Advanced Studies in Pure Mathematics 2, 1983
Galois Groups and their Representations
pp. 69–88

On Generalized Hasse-Witt Invariants of an Algebraic Curve

Shōichi Nakajima

§ 1. Introduction

Let k be an algebraically closed field of characteristic $p>0$, and C a connected complete non-singular curve over k. Denote by $\pi_1(C)$ the Grothendieck fundamental group of C. (cf. [3] exp. V. The group $\pi_1(C)$ is isomorphic to Gal (K_{ur}/K), where K is the function field of C and K_{ur} means the maximal unramified extension field of K.) Concerning this group $\pi_1(C)$, we shall generalize the result of Katsurada [7] (Theorem 1 in Section 2) and then prove another related theorem (Theorem 2 in Section 4).

To begin with, a short account will be given on the known facts about the structure of the group $\pi_1(C)$. For a non-negative integer g, put $\Gamma_g=\langle a_1, \cdots, a_g, b_1, \cdots, b_g \,|\, a_1b_1a_1^{-1}b_1^{-1}\cdots a_gb_ga_g^{-1}b_g^{-1}=1\rangle$, the group generated by $2g$ elements $a_1, \cdots, a_g, b_1, \cdots, b_g$ with one defining relation $a_1b_1a_1^{-1}b_1^{-1}\cdots a_gb_ga_g^{-1}b_g^{-1}=1$. ($\Gamma_g=\{1\}$ if $g=0$.) The group Γ_g is nothing but the topological fundamental group of a Riemann surface of genus g. Further, let $\hat{\Gamma}_g$ be the pro-finite completion of Γ_g, i.e. $\hat{\Gamma}_g=\varprojlim(\Gamma_g/\Gamma)$ where Γ ranges over all normal subgroups of Γ_g with finite indices. Then, we can state a fundamental result of Grothendieck about $\pi_1(C)$ ([3] exp. X): If the genus of C equals g, then there exists a surjective continuous homomorphism $\varphi\colon \hat{\Gamma}_g\to\pi_1(C)$ with the following property:

(*) Ker φ is contained in every open normal subgroup N of $\hat{\Gamma}_g$ such that $[\hat{\Gamma}_g\colon N]$ is prime to p.

The surjectivity of φ says that to each finite étale covering $C'\to C$ there corresponds a unique open subgroup N of $\hat{\Gamma}_g$. (The correspondence is given by $N=\varphi^{-1}(\pi_1(C'))$.) And the property (*) ensures that each open normal subgroup N of $\hat{\Gamma}_g$ with $[\hat{\Gamma}_g\colon N]$ prime to p can be obtained as $\varphi^{-1}(\pi_1(C'))$ for some connected étale covering $C'\to C$. But how about the groups N for which $[\hat{\Gamma}_g\colon N]$ is divisible by p? Or, we naturally ask a

Received December 7, 1982.

question: *Can we determine the whole structure of* $\pi_1(C)$, *not only its "prime-to-p part"*? Unfortunately, when $g \geqq 2$ no complete answer is known to the question above. If $g \geqq 2$, the structure of $\pi_1(C)$ has not yet been determined explicitly for any single example of C.

But classically, the following two facts have been known about the structure of $\pi_1(C)$. Let γ_C be the Hasse-Witt invariant of C. (cf. [6]; it is an integer satisfying $0 \leqq \gamma_C \leqq g$, and coincides with the p-rank of the Jacobian variety of C.) Then we have

(i) There exists an isomorphism

$$\pi_1(C)^{\mathrm{ab}} \cong (\prod_{l \neq p} Z_l^{2g}) \times Z_p^{\gamma_C},$$

where $\pi_1(C)^{\mathrm{ab}}$ denotes the maximal abelian quotient of $\pi_1(C)$ and, on the right side, l ranges over all primes other than p (Hasse-Witt [6]).

(ii) The maximal pro-p quotient of $\pi_1(C)$ is isomorphic to the free pro-p group of rank γ_C (Šafarevič [14]).

The results (i) and (ii) above ensure, in particular, that the structures of the maximal abelian and the maximal pro-p quotients of $\pi_1(C)$ are determined by the invariants g and γ_C of C. Then naturally, we come to a question: *Is it true that the structure of* $\pi_1(C)$ *itself is determined by* g *and* γ_C *only*? But Katsurada [7] showed that the answer to this question is *No*, by introducing generalized Hasse-Witt invariants of C. His result will be generalized hereafter in this paper.

In Section 2, generalized Hasse-Witt invariants are defined and Theorem 1 is stated which connects the generalized Hasse-Witt invariants with the structure of $\pi_1(C)$. The proof of Theorem 1 is given in Section 3. In Section 4, the notion of "n-ordinary curve" is introduced, and in Section 5 is proved Theorem 2 which states that "general" curves of given genus are n-ordinary. Examples are given in Section 6. Finally, a recent result of the author is mentioned in Section 7. It does not concern the generalized Hasse-Witt invariants, but gives a necessary condition for a finite group to be a quotient group of $\pi_1(C)$.

The author wishes to express his hearty thanks to Professor Y. Ihara, particularly for suggesting Theorem 2.

§ 2. Generalized Hasse-Witt invariants

As above, let C be a connected complete non-singular algebraic curve over an algebraically closed field k of characteristic $p>0$. We shall define the generalized Hasse-Witt invariants of C. For that purpose, some notations are necessary.

Let $\mathfrak{D}$ and $\bar{\mathfrak{D}}$ be respectively the divisor group and the divisor class group of C. For a natural number n, put

$$\bar{\mathfrak{D}}_n=\{\bar{A}\in\bar{\mathfrak{D}}\mid n\bar{A}=0\}$$

and

$${}_n\bar{\mathfrak{D}}=\{\bar{A}\in\bar{\mathfrak{D}}_n\mid \text{the order of } \bar{A} \text{ is precisely equal to } n\}.$$

Further, for a natural number n which is prime to $p=\mathrm{char}\ k$, define an equivalence relation $\approx$ in $\bar{\mathfrak{D}}_n$ (and also in ${}_n\bar{\mathfrak{D}}$) by

$$\bar{A}\approx\bar{B}\Longleftrightarrow\bar{A}=p^k\bar{B}\qquad\text{for some } k\in N\quad(\bar{A},\ \bar{B}\in\bar{\mathfrak{D}}_n).$$

(Since n is prime to p, $\approx$ is actually an equivalence relation.) Then put $\mathfrak{A}_n=\bar{\mathfrak{D}}_n/\approx$ and ${}_n\mathfrak{A}={}_n\bar{\mathfrak{D}}/\approx$, the sets of equivalence classes under $\approx$. Obviously we have

$$\mathfrak{A}_n=\bigcup_{d|n}{}_d\mathfrak{A}\qquad\text{(disjoint union).}$$

Corresponding to each element $\alpha\in\mathfrak{A}=\bigcup_n {}_n\mathfrak{A}$ (n varies over all natural numbers prime to p), the generalized Hasse-Witt invariant γ_α is defined in the following way: Let n be the natural number for which $\alpha\in{}_n\mathfrak{A}$ holds, and let m be the order of p in $(Z/nZ)^\times$. Take an element $\bar{A}\in{}_n\bar{\mathfrak{D}}$ which belongs to α, and a divisor A in the class $\bar{A}$. Since $n\mid(p^m-1)$ and $n\bar{A}=0$, there is a rational function x on C such that $(x)=(p^m-1)A$ holds. Let $\mathscr{L}(A)$ be the invertible sheaf determined by A (cf. [16] chap. II; we regard $\mathscr{L}(A)$ as contained in the constant sheaf of rational functions on C). Multiplication by the rational function x induces an isomorphism $\mu=\mu_x$: $\mathscr{L}(p^mA)\simeq\mathscr{L}(A)$. On the other hand, we have a morphism $F^m=(F^m)^*$: $\mathscr{L}(A)\to\mathscr{L}(p^mA)$, where F denotes the Frobenius morphism of C. Hence we have a morphism μF^m: $\mathscr{L}(A)\to\mathscr{L}(A)$, and it induces a map μF^m: $H^1(C,\mathscr{L}(A))\to H^1(C,\mathscr{L}(A))$. Put

$$H^1(C,\mathscr{L}(A))^{\mu F^m}=\{\xi\in H^1(C,\mathscr{L}(A))\mid \mu F^m(\xi)=\xi\}.$$

Then $H^1(C,\mathscr{L}(A))^{\mu F^m}$ is a vector space over F_q ($q=p^m$) since μF^m: $H^1(C,\mathscr{L}(A))\to H^1(C,\mathscr{L}(A))$ is a q-linear map, i.e.

$$\mu F^m(a_1\xi_1+a_2\xi_2)=a_1^q\mu F^m(\xi_1)+a_2^q\mu F^m(\xi_2)$$

holds for any $a_1,\ a_2\in k$, $\xi_1,\ \xi_2\in H^1(C,\mathscr{L}(A))$. We define the invariant γ_α by

$$\gamma_\alpha=\dim_{F_q}H^1(C,\mathscr{L}(A))^{\mu F^m}.$$

It is easily verified that γ_α depends only on the class $\bar{A}$, i.e. γ_α does not depend on the choice of A or x. Further, by virtue of Lemma 1 below, γ_α is also independent of the choice of $\bar{A}\in\alpha$, and hence γ_α is well-defined.

