bar{\ell}$ (cf. the example of §1-6). Now let $\zeta \in D(L)^{\times}$ be any solution of $\bar{S}\langle\zeta\rangle = 0$, and put $\bar{\omega}' = (\gamma(\zeta)/\zeta)^{\frac{p}{p-1}} \cdot \zeta$. Then $\bar{\omega}'$ is another solution, and satisfies $\gamma(\bar{\omega}') = \bar{\omega}'$; hence $\bar{\omega}' = \bar{\omega}$ (by the Main Theorem 1 (vi)).

(II) We shall put in practice the calculations of $\bar{\omega}$ assuming (in addition to (i) (ii) (iii)) the following conditions (iv)*, (iv)** and (v)*. The conditions (iv)* and (v)* are stronger than (iv) and (v) of (I).

(iv)* $\Delta$ is triangular.

Let $(\Delta^{\mathfrak{H}})^*$ denote the compactification of $\Delta^{\mathfrak{H}}$. Then $(\mathrm{iv})^*$ implies that $(\Delta^{\mathfrak{H}})^*$ is of genus 0 and that there are exactly three points P on $(\Delta^{\mathfrak{H}})^*$ with $e(P) > 1$. Here, as in §2·2, $e(P)$ is the ramification index of the covering map $\mathfrak{H} \to \Delta^{\mathfrak{H}} \subset (\Delta^{\mathfrak{H}})^*$ at P. Hence there is a biholomorphic map $x : (\Delta^{\mathfrak{H}})^* \hookrightarrow \mathbb{C} \cup (\infty)$ such that $x(P) = 0, 1, \infty$ for the above three points P of $(\Delta^{\mathfrak{H}})^*$. As is well-known, there are six different choices of x; namely, if x is one of them, the others are given by $x^{-1}$, $1-x$, $1-x^{-1}$, $(1-x)^{-1}$, $(1-x^{-1})^{-1}$. Fix any one x, and regard $\mathbb{C} \cup (\infty)$ as a rational algebraic curve. Put $e(P) = e_0, e_1, e_\infty$, accordingly to $x(P) = 0, 1, \infty$, respectively.

$(\mathrm{iv})^{**}$ $\mathcal{C}$ <u>is a rational curve, identified with</u> $(\Delta^{\mathfrak{H}})^*$ <u>in the above manner</u>.

This condition will be abbreviated as "$\mathcal{C}$ <u>is a rational</u> x-<u>curve</u>."

$(\mathrm{v})^*$ $q = p \neq 2$, $v(p) = 1$, <u>and the following two congruences hold for some suitable choice of</u> $\varepsilon_i = \pm 1$ $(i = 0, 1, \infty)$:

$$p \equiv \varepsilon_i \pmod{e_i} \qquad \ldots\ i = 0, 1, \infty,$$

$$\sum_{i=0,1,\infty} \frac{p - \varepsilon_i}{e_i} \equiv 0 \pmod{2}.$$

(<u>E.g.</u>, $p \equiv 1 \pmod{2e_i}$ <u>for</u> $i = 0, 1, \infty$.) <u>In particular</u>, $e_i$ <u>are not divisible by</u> p.

Now we shall calculate $\overline{\omega}$. By the Corollary of Proposition 7 (§2-4), the canonical S-operator S of $\mathcal{C}$ with respect to $\Delta$ is given by the formula

$$S\langle dx\rangle = \frac{ax^2 + bx + c}{x^2(1-x)^2}(dx)^2 ,$$

with

$$a = \frac{1}{e_\infty^2} - 1, \quad a + b + c = \frac{1}{e_1^2} - 1, \quad c = \frac{1}{e_0^2} - 1.^{*)}$$

Therefore, if we put

$$\rho_i = \frac{\varepsilon_i}{e_i} \qquad (i = 0, 1, \infty)$$

and consider $\rho_i$ as elements of $\mathbb{F}_p$, then

$$\overline{S}\langle dt\rangle = \frac{\alpha t^2 + \beta t + \gamma}{t^2(1-t)^2}(dt)^2,$$

with

$$\alpha + 1 = \rho_\infty^2, \quad \alpha + \beta + \gamma + 1 = \rho_1^2, \quad \gamma + 1 = \rho_0^2.$$