Lemma 1. *Define the morphism* $\tilde{\mu}$: $\mathscr{L}(p^{m+1}A) \to \mathscr{L}(pA)$ *and the* $\boldsymbol{F}_q$-*vector space* $H^1(C, \mathscr{L}(pA))^{\tilde{\mu}F^m}$ *as above, taking* pA *and* x^p *instead of* A *and* x. *Then we have an isomorphism* $H^1(C, \mathscr{L}(A))^{\mu F^m} \cong H^1(C, \mathscr{L}(pA))^{\tilde{\mu}F^m}$ *as* $\boldsymbol{F}_q$-*vector spaces.*

Proof. We have morphisms F: $H^1(C, \mathscr{L}(A)) \to H^1(C, \mathscr{L}(pA))$ and μF^{m-1}: $H^1(C, \mathscr{L}(pA)) \to H^1(C, \mathscr{L}(A))$. Then since $\tilde{\mu}F \doteq F\mu$ holds, it is easy to check that the restrictions of F and μF^{m-1} above give isomorphisms between $H^1(C, \mathscr{L}(A))^{\mu F^m}$ and $H^1(C, \mathscr{L}(pA))^{\tilde{\mu}F^m}$ which are inverse to each other.

By the following Proposition 1, we see that γ_α is an integer satisfying

$$0 \leqq \gamma_\alpha \leqq \dim_k H^1(C, \mathscr{L}(A)) = \begin{cases} g & (n=1) \\ g-1 & (n>1) \end{cases},$$

where g is the genus of C. (Since $\deg \mathscr{L}(A) = \deg A = 0$, $\dim_k H^1(C, \mathscr{L}(A))$ is easily calculated by using the Riemann-Roch theorem.) Proposition 1 is due to Hasse-Witt [6]. (In [6] only the case $l=-1$ is treated. But the proof there applies to arbitrary l.)

Proposition 1 (Hasse-Witt). *Let* k *be an algebraically closed field of characteristic* $p>0$, *and* V *a vector space over* k *of dimension* d. *If* l *is a non-zero integer and* f: $V \to V$ *is a* p^l-*linear map, then the set* $V^f = \{x \in V \mid f(x) = x\}$ *is an* $\boldsymbol{F}_q$-*vector space* ($q = p^{|l|}$). *Let* V_s *be the* k-*linear subspace of* V *spanned by* V^f, *and put* $V_n = \{x \in V \mid f^d(x) = 0\}$. *Then* V_n *is also a* k-*linear subspace of* V, *and we have*

(i) $V = V_s \oplus V_n$ *(direct sum)*,

(ii) $\dim_k V_s = \dim_{\boldsymbol{F}_q} V^f$. *In particular,*

$$\begin{aligned} \dim_{\boldsymbol{F}_q} V^f = d &\Longleftrightarrow V_s = V \\ &\Longleftrightarrow f\colon V \longrightarrow V \text{ is invertible} \\ &\Longleftrightarrow f \text{ is surjective} \\ &\Longleftrightarrow f \text{ is injective.} \end{aligned}$$

Remarks. (1) When $n=1$, the set ${}_1\mathfrak{A}$ consists of only one element 0, and the corresponding invariant γ_0 coincides with the classical Hasse-Witt invariant γ_C of C. Hence γ_α's are called generalized Hasse-Witt invariants.

(2) The value of γ_α can be calculated by using differentials and the Cartier operator (Proposition 2 below). The formula in Proposition 2 may be regarded as the definition of γ_α.

(3) Originally, the generalized Hasse-Witt invariants γ_α were defined in Katsurada [7] under the assumption that $n \mid (p-1)$, i.e. for $\alpha \in {}_n\mathfrak{A}$ such that $n \mid (p-1)$. (For definition, he used differentials. cf. Remark (2)

above.) He also proved Theorem 1 below in that case. Our definition of γ_α's for arbitrary n $(p\nmid n)$ is a natural generalization of Katsurada's one. But by this generalization, infinitely many invariants $\{\gamma_\alpha\}$ have been defined for each curve C.

(4) The generalized Hasse-Witt invariants $\{\gamma_\alpha\}$ are actually new invariants other than g or γ_C, that is, there exist curves with the same g and γ_C which have different γ_α's. This fact is shown in [7] and Section 6 of this article by concrete examples. However, I do not know whether the infinitely many invariants $\{\gamma_\alpha\}$ are "independent" or not.

Now we state Theorem 1 which connects the structure of $\pi_1(C)$ with the generalized Hasse-Witt invariants $\{\gamma_\alpha\}$ defined above. For a natural number n which is prime to p, put

$$G_{n,p}=\left\{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in GL(2, F_q)\,\middle|\, a^n=1\right\},$$

where $q=p^m$ and m is the order of p in $(Z/nZ)^\times$. By the definition of m, the field F_q contains a primitive n-th root of unity, and hence the order of $G_{n,p}$ equals np^m. By the word "$G_{n,p}$-covering of C" we mean a Galois covering $C'\to C$ with Galois group isomorphic to $G_{n,p}$. Let $N=N_{C,n}$ be the number of C-isomorphism classes of connected étale $G_{n,p}$-coverings of C. In other words, N is the number of open normal subgroups H of $\pi_1(C)$ for which $\pi_1(C)/H\cong G_{n,p}$ holds. Then, we have the following

Theorem 1. *The number $N=N_{C,n}$ is expressed by the generalized Hasse-Witt invariants $\{\gamma_\alpha\,|\,\alpha\in{}_n\mathfrak{A}\}$ in the form*

$$N=\sum_{\alpha\in{}_n\mathfrak{A}}\frac{q^{\gamma_\alpha}-1}{q-1},$$

where $q=p^m$ and m is the order of p in $(Z/nZ)^\times$.

Remark. By virtue of Theorem 1, we see that the structure of $\pi_1(C)$ actually depends on generalized Hasse-Witt invariants and can not be determined by g and γ_C only. (cf. examples in Section 6 and [7].)

Theorem 1 will be proved in Section 3. Before that, we explain here a method of calculating γ_α by using differentials and the Cartier operator. Let K be the function field of C over k and Ω_C the module of rational differentials on C; $\Omega_C=\{xdy\,|\,x,y\in K\}$. Further, for a divisor A of C, put $\Omega_C(A)=\{\omega\in\Omega_C\,|\,(\omega)\succ A\}$, which is a finite-dimensional vector space over k. Let γ be the Cartier operator. It is a map $\gamma\colon \Omega_C\to\Omega_C$ with the following properties (cf. [1], [15]);

(i) $\gamma(x_1^p\omega_1+x_2^p\omega_2)=x_1\gamma(\omega_1)+x_2\gamma(\omega_2)$, $x_1, x_2 \in K$, $\omega_1, \omega_2 \in \Omega_C$.

(ii) $\gamma(dx)=0$, $\gamma\left(\frac{dx}{x}\right)=\frac{dx}{x}$, $x \in K^\times$.

(iii) $\gamma(\Omega_C(pA))\subset\Omega_C(A)$ for any divisor A of C.

For a given $\alpha \in {}_n\mathfrak{A}$ $(p\nmid n)$, choose $\bar{A} \in \bar{\mathfrak{D}}$, $A \in \mathfrak{D}$ and $x \in K^\times$ in the same way as at the beginning of this section. Define a map $\beta=\beta_{A,x}: \Omega_C(A)\rightarrow \Omega_C(A)$ by $\beta(\omega)=\gamma^m(x\omega)$ for $\omega \in \Omega_C(A)$ (m is the order of p in $(\boldsymbol{Z}/n\boldsymbol{Z})^\times$). By the property (iii) of γ, β is well-defined. Since β is a p^{-m}-linear map (cf. property (i) of γ), the set $\Omega_C(A)^\beta=\{\omega \in \Omega_C(A)\,|\,\beta(\omega)=\omega\}$ is a vector space over $\boldsymbol{F}_q$ $(q=p^m)$. Here Proposition 2 below holds, which gives us a method of calculating the generalized Hasse-Witt invariant γ_α.