Hence we can apply the results of §1-6. Put

$$g_i = \frac{p - \varepsilon_i}{e_i} \qquad (i = 0, 1, \infty).$$

Then, $A^\bullet$, $B^\bullet$, $C^\circ$ of §1-6 are given by

$$\frac{1}{2}(1 + p + g_0 + g_1 + g_\infty), \quad \frac{1}{2}(1 + p + g_0 + g_1 - g_\infty), \quad 1 + g_0,$$

respectively. Since $e_0^{-1} + e_1^{-1} + e_\infty^{-1} < 1$ ((e2) of §2-2), it follows

---

*) Recall that we used the condition " $\Delta$ and $\varepsilon^{-1}\Delta\varepsilon$ generate a dense subgroup of $G_R$," only to deduce the k-rationality of S (by the Corollary of Theorem 1A). But here, the k-rationality is obvious by this explicit formula. Hence we need not check the density assumption in the triangular case. See also the remark at the end of §8-2(I).

easily that $1 \leq C^{\bullet} \leq B^{\bullet} \leq A^{\bullet} \leq p$ and $\frac{1}{2}(p+1) \leq A^{\bullet}$. Therefore, by §1 6, the solutions of ($\natural$) are 1 dimensional, and one of them is given by

$$u(t) = f(A^{\bullet}, B^{\bullet}; C^{\bullet}; t).$$

Put

$$\delta_i = \frac{1}{2}(p - 1 - g_i) \qquad (i = 0, 1, \infty).$$

Theorem 9 The notations and the assumptions being as above, we have

$$(*) \qquad (\overline{\omega})^{\frac{1}{2}(p-1)} = \frac{u(t)}{t^{\delta_0}(1-t)^{\delta_1}}(dt)^{\frac{1}{2}(p-1)}.$$

The degree of the polynomial $u(t)$ is $p - A^{\bullet}$, and the roots of $u(t)$ are simple and are neither 0 nor 1.

Proof First, we shall check our assertions on the polynomial $u(t)$. Since $u(t) = f(A^{\bullet}, B^{\bullet}; C^{\bullet}; t)$ and $1 \leq C^{\bullet} \leq B^{\bullet} \leq A^{\bullet} \leq p$, the degree of $u(t)$ is $p - A^{\bullet}$. It is clear that $u(0) \neq 0$. That $u(1) \neq 0$ follows immediately by changing the variable $t \to 1 - t$. That $u(t)$ has no multiple roots follows by an argument of Igusa ([ ]). Namely, if $u(t)$ has a multiple root $\lambda$, then $u(\lambda) = \frac{du}{dt}(\lambda) = 0$; hence $\frac{d^2u}{dt^2}(\lambda) = 0$ by ($\natural$) (since $\lambda \neq 0, 1$). By differentiating ($\natural$), we obtain successively $\frac{d^3u}{dt^3}(\lambda) = \cdots = 0$, which is a contradiction since $u(t)$ is a non-zero polynomial of a degree less than p.

Now let us define $\overline{\omega}$ by the formula (*), and complete the proof by showing that $\overline{\omega}$ satisfies the two equations $\overline{S}\langle\overline{\omega}\rangle = 0$ and $\gamma(\overline{\omega}) = \overline{\omega}$. Put

$$v(t) = \frac{u(t)}{t^{\delta_0}(1 - t)^{\delta_1}}.$$

Then $v(t)$ concides with $t^{\frac{1}{2}(1-\rho_0)}(1 - t)^{\frac{1}{2}(1-\rho_1)}\, u(t)$, up to $(\overline{L}^{\times})^{p}$-multiples, $\overline{L}$ being the separable closure of $\overline{K} = \mathbb{F}_p(t)$. Hence $v(t)$ satisfies the equation $(b)$ of §1-6. But $\overline{\omega} = v(t)^{\frac{2}{p-1}}dt$; hence $\overline{\omega}$ coincides with $v(t)^{-2}dt$ up to $(\overline{L}^{\times})^{p}$-multiples. Therefore, $\overline{\omega}$ satisfies (#); i.e., $\overline{S}\langle\overline{\omega}\rangle = 0$. On the other hand, the $\gamma$-invariance of $\overline{\omega}$ is equivalent to the following:

<u>Lemma 3</u> $\qquad \gamma(v(t)^{-2}dt) = c\ dt \qquad (c \in \mathbb{F}_p^{\times})$.