Proposition 2. *With the notations above, we have*

$$\gamma_\alpha=\dim_{\boldsymbol{F}_q}\Omega_C(A)^\beta.$$

Proof. The vector spaces $H^1(C, \mathscr{L}(A))$ and $\Omega_C(A)$ are dual to each other ([16] chap. II). And as is easily checked (cf. [15] n° 10), the q-linear map $\mu F^m: H^1(C, \mathscr{L}(A))\rightarrow H^1(C, \mathscr{L}(A))$ (for μF^m, see the definition of γ_α) is the transpose of the q^{-1}-linear map $\beta: \Omega_C(A)\rightarrow\Omega_C(A)$, i.e. $\langle\mu F^m(\xi), \omega\rangle =\langle\xi, \beta(\omega)\rangle^q$ holds for any $\xi \in H^1(C, \mathscr{L}(A))$ and $\omega \in \Omega_C(A)$. ($\langle\xi, \omega\rangle$ is the dual pairing; cf. [15] Proposition 9.) Then the argument of [15] p. 38–39 shows that $H^1(C, \mathscr{L}(A))^{\mu F^m}$ and $\Omega_C(A)^\beta$ are dual vector spaces over $\boldsymbol{F}_q$. Therefore we have $\gamma_\alpha=\dim_{\boldsymbol{F}_q}H^1(C, \mathscr{L}(A))^{\mu F^m}=\dim_{\boldsymbol{F}_q}\Omega_C(A)^\beta$, and Proposition 2 is proved.

§ 3. Proof of Theorem 1

The group $G_{n,p}$ has a normal (hence unique) p-Sylow subgroup $H=\left\{\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix} \in GL(2, \boldsymbol{F}_q)\right\}$, and the quotient $G_{n,p}/H$ is isomorphic to $\boldsymbol{Z}/n\boldsymbol{Z}$. Hence, if $C''\rightarrow C$ is a connected étale $G_{n,p}$-covering of C, then $C''\rightarrow C$ has a unique subcovering $C'\rightarrow C$ which is cyclic of degree n. For each connected étale cyclic covering $C'\rightarrow C$ of degree n, let $N_{C'}$ be the number of connected étale $G_{n,p}$-coverings of C which contain $C'\rightarrow C$ as a subcovering. Then, by the fact explained above, we have

$$N=\sum_{C'} N_{C'}, \tag{3.1}$$

where C' ranges over all connected étale cyclic coverings of degree n of C. Therefore we fix a connected étale cyclic covering $C'\rightarrow C$ of degree n, and will calculate $N_{C'}$.

Let μ_n be the group of n-th roots of unity in k and let $\mathfrak{D}_n$ be as defined in Section 2. Then, by Kummer theory, we have an isomorphism $\mathfrak{D}_n \cong \mathrm{Hom}(\pi_1(C), \mu_n)$ (the right side means, also in the following, the group of *continuous* homomorphisms). Let $\mathfrak{D}(C')$ be the subgroup of $\mathfrak{D}_n$ which corresponds to $\mathrm{Hom}(\mathrm{Gal}(C'/C), \mu_n)$ by the above isomorphism. Obviously this set $\mathfrak{D}(C')$ is closed under the equivalence relation $\approx$ defined in Section 2. Put $\mathfrak{A}(C') = \mathfrak{D}(C')/\approx$ and ${}_n\mathfrak{A}(C') = \mathfrak{A}(C') \cap {}_n\mathfrak{A}$. Then we have

$$(3.2) \qquad {}_n\mathfrak{A} = \bigcup_{C'} {}_n\mathfrak{A}(C') \qquad \text{(disjoint union)}$$

where C' ranges over all connected étale cyclic coverings of degree n of C. Our aim is to prove the equality

$$N_{C'} = \sum_{\alpha \in {}_n\mathfrak{A}(C')} \frac{q^{r_\alpha} - 1}{q - 1}.$$

Concerning the set $\mathfrak{A}(C')$, we have

Proposition 3. *Let R be the set of all equivalence classes of F_p-irreducible representations of the group* $\mathrm{Gal}(C'/C)$ *on vector spaces over F_p. Then we have a bijective map f: $\mathfrak{A}(C') \to R$ such that, for $\alpha \in \mathfrak{A}(C')$, the F_p-irreducible representation $f(\alpha)$ of* $\mathrm{Gal}(C'/C)$ *is faithful if and only if $\alpha \in {}_n\mathfrak{A}(C')$.*

Proof. The map f is constructed as follows: For an element $\alpha \in \mathfrak{A}(C')$, we have $\alpha = \{\bar{A}, p\bar{A}, \cdots, p^{l-1}\bar{A}\}$ for some $\bar{A} \in \mathfrak{D}_n$ and $l \in N$. Let $\chi = \chi_{\bar{A}}$ be the element of $\mathrm{Hom}(\mathrm{Gal}(C'/C), \mu_n)$ which corresponds to $\bar{A}$. Then, $\chi, \chi^p, \cdots, \chi^{p^{l-1}}$ are all the conjugates of χ over F_p. Hence the representation $\rho = \chi \oplus \chi^p \oplus \cdots \oplus \chi^{p^{l-1}}$ is equivalent to a representation which is realized and irreducible over F_p. This element ρ of R is the image $f(\alpha)$ of α. The map f thus defined is obviously injective. Since $\mathrm{Gal}(C'/C)$ is abelian, all irreducible representations of $\mathrm{Gal}(C'/C)$ over an algebraically closed field are one-dimensional. Hence an element ρ of R decomposes over k in the form $\rho \sim \chi \oplus \chi^p \oplus \cdots \oplus \chi^{p^{l-1}}$ where $\chi \in \mathrm{Hom}(\mathrm{Gal}(C'/C), \mu_n)$ and $\chi, \chi^p, \cdots, \chi^{p^{l-1}}$ are all the conjugates of χ over F_p (ρ is F_p-irreducible). This means that $\rho = f(\alpha)$ for some $\alpha \in \mathfrak{A}(C')$, that is, f is also surjective. It is an immediate consequence of the decomposition

$$(3.3) \qquad f(\alpha) \sim \chi \oplus \chi^p \oplus \cdots \oplus \chi^{p^{l-1}}$$

($\chi = \chi_{\bar{A}}$, $\alpha = \{\bar{A}, p\bar{A}, \cdots, p^{l-1}\bar{A}\} \in \mathfrak{A}(C')$) that $f(\alpha)$ is faithful if and only if the order of χ, hence the order of $\bar{A}$, equals n, i.e. if and only if $\alpha \in {}_n\mathfrak{A}(C')$.

(When $\alpha \in {}_n\mathfrak{A}(C')$, we have $l=m=$the order of p in $(\boldsymbol{Z}/n\boldsymbol{Z})^{\times}$.)

We regard the group $\pi_1(C')$ as an open normal subgroup of $\pi_1(C)$, for which $\pi_1(C)/\pi_1(C') \cong \mathrm{Gal}\,(C'/C)$ holds. Consider the set $\mathrm{Hom}\,(\pi_1(C'), \boldsymbol{Z}/p\boldsymbol{Z})$ which is a vector space over $\boldsymbol{F}_p$. The group $\mathrm{Gal}\,(C'/C)$ acts on $\mathrm{Hom}\,(\pi_1(C'), \boldsymbol{Z}/p\boldsymbol{Z})$ in the following way: For $\sigma \in \mathrm{Gal}\,(C'/C)$, choose a $\tilde{\sigma} \in \pi_1(C)$ whose image in $\mathrm{Gal}\,(C'/C)$ coincides with σ. Then for $\chi \in \mathrm{Hom}\,(\pi_1(C'), \boldsymbol{Z}/p\boldsymbol{Z})$, χ^{σ} is given by $\chi^{\sigma}(\tau)=\chi(\tilde{\sigma}\cdot\tau\cdot\tilde{\sigma}^{-1})$ for any $\tau \in \pi_1(C')$. (This action is well-defined since $\boldsymbol{Z}/p\boldsymbol{Z}$ is abelian.)

There exists a one-to-one correspondence between the two sets S_1 and S_2 below;

$$S_1=\{C'' \longrightarrow C' \mid C'' \longrightarrow C' \text{ is a connected étale Galois covering such that } \mathrm{Gal}\,(C''/C') \cong (\boldsymbol{Z}/p\boldsymbol{Z})^l \text{ for some } l\},$$

$$S_2=\{V \mid V \text{ is an } \boldsymbol{F}_p\text{-subspace of } \mathrm{Hom}\,(\pi_1(C'), \boldsymbol{Z}/p\boldsymbol{Z})\}.$$

The correspondence is given by

(a) $C'' \to C'$ is the covering determined by the open subgroup $\bigcap_{\chi \in V} (\mathrm{Ker}\,\chi)$ of $\pi_1(C')$,

(b) $V=\mathrm{Hom}\,(\mathrm{Gal}\,(C''/C'), \boldsymbol{Z}/p\boldsymbol{Z})$.