To check this, put $y(t) = u(t)^{p}v(t)^{-2} = t^{2\delta_0}(1 - t)^{2\delta_1}u(t)^{p-2}$. Put $H = \deg u(t) = p - A^{\bullet}$. Then $y(t)$ is a polynomial of degree $p(H + 1) + g_{\infty} - 1$, which is strictly smaller than $p(H + 2) - 1$. Therefore, $\gamma(y(t)dt) = z(t)dt$ with some polynomial $z(t)$ of degree at most $H$. But since $\gamma(v(t)^{-2}dt) = u(t)^{-1}z(t)dt$, it suffices to show that $z(t)$ is divisible by $u(t)$. Therefore, it suffices to show that $\gamma(v(t)^{-2}dt)$ has no poles at the roots $\lambda$ of $u(t)$. Let $\lambda$ be a root of $u(t)$. Since it is a simple root, the pole of $v(t)^{-2}dt$ at $\lambda$ is of order 2. Hence it is enough to show that the residue of $v(t)^{-2}dt$ at $\lambda$ is zero, or equivalently, that

$$\frac{d\log}{dt}\left\{t^{2\delta_0}(1-t)^{2\delta_1}u(t)^{-2}(t-\lambda)^2\right\}_{t=\lambda} = 0.$$

This is equivalent to

$$\delta_0\lambda^{-1} + \delta_1(\lambda-1)^{-1} - \sum_{\mu\neq\lambda}(\lambda-\mu)^{-1} = 0,$$

where $\mu$ runs over all roots $\neq\lambda$ of $u(t)$. But

$$\sum_{\mu\neq\lambda}(\lambda-\mu)^{-1} = a_2/a_1,$$

where

$$u(t+\lambda) = a_1t + a_2t^2 + \cdots;$$

hence $a_1 = \frac{du}{dt}(\lambda)$, $a_2 = \frac{1}{2}\frac{d^2u}{dt^2}(\lambda)$. But by ($\natural$), we obtain

$$\lambda(1-\lambda)\frac{\frac{d^2u}{dt^2}(\lambda)}{\frac{du}{dt}(\lambda)} + (C^{\circ} - (A^{\circ}+B^{\circ}+1)\lambda) = 0;$$

whence

$$\sum_{\mu\neq\lambda}(\lambda-\mu)^{-1} = -\frac{(A^{\circ}+B^{\circ}+1)\lambda - C^{\circ}}{2\lambda(\lambda-1)}$$

$$= \delta_0\lambda^{-1} + \delta_1(\lambda-1)^{-1};$$

which proves Lemma 3 and hence also Theorem 9.

§8-6 The differential $\overline{\omega}$ in the elliptic modular case.(I) This is the case of $\Delta = PSL_2(\mathbb{Z})$. Put $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup (\infty)$, so that $\Delta\backslash\mathbb{H}^*$ compactifies $\Delta\backslash\mathbb{H}$. Put $i = \sqrt{-1}$, $\rho = \frac{1}{2}(-1+\sqrt{-3})$, and let $P^i$, $P^\rho$, $P^\infty$

respectively denote the points of $\Delta^{\backslash \mathbb{H}^*}$ represented by $i, \rho, \infty \in \mathbb{H}^*$. Then, $e(P) = 2, 3, \infty$, or $1$, according to $P = P^i, P^\rho, P^\infty$, or others. Since the genus of $\Delta^{\backslash \mathbb{H}^*}$ is 0, this shows that $\Delta$ is triangular. Let $j(\tau)$ be the "analyst's modular function," i.e., the unique biholomorphic isomorphism $j : \Delta^{\backslash \mathbb{H}^*} \to \mathbb{C} \cup (\infty)$ that maps $P^i$, $P^\rho$, $P^\infty$ to $1, 0, \infty$ respectively. Put $J(\tau) = 12^3 j(\tau)$ ("arithmetist's modular function"), and <u>first, take $\mathcal{C}$ to be the rational curve with the coordinate variable</u> $J(\tau)$.