When $C'' \to C' \in S_1$ and $V \in S_2$ correspond, elementary Galois theory shows

(i) $\mathrm{Gal}\,(C''/C') \cong (\boldsymbol{Z}/p\boldsymbol{Z})^l \Longleftrightarrow \dim_{\boldsymbol{F}_p} V=l$,

(ii) $C'' \to C$ is a Galois covering
$\Longleftrightarrow V$ is stable under the action of $\mathrm{Gal}\,(C'/C)$ on $\mathrm{Hom}\,(\pi_1(C'), \boldsymbol{Z}/p\boldsymbol{Z})$.

Assume that $C'' \to C$ is Galois, i.e. $\mathrm{Gal}\,(C'/C)$ acts on V. Then we have

Lemma 2. (i) *Let V^* be the dual vector space of V with the action of* $\mathrm{Gal}\,(C'/C)$ *contragredient to that on V. Then we have an isomorphism* $\mathrm{Gal}\,(C''/C) \cong \mathrm{Gal}\,(C'/C) \ltimes V^*$ *where the right side is the semi-direct product of* $\mathrm{Gal}\,(C'/C)$ *and V^* defined by the above action of* $\mathrm{Gal}\,(C'/C)$ *on V^*.* (*Here V^* is regarded as an additive group.*)

(ii) *We have* $\mathrm{Gal}\,(C''/C) \cong G_{n,p}$ *if and only if the action of* $\mathrm{Gal}\,(C'/C)$ *on V^** (*hence on V*) *is faithful and $\boldsymbol{F}_p$-irreducible.*

Proof. (i) Since $V=\mathrm{Hom}\,(\mathrm{Gal}\,(C''/C'), \boldsymbol{Z}/p\boldsymbol{Z})$, we have an exact sequence of groups $1 \to V^* \to \mathrm{Gal}\,(C''/C) \to \mathrm{Gal}\,(C'/C) \to 1$. This sequence necessarily splits because the orders of $\mathrm{Gal}\,(C'/C)$ $(\cong \boldsymbol{Z}/n\boldsymbol{Z})$ and V^* $(\cong (\boldsymbol{Z}/p\boldsymbol{Z})^l)$ are prime to each other (cf. [5] Theorem 15.2.2., for example). Hence we have $\mathrm{Gal}\,(C''/C) \cong \mathrm{Gal}\,(C'/C) \ltimes V^*$.

(ii) By (i), our task is to prove that $\mathrm{Gal}\,(C'/C) \ltimes V^* \cong G_{n,p}$ holds if and only if the action of $\mathrm{Gal}(C'/C)$ on V^* is faithful and F_p-irreducible. The group $G_{n,p}$ is of the form $G_{n,p} \cong D \ltimes H$ (semi-direct product), where

$$D=\left\{\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \in GL(2, F_q) \middle| a^n=1\right\} \qquad (\cong Z/nZ)$$

and

$$H=\left\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in GL(2, F_q)\right\} \qquad (\cong F_q \cong (Z/pZ)^m).$$

If an isomorphism φ: $\mathrm{Gal}(C'/C) \ltimes V^* \rightrightarrows G_{n,p}$ exists, it induces an isomorphism φ_0: $V^* \rightrightarrows H$ since V^* [resp. H] is the unique p-Sylow subgroup of $\mathrm{Gal}(C'/C) \ltimes V^*$ [resp. $G_{n,p}$]. Then φ also induces an isomorphism φ_1: $\mathrm{Gal}(C'/C) \rightrightarrows D$. Here the action ρ' of $\mathrm{Gal}(C'/C)$ on V^* is given by $\rho' = \varphi_0^{-1} \circ \rho \circ \varphi_1$ where ρ is the action of D on H. Since ρ is faithful and F_p-irreducible, ρ' is also faithful and F_p-irreducible. Conversely, if ρ' is a faithful F_p-irreducible representation of $\mathrm{Gal}(C'/C)$, then ρ' has a decomposition (3.3) (replacing $f(\alpha)$ by ρ'). In that decomposition, the order of χ equals n since ρ' is faithful, and hence we have $l=m$. Therefore, we can easily construct isomorphisms φ_0: $V^* \rightrightarrows H$ and φ_1: $\mathrm{Gal}(C'/C) \rightrightarrows D$ so that $\rho' = \varphi_0^{-1} \circ \rho \circ \varphi_1$ holds, and from these, an isomorphism φ: $\mathrm{Gal}(C'/C) \ltimes V^* \rightrightarrows G_{n,p}$. Thus Lemma 2 has been proved.

By Lemma 2 the number $N_{C'}$ is equal to the number of $\mathrm{Gal}(C'/C)$-invariant subspaces of $\mathrm{Hom}(\pi_1(C'), Z/pZ)$ which correspond to faithful F_p-irreducible representations of $\mathrm{Gal}(C'/C)$.

Put $H^1(C') = H^1(C', \mathcal{O}_{C'})$ and $H^1(C')^F = \{\xi \in H^1(C') \mid F(\xi) = \xi\}$, where F: $H^1(C') \to H^1(C')$ donotes the p-linear map induced by the Frobenius morphism of C'. (The group $\mathrm{Gal}(C'/C)$ acts on $H^1(C')$ and $H^1(C')^F$ in the natural way.) Then we have an isomorphism $\mathrm{Hom}(\pi_1(C'), Z/pZ) \cong H^1(C')^F$ (cf. [15] Proposition 12, for example). As is easily checked, this isomorphism commutes with the action of $\mathrm{Gal}(C'/C)$. For each element $\chi \in \mathrm{Hom}(\mathrm{Gal}(C'/C), \mu_n)$, put $H^1(C')^\chi = \{\xi \in H^1(C') \mid \xi^\sigma = \chi(\sigma)\xi$ for every $\sigma \in \mathrm{Gal}(C'/C)\}$. Since F is p-linear, we have

$$F(H^1(C')^\chi) \subset H^1(C')^{\chi^p} \tag{3.4}$$

For $\alpha \in \mathfrak{A}(C')$, let $f(\alpha)$ be the representation of $\mathrm{Gal}(C'/C)$ defined in Proposition 3 and denote by $(H^1(C')^F)^\alpha$ the union of all $\mathrm{Gal}(C'/C)$-invariant subspaces of $H^1(C')^F$ which correspond to the representation $f(\alpha)^*$ of $\mathrm{Gal}(C'/C)$. Here $f(\alpha)^*$ means the contragredient representation of $f(\alpha)$.

Assume $\alpha \in {}_n\mathfrak{A}(C')$. Then we have $f(\alpha) \sim \chi \oplus \chi^p \oplus \cdots \oplus \chi^{p^{m-1}}$ for some $\chi \in \mathrm{Hom}(\mathrm{Gal}(C'/C), \mu_n)$ of order n, where m is the order of p in

$(\boldsymbol{Z}/n\boldsymbol{Z})^{\times}$ (cf. proof of Proposition 3). Consequently, we have $f(\alpha)^* \sim \chi^{-1} \oplus \chi^{-p} \oplus \cdots \oplus \chi^{-p^{m-1}}$. Here (3.4) shows that F^m acts on $H^1(C')^{\chi^{-1}}$. Put $(H^1(C')^{\chi^{-1}})^{F^m} = \{\xi \in H^1(C')^{\chi^{-1}} \mid F^m(\xi) = \xi\}$. Then we have

Lemma 3. *There exists an isomorphism of* Gal(C'/C)*-modules*

$$(H^1(C')^F)^\alpha \cong (H^1(C')^{\chi^{-1}})^{F^m}.$$

Proof. Put $W = \oplus_{\chi'} H^1(C')^{\chi'} \subset H^1(C')$, where χ' ranges over $\{\chi^{-1}, \chi^{-p}, \cdots, \chi^{-p^{m-1}}\}$. Then, from definition we have $(H^1(C')^F)^\alpha = W^F = \{\xi \in W \mid F(\xi) = \xi\}$. Consider the projection π: $W \to H^1(C')^{\chi^{-1}}$. We have $\pi(W^F) \subset (H^1(C')^{\chi^{-1}})^{F^m}$ by the property (3.4). Further, the map μ: $(H^1(C')^{\chi^{-1}})^{F^m} \to W^F$, $\mu(\xi) = (\xi, F(\xi), \cdots, F^{m-1}(\xi))$, gives a homomorphism inverse to π. Hence we have $W^F \cong (H^1(C')^{\chi^{-1}})^{F^m}$.

The set $(H^1(C')^{\chi^{-1}})^{F^m}$ has a structure of vector space over $\boldsymbol{F}_q$ where $q = p^m$ (cf. Proposition 1), and an element $\sigma \in \mathrm{Gal}(C'/C)$ acts on $(H^1(C')^{\chi^{-1}})^{F^m}$ as multiplication by $\chi^{-1}(\sigma) \in \mu_n \subset \boldsymbol{F}_q$. Since χ^{-1}: Gal$(C'/C) \to \mu_n$ is surjective (χ^{-1} has order n) and μ_n generates $\boldsymbol{F}_q$ over $\boldsymbol{F}_p$, an $\boldsymbol{F}_p$-subspace of $(H^1(C')^{\chi^{-1}})^{F^m}$ is Gal(C'/C)-invariant if and only if it is an $\boldsymbol{F}_q$-subspace of $(H^1(C')^{\chi^{-1}})^{F^m}$. Consequently, a Gal$(C'/C)$-invariant $\boldsymbol{F}_p$-subspace of $(H^1(C')^{\chi^{-1}})^{F^m}$ is irreducible if and only if it is a one-dimensional $\boldsymbol{F}_q$-subspace. Hence by Lemma 3 and the following Lemma 4, we have an equality ($\alpha \in {}_n\mathfrak{A}(C')$),

(3.5) the number of irreducible Gal(C'/C)-invariant subspaces of
$$(H^1(C')^F)^\alpha = \frac{q^{\gamma_\alpha} - 1}{q - 1}$$

Lemma 4. $\gamma_\alpha = \dim_{\boldsymbol{F}_q} (H^1(C')^{\chi^{-1}})^{F^m}$

Proof. We have $\chi = \chi_{\bar{A}}$ for some $\bar{A} \in \alpha$. Choose A and x as in the definition of γ_α (§ 2). Then $y = x^{l^{-1}}$ ($l = p^m - 1$) is a rational function on C' whose divisor (y) coincides with A considered as a divisor on C'. Further we have $y^\sigma = \chi(\sigma) y$ for any $\sigma \in \mathrm{Gal}(C'/C)$. Let $\mathcal{O}_{C'}^{\chi^{-1}}$ be a subsheaf of $\mathcal{O}_{C'}$ whose stalk at $z \in C'$ equals

$$\mathcal{O}_{C',z}^{\chi^{-1}} = \{\xi \in \mathcal{O}_{C',z} \mid \xi^\sigma = \chi^{-1}(\sigma)\xi \text{ for any } \sigma \in \mathrm{Gal}(C'/C)\}.$$

Then, multiplication by the rational function y gives an isomorphism η: $\mathcal{O}_{C',z}^{\chi^{-1}} \simeq f^{-1}\mathscr{L}(A)$ (f: $C' \to C$). Hence we have an isomorphism

$$H^1(C')^{\chi^{-1}} = H^1(C', \mathcal{O}_{C'}^{\chi^{-1}}) \xrightarrow[\sim]{\eta} H^1(C', f^{-1}\mathscr{L}(A)) = H^1(C, \mathscr{L}(A)),$$

and further we have $\mu F^m = \eta F^m \eta^{-1}$ (for $\mu F^m : H^1(C, \mathscr{L}(A)) \to H^1(C, \mathscr{L}(A))$, see § 2). Therefore η gives an isomorphism $(H^1(C')^{\chi^{-1}})^{F^m} \to H^1(C, \mathscr{L}(A))^{\mu F^m}$, and in particular, we have $\gamma_\alpha = \dim_{F_q} H^1(C, \mathscr{L}(A))^{\mu F^m} = \dim_{F_q} (H^1(C')^{\chi^{-1}})^{F^m}$.

Now we are at the final step of the proof of Theorem 2. By Proposition 3, Lemma 2 (ii) and the formula (3.5), we have

$$N_{C'} = \sum_{\alpha \in {}_n\mathfrak{A}(C')} \frac{q^{\gamma_\alpha} - 1}{q - 1}.$$

Therefore the equalities (3.1) and (3.2) show

$$N = \sum_{\alpha \in {}_n\mathfrak{A}} \frac{q^{\gamma_\alpha} - 1}{q - 1},$$

and hence Theorem 2 has been proved.

§ 4. *n*-ordinary curves

In this section we introduce the notion of "n-ordinary curve" and state Theorem 2 which says that "general" curves of given genus are n-ordinary.

Let k be an algebraically closed field of characteristic $p > 0$, and C a connected complete non-singular algebraic curve of genus g over k. We have the generalized Hasse-Witt invariants $\{\gamma_\alpha\}$ of C defined in Section 2. Let n be a natural number prime to $p = \text{char } k$. Then we call the curve C "*n-ordinary*" if and only if $\gamma_\alpha = \begin{cases} g & (n=1) \\ g-1 & (n>1) \end{cases}$ for all $\alpha \in {}_n\mathfrak{A}$. When $n = 1$, the word "1-ordinary" means the same as the word "ordinary" in the usual sense (i.e. $\gamma_C = g$). As is seen from Theorem 1, an n-ordinary curve has a maximal possible number of connected étale $G_{n,p}$-coverings, as a curve of genus g over k. (Recall that $l = \begin{cases} g & (n=1) \\ g-1 & (n>1) \end{cases}$ is the maximal possible value of γ_α for $\alpha \in {}_n\mathfrak{A}$.) The fundamental group $\pi_1(C)$ of an n-ordinary curve C is "big" in this sense.

Here we mention a sufficient condition for a curve to be n-ordinary.

Proposition 4. *Let C and n be as above. Then C is n-ordinary if for every connected étale cyclic covering $C' \to C$ of degree n, C' is an ordinary curve.*

Proof. We use the notation of Section 3. For $\alpha \in {}_n\mathfrak{A}$, Lemma 4 in Section 3 shows that $\gamma_\alpha = \dim_{F_q} (H^1(C')^{\chi^{-1}})^{F^m}$ for some connected étale cyclic covering $C' \to C$ of degree n. But F: $H^1(C') \to H^1(C')$ is invertible since C' is ordinary by assumption. Then, a fortiori, F^m: $H^1(C')^{\chi^{-1}} \to H^1(C')^{\chi^{-1}}$ is invertible. Hence we have by Proposition 1,

$$\gamma_\alpha = \dim_{F_q}(H^1(C')^{\chi^{-1}})^{F^m} = \dim_k H^1(C')^{\chi^{-1}} = \dim_k H^1(C, \mathscr{L}(A))$$
$$= \begin{cases} g & (n=1) \\ g-1 & (n>1) \end{cases} \qquad \text{(cf. proof of Lemma 4).}$$

This equality holds for every $\alpha \in {}_n\mathfrak{A}$, i.e. the curve C is n-ordinary.

Until now we considered generalized Hasse-Witt invariants, fixing a curve. Here we let curves vary, fixing genus, and show that "general" curves of given genus are n-ordinary for each fixed natural number n which is prime to p. First we recall the moduli space of curves over k. As before, k denotes an algebraically closed field of characteristic $p>0$. For a non-negative integer g, let $M_g \to \operatorname{Spec} k$ be the coarse moduli scheme of connected complete non-singular algebraic curves of genus g over k. For the precise definition of coarse moduli scheme,see [11]. In particular, for any algebraically closed field Ω which contains k, Ω-valued points of M_g correspond bijectively with isomorphism classes of connected complete non-singular algebraic curves of genus g over Ω. The existence of M_g is shown in [11]. It is known that M_g is an irreducible quasi-projective variety over k (cf. [2], [11]).

Let n be a natural number prime to $p = \operatorname{char} k$, and U_n the subset of M_g consisting of all points which correspond to n-ordinary curves. Then we have

Theorem 2. *The set U_n is a non-empty Zariski-open set of M_g. (Hence U_n is Zariski-dense in M_g since M_g is irreducible.)*

Remark. By Theorem 2, U_n is open in M_g for *each n*. But I do not know whether or not the intersection $\bigcap_{p \nmid n} U_n$ of U_n for *all n* $(p \nmid n)$ is still an open set of M_g.

Theorem 2 will be proved in the following section.

§ 5. Proof of Theorem 2

First we settle the cases $g=0$ and $g=1$. When $g=0$, the projective line $\boldsymbol{P}^1$ is the only one curve of genus zero and is n-ordinary for any n. Hence Theorem 2 is formally true (but trivial) in this case. When $g=1$, all curves of genus one (i.e. elliptic curves) are n-ordinary by definition, if $n \geqq 2$. When $n=1$, it is a well-known fact that 1-ordinary (i.e. ordinary) elliptic curves make an open set in j-line, the coarse moduli variety of elliptic curves.

Hereafter, we assume $g \geqq 2$ and prove Theorem 2. The proof is divided into two parts.