Let $p$ be any prime number, and let $\varepsilon^*$ be the element of $G_{\mathbb{R}}$, which is represented by the matrix $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ modulo scalar multiples. Let $\varepsilon$ be any element of the double coset $\Delta \varepsilon^* \Delta$. Then $\varepsilon^{-1} \Delta \varepsilon$ is conjugate, by some element of $\Delta$, to the group

$$\left\{ \begin{pmatrix} a & p^{-1}b \\ pc & d \end{pmatrix} \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Delta \right\};$$

hence $(\Delta : \Delta \cap \varepsilon^{-1} \Delta \varepsilon) = (\varepsilon^{-1} \Delta \varepsilon : \Delta \cap \varepsilon^{-1} \Delta \varepsilon) = p + 1$. The correspondence $\mathfrak{X}$ defined by $\varepsilon$ (as in § 8-2) consists of all points on $\mathcal{C} \times \mathcal{C}$ of the form $(J(\tau), J(\varepsilon\tau))$ $(\tau \in \mathbb{H}^*)$. Let $\Phi(X,Y) = 0$ be the irreducible equation defining $\mathfrak{X}$. The polynomial $\Phi$ is determined only up to constant multiples, but we know that if the constant is suitably chosen, then $\Phi(X, Y) \in \mathbb{Z}[X, Y]$, and moreover that the <u>Kronecker congruence relation</u> is satisfied, i.e.,

$$\Phi(X, Y) \equiv (Y - X^p)(Y^p - X) \qquad \mod (p\mathbb{Z}[X, Y]);$$

(cf. e.g., Deuring [ ]). In other words, $\mathcal{E}$ and $\mathfrak{X}$ are defined over $\mathbb{Q}$, and

$$\overline{\mathfrak{X}} = \Pi + \Pi'$$

holds, where $\Pi$ is the p-th power correspondence of $\overline{\mathcal{E}}$, and $\Pi'$ is the transpose of $\Pi$. Therefore, the conditions (i) (ii) (iii) (§§ 8-1, 2) are satisfied with $k = \mathbb{Q}$ and $q = p$.

First, we shall specialize the notations of §8-1(II) to this case. Let J be a generic point of $\mathcal{E}$ over $\mathbb{Q}$, and let $(J, J') \in \mathfrak{X}$. Then, with the notations of §8-2, we have $K = \mathbb{Q}(J)$, $J^{\sigma} = J'$ and $L = \mathbb{Q}(J, J')$. The valuation V of K is defined by

$$V\left(p^c \frac{f(J)}{g(J)}\right) = c, \qquad \text{for } f(J), g(J) \in \mathbb{Z}[J] \notin p\mathbb{Z}[J]$$

By the Kronecker congruence relation and Hensel's lemma, there is a unique solution * of the equation $\Phi(J, *) = 0$ in the completion $K_V$ of K, and it satisfies $* \equiv J^p \pmod{p}$. Hence there is a unique K-isomorphism of L into $K_V$, and if L is considered as a subfield of $K_V$ by this embedding, then $J' \equiv J^p \pmod{p}$; hence $\sigma$ induces a p-th Frobenius map $K \mapsto K^{\sigma} \hookrightarrow K_V$.

Now let $\omega$ be the differential associated with $\sigma$ ( in the sense of §6-3(IV)), normalized by the two conditions $\omega^{\sigma}/\omega = p$ and $V(\omega) = 0$. We shall calculate $\overline{\omega}$ by applying Theorem 9 (§8-5). First, let $p \neq 2, 3$, and <u>now take $\mathcal{E}$ to be the</u> $j(\tau)$-<u>curve</u> (instead of the $J(\tau)$-curve).*) Then, the conditions $(iv)^*$, $(iv)^{**}$ and $(v)^*$ of §8-5(II) are satisfied for $x = j$ (hence $e_0, e_1, e_\infty = 3, 2, \infty$, respectively). The signs of $\varepsilon_0$, $\varepsilon_1$ are determined by the congruences $p \equiv \varepsilon_0 \pmod 3$, $\equiv \varepsilon_1 \pmod 4$, whereas $\varepsilon_\infty$ can be either of $\pm 1$. Therefore, Theorem 9 gives the following explicit formula for $\bar{\omega}$. (Note that $\bar{\omega}$ is determined up to $\mathbb{F}_p^\times$-multiples, and hence $\bar{\omega}^{\frac{1}{2}(p-1)}$, up to the signs.)

$$(*) \qquad \bar{\omega}^{\frac{1}{2}(p-1)} = \pm \frac{P(T)}{Q(T)} (dT)^{\frac{1}{2}(p-1)} \qquad (T = \bar{J}),$$

where

$$P(T) = T^{\frac{1}{2}(1-\varepsilon_0)} (T - 12^3)^{\frac{1}{2}(1-\varepsilon_1)} u(T),$$

$$Q(T) = T^{\frac{1}{3}(p-\varepsilon_0)} (T - 12^3)^{\frac{1}{4}(p-\varepsilon_1)},$$

$$u(T) = f(p - H, p - H; \frac{p - \varepsilon_0}{3} + 1; 12^{-3}T),$$

$$H = \frac{p-6}{12} + \frac{\varepsilon_0}{6} + \frac{\varepsilon_1}{4}.$$

$u(T)$ is a polynomial of degree $H$ such that $u(0)u(12^3) \neq 0$, and has no multiple roots.

In the cases of $p = 2, 3$, the difference between $j(\tau)$ and $J(\tau)$ is of essential nature, and replacing $J(\tau)$ by $j(\tau)$ would break down the congruence relation. Thus, we cannot apply the

---

*) This change (for $p \neq 2, 3$) will not affect $\sigma$, nor consequently $\omega$.

result of our calculations of §8-5 to the cases of p = 2, 3. But we can apply the same method. The calculations are easy, and we obtain

$$\bar{\omega} = \frac{dT}{T} \qquad (p = 2,\ 3;\ T = \bar{J}).$$

Remarks We obtain the same differential $\omega$, but in different forms of expression when we replace $\Delta$ by the congruence subgroups (see § ). For instance, if we replace $\Delta$ and $J(\tau)$ by the principal congruence subgroup of level 2 and the $\lambda$-function, we obtain the following simpler expression of $\bar{\omega}$ for $p \neq 2$:

$$(**) \qquad \bar{\omega}^{\frac{1}{2}(p-1)} = \pm \frac{u_2(\bar{\lambda})}{\{\bar{\lambda}(\bar{\lambda} - 1)\}^{\frac{1}{2}(p-1)}} (d\bar{\lambda})^{\frac{1}{2}(p-1)}$$

where $u_2(\bar{\lambda}) = f(\frac{p-1}{2}, \frac{p-1}{2}; 1; \bar{\lambda}) = \sum_{i=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{i}^2 \bar{\lambda}^i$. Of course the formula should also be obtained by substituting the equality

$$J = 2^8 \frac{(\bar{\lambda}^2 - \bar{\lambda} + 1)^3}{\{\bar{\lambda}(\bar{\lambda} - 1)\}^2}$$

in (*).

Another point to note is that we shall still obtain the same differential $\omega$, if we take $\varepsilon$ from the double coset $\Delta \varepsilon^{*f} \Delta$ ($f \geq 1$) and normalize $\omega$ by $\omega^\sigma/\omega = p^f$. Indeed, the Frobenius map for this case is nothing but the f-th iterate of the former $\sigma$. See §