I. Openness of U_n

Since $g \geqq 2$, M_g is obtained in the following way: There is a proper smooth morphism $f: \Gamma \to H$ of varieties over k such that the fibers of f are connected curves of genus g. An algebraic group G acts on $\Gamma \to H$ and M_g is the geometric quotient of H by G. (cf. [2], [11]. We can take as $f: \Gamma \to H$ the universal family of tri-canonically embedded connected complete non-singular curves of genus g ($\Gamma \subset H \times \boldsymbol{P}^{5g-6}$ and $G = PGL(5g-6)$).) Let V_n be the subset of H consisting of all points x for which the fiber $f^{-1}(x)$ is n-ordinary. Then V_n is stable by the action of G and U_n is the quotient set of V_n. Hence it suffices for us to prove that V_n is an open subset of H.

Since $f: \Gamma \to H$ is proper smooth, [9] chap. VI Corollary 4.2 shows that the sheaf $R^1 f_*(\mu_n)$ is locally isomorphic to $(\boldsymbol{Z}/n\boldsymbol{Z})^{2g}$ in the étale topology of H (μ_n is the group of n-th roots of unity. We have $\mu_n \cong \boldsymbol{Z}/n\boldsymbol{Z}$). Hence we can take an open covering $\{U_i\}$ of H in the étale topology such that $g_i^* R^1 f_*(\mu_n) = R^1(f_i)_*(\mu_n) \cong (\boldsymbol{Z}/n\boldsymbol{Z})^{2g}$ holds.

$$\begin{array}{ccc} \Gamma & \longleftarrow & \Gamma \times_H U_i \\ \downarrow f & & \downarrow f_i \\ H & \xleftarrow{g_i} & U_i \end{array}$$

It is sufficient to prove that, for each i, $g_i^{-1}(V_n)$ is open in U_i. Hence, in order to save symbols, we assume that $R^1 f_*(\mu_n) \cong (\boldsymbol{Z}/n\boldsymbol{Z})^{2g}$ holds for $f: \Gamma \to H$ itself, and prove that V_n is open. Further we may assume that $f: \Gamma \to H$ admits a section. For, if f does not have a section, replace $f: \Gamma \to H$ by $g: \Gamma \times_H \Gamma \to \Gamma$ (the diagram below).

$$\begin{array}{ccc} \Gamma & \longleftarrow & \Gamma \times_H \Gamma \\ \downarrow f & & \downarrow g \\ H & \xleftarrow{f} & \Gamma \end{array}$$

This g admits a section (diagonal embedding), and V_n is open in H if and only if $f^{-1}(V_n)$, which consists of all points x of Γ such that the fiber $g^{-1}(x)$ is n-ordinary, is open in Γ. (f is proper smooth, hence a surjective open mapping.) Therefore we assume that $f: \Gamma \longrightarrow H$ has a section.

Concerning an algebraic curve C over k, we see, by Proposition 1 and the definition of γ_α, that $\gamma_\alpha=\begin{cases} g & (n=1) \\ g-1 & (n>1)\end{cases}$ if and only if the map $\mu F^m\colon H^1(C, \mathscr{L}(A)) \to H^1(C, \mathscr{L}(A))$ is invertible (for the notation, see Section 2), which is equivalent to the condition that $F^m\colon H^1(C, \mathscr{L}(A)) \to H^1(C, \mathscr{L}(p^m A)) = H^1(C, (F^m)^*\mathscr{L}(A))$ is invertible ($\mu\colon H^1(C, \mathscr{L}(p^m A)) \to H^1(C, \mathscr{L}(A))$ is always invertible). Hence C is n-ordinary if and only if $F^m\colon H^1(C, \mathscr{L}) \to H^1(C, (F^m)^*\mathscr{L})$ is invertible for every invertible sheaf $\mathscr{L}$ whose order (in the Picard group of C) equals n. We shall prove the openness of V_n using this fact.

From $R^1f_*(\mu_n) \cong (Z/nZ)^{2g}$ we obtain $\mathrm{Pic}(\Gamma/H)_n = \{\xi \in \mathrm{Pic}(\Gamma/H) \mid n\xi = 0\} \cong (Z/nZ)^{2g}$. The homomorphism $\mathrm{Pic}(\Gamma) \to \mathrm{Pic}(\Gamma/H)$ is surjective since $f\colon \Gamma \to H$ has a section (cf. [4]). Therefore we can choose a finite number of elements $\mathscr{L}_1, \cdots, \mathscr{L}_\lambda \in \mathrm{Pic}(\Gamma)$ such that

(*) the image of $\mathscr{L}_i$ in $\mathrm{Pic}(\Gamma/H)$ has order n ($i=1, \cdots, \lambda$), and each element of order n in $\mathrm{Pic}(\Gamma/H)$ is the image of $\mathscr{L}_i \in \mathrm{Pic}(\Gamma)$ for some $i=1, \cdots, \lambda$.

For each $y \in H$ and invertible sheaf $\mathscr{L}$ over Γ, put $\Gamma_y = f^{-1}(y)$ and $\mathscr{L}_y = \mathscr{L}|_{\Gamma_y}$. Then for every $y \in H$ and $i=1, \cdots, \lambda$, $(\mathscr{L}_i)_y$ is an invertible sheaf of order n over the curve Γ_y and further, because of the property (*), $(\mathscr{L}_i)_y$ ($i=1, \cdots, \lambda$) give all the elements of order n in $\mathrm{Pic}(\Gamma_y)$. (Since $R^1f_*(\mu_n)$ is a constant sheaf, we have $\mathrm{Pic}(\Gamma/H)_n \rightrightarrows \mathrm{Pic}(\Gamma_y)_n$.) For each $i=1, \cdots, \lambda$, we have

$$\dim_{\kappa(y)} H^1(\Gamma_y, (\mathscr{L}_i)_y) = \dim_{\kappa(y)} H^1(\Gamma_y, ((F^m)^*\mathscr{L}_i)_y) = \begin{cases} g & (n=1) \\ g-1 & (n>1)\end{cases},$$

where $\kappa(y)$ denotes the residue field of y (F is the (p-th power) Frobenius morphism and m is the order of p in $(Z/nZ)^\times$). Therefore by [10] p. 50 Corollary 2, there exists a covering $H=\bigcup_{j\in I} W_j$ ($W_j = \mathrm{Spec}\, R_j$) of H by affine open subsets such that

$$H^1(\Gamma|_{W_j}, \mathscr{L}|_{W_j}) \cong R_j^l \qquad \left(l=\begin{cases} g & (n=1) \\ g-1 & (n>1)\end{cases}\right)$$

holds for each $j \in I$ and $\mathscr{L} \in \{\mathscr{L}_1, \cdots, \mathscr{L}_\lambda, (F^m)^*\mathscr{L}_1, \cdots, (F^m)^*\mathscr{L}_\lambda\}$. For every $j \in I$ and $i=1, \cdots, \lambda$, we have a p^m-linear map

$$F^m\colon H^1(\Gamma|_{W_j}, \mathscr{L}_i|_{W_j}) \longrightarrow H^1(\Gamma|_{W_j}, (F^m)^*\mathscr{L}_i|_{W_j}).$$

Since we have

$$H^1(\Gamma|_{W_j}, \mathscr{L}_i|_{W_j}) \cong H^1(\Gamma|_{W_j}, (F^m)^*\mathscr{L}_i|_{W_j}) \cong R_j^l,$$

we obtain, fixing R_j-bases of $H^1(\Gamma|_{W_j}, \mathscr{L}_i|_{W_j})$ and $H^1(\Gamma|_{W_j}, (F^m)^*\mathscr{L}_i|_{W_j})$, the determinant $d_{i,j} \in R_j$ of the map F^m above. Put $d_j = \prod_{i=1}^{\lambda} d_{i,j} \in R_j$. Then, $d_j \neq 0$ at $y \in W_j = \operatorname{Spec} R_j$ if and only if

$$F^m: H^1(\Gamma_y, (\mathscr{L}_i)_y) \longrightarrow H^1(\Gamma_y, (F^m)^*(\mathscr{L}_i)_y)$$

is invertible for every $i=1, \cdots, \lambda$. Hence $d_j \neq 0$ at $y \in W_j$ is equivalent to the condition that the curve Γ_y is n-ordinary, because $(\mathscr{L}_i)_y$ ($i=1, \cdots, \lambda$) give all the invertible sheaves of order n over Γ_y. In other words, we have $V_n \cap W_j = \{y \in W_j \mid d_j \neq 0 \text{ at } y\}$, and consequently $V_n \cap W_j$ is open in W_j for all $j \in I$. Therefore V_n is open in H (recall $H = \bigcup_{j \in I} W_j$) and hence U_n is open in M_g as we wanted to prove.

II. Non-emptiness of U_n

In [8], Koblitz used the degenerate curve C_0 below to show the existence of an ordinary (i.e. 1-ordinary) curve of genus g. Here we start from the curve C_0 and construct an n-ordinary (non-singular) curve as a deformation of C_0.

Let C_0 be a stable curve of genus g over k of the following form (for the definition of stable curve, see [2]):

$$C_0 = E_1 \cup \cdots \cup E_g,$$

(*a*) each E_i is an ordinary elliptic curve over k.

(*b*) for $i<j$, $E_i \cap E_j = \begin{cases} P_i & j=i+1 \\ \phi & \text{otherwise} \end{cases}$.

(*c*) each P_i is an ordinary double point of C_0.

Concerning this curve C_0, we have

Proposition 5. (i) $\operatorname{Pic}(C_0)_n \cong (Z/nZ)^{2g}$.

(ii) *Let $f: C_0' \to C_0$ be an étale covering of degree n and $F: C_0' \to C_0'$ the (p-th power) Frobenius morphism. Then*

$$F = F^*: H^1(C_0', \mathcal{O}_{C_0'}) \longrightarrow H^1(C_0', \mathcal{O}_{C_0'}),$$

the p-linear map induced by F, is invertible.

Proof. (i) Let $\mathcal{O}_{P_i}^\times$ ($i=1, \cdots, g-1$) be a sheaf over C_0 whose stalk at $x \in C_0$ is given by

$$\mathcal{O}_{P_i,x}^\times = \begin{cases} k^\times & x = P_i \\ \{1\} & x \neq P_i \end{cases}.$$

Then there is an exact sequence

$$0 \longrightarrow \mathcal{O}_{C_0}^\times \longrightarrow \bigoplus_{i=1}^{g} \mathcal{O}_{E_i}^\times \longrightarrow \bigoplus_{i=1}^{g-1} \mathcal{O}_{P_i}^\times \longrightarrow 0.$$

From the cohomology sequence of this exact sequence and the exactness of

$$0 \longrightarrow H^0(\mathcal{O}_{C_0}^{\times}) \longrightarrow \bigoplus_{i=1}^{g} H^0(\mathcal{O}_{E_i}^{\times}) \longrightarrow \bigoplus_{i=1}^{g-1} H^0(\mathcal{O}_{P_i}^{\times}) \longrightarrow 0,$$

we have

$$H^1(\mathcal{O}_{C_0}^{\times}) \cong \bigoplus_{i=1}^{g} H^1(\mathcal{O}_{E_i}^{\times}).$$

Hence we obtain

$$\mathrm{Pic}\,(C_0)_n = H^1(\mathcal{O}_{C_0}^{\times})_n \cong \bigoplus_{i=1}^{g} H^1(\mathcal{O}_{E_i}^{\times})_n \cong (Z/nZ)^{2g}.$$

(ii) Since f: $C_0' \to C_0$ is an étale covering, every singular point of C_0' lies over some P_i $(i=1, \cdots, g-1)$ and is an ordinary double point. Further, each irreducible component of C_0' is an ordinary elliptic curve since it is a finite étale covering of some E_i $(i=1, \cdots, g)$. Consequently, C_0' is of the form

$$C_0' = E_1' \cup \cdots \cup E_l',$$

where each E_i' is an ordinary elliptic curve and $E_i' \cap E_j'$ $(i \neq j)$ consists of a finite number of ordinary double points. Put $f^{-1}(P_i) = \{Q_{n(i-1)+1}, \cdots, Q_{ni}\}$ $(i=1, \cdots, g-1)$. Then $Q_1, \cdots, Q_{n(g-1)}$ are ordinary double points of C_0' and give all the singular points of C_0'. For each $i=1, \cdots, n\,(g-1)$, define a sheaf $\mathcal{O}_{Q_i}$ over C_0' by

$$\mathcal{O}_{Q_i,x} = \begin{cases} k & x = Q_i \\ \{0\} & x \neq Q_i \end{cases} \qquad \text{for each } x \in C_0'.$$

From the exact sequence

$$0 \longrightarrow \mathcal{O}_{C_0'} \longrightarrow \bigoplus_{i=1}^{l} \mathcal{O}_{E_i'} \longrightarrow \bigoplus_{i=1}^{n(g-1)} \mathcal{O}_{Q_i} \longrightarrow 0,$$

we have a commutative diagram

$$\begin{array}{ccccccccc}
\bigoplus_i H^0(\mathcal{O}_{Q_i}) & \longrightarrow & H^1(\mathcal{O}_{C_0'}) & \longrightarrow & \bigoplus_i H^1(\mathcal{O}_{E_i'}) & \longrightarrow & 0 & & \text{(exact)} \\
\downarrow{\scriptstyle F} & & \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle F} & & & & \\
\bigoplus_i H^0(\mathcal{O}_{Q_i}) & \longrightarrow & H^1(\mathcal{O}_{C_0'}) & \longrightarrow & \bigoplus_i H^1(\mathcal{O}_{E_i'}) & \longrightarrow & 0 & & \text{(exact).}
\end{array}$$

Here F: $H^0(\mathcal{O}_{Q_i}) \longrightarrow H^0(\mathcal{O}_{Q_i})$ is surjective since it is the p-th power map of $k = H^0(\mathcal{O}_{Q_i})$, and F: $H^1(\mathcal{O}_{E_i'}) \to H^1(\mathcal{O}_{E_i'})$ is also surjective since E_i' is an ordinary elliptic curve. Therefore, as is easily checked by diagram chase, F: $H^1(\mathcal{O}_{C_0'}) \to H^1(\mathcal{O}_{C_0'})$ is surjective, i.e. it is invertible.

Put $R = k[[t_1, \cdots, t_N]]$ $(N = g-1)$ and let s and η be respectively the closed and generic points of Spec R. Then by the results of [2] Section 1, there exists a scheme $\mathcal{C} \to \operatorname{Spec} R$ with the following properties:

(i) $\mathcal{C} \to \operatorname{Spec} R$ is a stable curve of genus g.

(ii) Denote by $\mathcal{C}_s$ and $\mathcal{C}_\eta$ the fibers of $\mathcal{C} \to \operatorname{Spec} R$ at s and η. Then $\mathcal{C}_s$ is isomorphic to the curve C_0 defined above, and $\mathcal{C}_\eta$ is non-singular.

Put $\kappa = k((t_1, \cdots, t_N))$ and let $\bar{\kappa}$ be the algebraic closure of κ. We shall show that $C = \mathcal{C}_\eta \times_{\operatorname{Spec} \kappa} \operatorname{Spec} \bar{\kappa}$ is an n-ordinary curve. We first prove

Lemma 5. *Let $C' \to C$ be a connected étale cyclic covering of degree n. Then there exists a connected étale cyclic covering $\mathcal{C}' \to \mathcal{C}$ of degree n such that $\mathcal{C}'_\eta \times \operatorname{Spec} \bar{\kappa} \to \mathcal{C}_\eta \times \operatorname{Spec} \bar{\kappa} = C$ is isomorphic to $C' \to C$.*

Proof. By [3] exp. X Corollaire 2.3, the specialization homomorphism $\pi_1(C) \to \pi_1(\mathcal{C}_s) \cong \pi_1(\mathcal{C})$ is surjective. Hence $\operatorname{Hom}(\pi_1(\mathcal{C}_s), \boldsymbol{Z}/n\boldsymbol{Z}) \to \operatorname{Hom}(\pi_1(C), \boldsymbol{Z}/n\boldsymbol{Z})$ is injective. On the other hand, $\operatorname{Hom}(\pi_1(\mathcal{C}_s), \boldsymbol{Z}/n\boldsymbol{Z}) \cong \operatorname{Pic}(C_0)_n \cong (\boldsymbol{Z}/n\boldsymbol{Z})^{2g}$ holds by Proposition 5 (i) (recall $\mathcal{C}_s \cong C_0$), and $\operatorname{Hom}(\pi_1(C), \boldsymbol{Z}/n\boldsymbol{Z})$ is also isomorphic to $(\boldsymbol{Z}/n\boldsymbol{Z})^{2g}$ since C is non-singular of genus g. Therefore, $\operatorname{Hom}(\pi_1(\mathcal{C}), \boldsymbol{Z}/n\boldsymbol{Z}) = \operatorname{Hom}(\pi_1(\mathcal{C}_s), \boldsymbol{Z}/n\boldsymbol{Z}) \to \operatorname{Hom}(\pi_1(C), \boldsymbol{Z}/n\boldsymbol{Z})$ is an injective homomorphism between finite groups of the same order, hence an isomorphism. In particular it is surjective, which is nothing but the assertion of Lemma 5.

Let $C' \to C$ be an arbitrary connected étale cyclic covering of degree n. Then by Lemma 5, it is obtained from a connected étale cyclic covering $\mathcal{C}' \to \mathcal{C}$ of degree n. Consider the morphism f: $\mathcal{C}' \to \operatorname{Spec} R$. By Corollary 2 of [10] p. 50, the sheaf $R^1 f_*(\mathcal{O}_{\mathcal{C}'})$ is locally free on Spec R. But R is a local ring, and hence $R^1 f_*(\mathcal{O}_{\mathcal{C}'})$ is free over Spec R, i.e. $H^1(\mathcal{C}', \mathcal{O}_{\mathcal{C}'})$ is a free R-module. Choose an R-basis of $H^1(\mathcal{C}', \mathcal{O}_{\mathcal{C}'})$ and let $d_F \in R$ be the determinant of the Frobenius morphism F: $H^1(\mathcal{C}', \mathcal{O}_{\mathcal{C}'}) \to H^1(\mathcal{C}', \mathcal{O}_{\mathcal{C}'})$ with respect to this basis. Then Proposition 5 (ii) shows that $d_F \neq 0$ at $s \in \operatorname{Spec} R$, which means $d_F \in R^\times$ since s is the closed point of Spec R. In particular, $d_F \neq 0$ at $\eta \in \operatorname{Spec} R$ and hence the Frobenius morphism F: $H^1(C', \mathcal{O}_{C'}) \to H^1(C', \mathcal{O}_{C'})$ is invertible (recall $C' = \mathcal{C}'_\eta \times \operatorname{Spec} \bar{\kappa}$), i.e. C' is an ordinary curve. Therefore by Proposition 4 in Section 4, the curve C is n-ordinary. Thus we have shown that U_n has at least one $\bar{\kappa}$-valued point. Hence the set U_n is not empty.

Thus, by the two steps I and II, the proof of Theorem 2 is completed.

§ 6. Examples

Given a connected complete non-singular curve C, we can calculate the generalized Hasse-Witt invariants of C by using Proposition 2 in Section 2. In this section, the results of computations are given for the case $p=2$, $g=2$, $n=3$. (The process of computations is omitted here. Details are explained in [12].) Examples of generalized Hasse-Witt invariants are also given in [7].

Let C be a connected complete non-singular algebraic curve of genus two over an algebraically closed field k of characteristic two. We shall give the values of γ_α's for $\alpha \in {}_3\mathfrak{A}$. Since the genus of C equals two, we have $\gamma_\alpha=0$ or 1 for $\alpha \in {}_3\mathfrak{A}$. Then, if we denote by N the number of connected étale $G_{3,2}$-coverings of C ($G_{3,2}\cong$the alternating group of degree 4), we have, by Theorem 1,

$$N=\sum_{\alpha\in {}_3\mathfrak{A}} \frac{q^{\gamma_\alpha}-1}{q-1}=\#\{\alpha \in {}_3\mathfrak{A} \mid \gamma_\alpha=1\}.$$

The set ${}_3\mathfrak{A}$ consists of 40 elements, hence the curve C is 3-ordinary if and only if $N=40$.

Connected complete non-singular curves of genus two over k (char $k=2$) are classified into three types (I, II and III below) according to the number of Weierstrass points. We give the number N above, for each curve.

I. $y^2+y=x^5+Ax^3$ ($A \in k$).

For every $A \in k$, $N=40$.

II. $y^2+y=Ax^3+\dfrac{B}{x}$ ($A, B \in k^\times$).

For every $A, B \in k^\times$, $N=40$.

III. $y^2+y=Ax+\dfrac{B}{x}+\dfrac{C}{x+1}$ ($A, B, C \in k^\times$).

In this case, we have

(a) When $(A+B+C)^3+ABC\neq 0$,
$N=40$.

(b) When $(A+B+C)^3+ABC=0$ and $(A+B)(B+C)(C+A)\neq 0$,
$N=39$.

(c) When $(A+B+C)^3+ABC=(A+B)(B+C)(C+A)=0$
(i.e. $A=B=C$), $N=38$.

The classical Hasse-Witt invariants of curves of type I, II and III are respectively equal to 0, 1 and 2. Hence, curves of type I and II are 3-ordinary but not 1-ordinary. Conversely, curves of type III (b) and (c) give examples of curves which are 1-ordinary but not 3-ordinary. Curves of type III (a) are both 1- and 3-ordinary.

§ 7. A recent result

In this section a result of the author will be mentioned, which was obtained after the Symposium.

Let C be a connected complete non-singular curve of genus g over an algebraically closed field k of characteristic $p>0$. Put

$$\mathscr{G}=\{G \mid G=\mathrm{Gal}(C'/C) \text{ for a connected étale finite Galois covering } C'\longrightarrow C\},$$

i.e. $\mathscr{G}$ is the set of all finite groups G such that $G=\pi_1(C)/N$ for some open normal subgroup N of $\pi_1(C)$. When $g\geqq 2$, the set $\mathscr{G}$ has not yet been determined explicitly. But the result of Grothendieck referred to in Section 1 gives a necessary condition for a finite group to belong to $\mathscr{G}$;

($\sharp$) If $G\in\mathscr{G}$, then G is a quotient group of Γ_g.

(If $p=\mathrm{char}\, k$ does not divide the order of G, the converse of ($\sharp$) is also true.)

In [13] the author obtained another necessary condition. Namely,

Theorem 3. *Let G be a finite group and I_G the augmentation ideal of its group algebra over k;*

$$I_G=\{\sum_{\sigma\in G} a_\sigma\cdot\sigma\in k[G] \mid \sum_{\sigma\in G} a_\sigma=0\}.$$

If G belongs to $\mathscr{G}$, there exists a surjective $k[G]$-homomorphism $k[G]^g\to I_G$ where g is the genus of C.

If the order of G is prime to $p=\mathrm{char}\, k$, I_G is a direct summand of $k[G]$ as a $k[G]$-module and there always exists a surjective homomorphism $k[G]\to I_G$. Hence Theorem 3 poses no restriction on such groups. But if the order of G is a multiple of p, there does not always exist a surjective homomorphism $k[G]^g\to I_G$, and Theorem 3 gives some information about the set $\mathscr{G}$. For example, take $G=(\boldsymbol{Z}/p\boldsymbol{Z})^d$ where d is a natural number. Then, a surjective homomorphism $k[G]^g\to I_G$ exists if and only if $d\leqq g$. On the other hand, this group G is a quotient of Γ_g if and only if $d\leqq 2g$. Thus the necessary condition given in Theorem 3 is not contained in the condition ($\sharp$) above. (Now we have concluded from Theorem 3 that the inequality $d \leqq g$ holds if $(Z/pZ)^d \in \mathscr{G}$. But this fact itself is well-known and can be derived from Hasse-Witt theory.) It seems a difficult problem to determine the minimal number of generators of I_G as a $k[G]$-module, and hence I do not know to what extent Theorem 3 restricts the set $\mathscr{G}$.

References

[1] P. Cartier, Une nouvelle opération sur les formes différentielles, C. R. Acad. Sci. Paris, **244** (1957), 426–428.
[2] P. Deligne and D. Mumford, The irreducibility of the space of curves of given genus, Publ. Math. IHES, **36** (1969), 75–109.
[3] A. Grothendieck, Revêtements étales et groupe fondamental (SGA 1), Springer lecture note **224** (1971).
[4] ——, Les schema de Picard: Theorèmes d'existence, Sem. Bourbaki, exp. **232** (1962).
[5] M. Hall, Jr., The theory of groups, Macmillan, New York (1959).
[6] H. Hasse and E. Witt, Zyklische unverzweigte Erweiterungskörper vom Primzahlgrad p über einem algebraischen Funktionenkörper der Charakteristik p, Monatshefte Math. Phys., **43** (1936), 477–492.
[7] H. Katsurada, Generalized Hasse-Witt invariants and unramified Galois extensions of an algebraic function field, J. Math. Soc. Japan, **31** (1979), 101–125.
[8] N. Koblitz, P-adic variation of the zeta function over families of varieties defined over finite fields, Compositio Math., **31** (1975), 119–218.
[9] J. S. Milne, Etale cohomology, Princeton Univ. Press, Princeton (1980).
[10] D. Mumford, Abelian varieties, Oxford Univ. Press, London (1970).
[11] D. Mumford and J. Fogarty, Geometric invariant theory (second enlarged edition), Springer Verlag, Berlin-Heidelberg-New York (1982).
[12] S. Nakajima, Generalized Hasse-Witt invariants and unramified extensions of function fields (in Japanese), Master thesis, Univ. of Tokyo (1980).
[13] ——, On Galois module structure of the cohomology groups of an algebraic variety (to appear).
[14] I. Šafarevič, On p-extensions, Math. Sbornik, **20** (1947), 351–363 (In Russian). (AMS transl. ser. 2, **4** (1956), 59–72).
[15] J.-P. Serre, Sur la topologie des variétés algébriques en caractéristique p, Symposium internacional de topologia algebraica, Univ. of Mexico and UNESCO, Mexico City (1958), 24–53.
[16] ——, Groupes algébriques et corps de classes, Hermann, Paris (1959).

Department of Mathematics
Faculty of Science
University of Tokyo
Hongo, Tokyo 113
Japan