RIMS-2000

The Generic Number of Nilpotent Ordinary Indigenous Bundles in Characteristic Three

By

Yuichiro HOSHI

July 2026

京都大学　数理解析研究所

RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES

KYOTO UNIVERSITY, Kyoto, Japan

The Generic Number of Nilpotent Ordinary Indigenous Bundles in Characteristic Three

Yuichiro Hoshi

July 2026

Abstract. — In the present paper, we study nilpotent ordinary indigenous bundles, which are among the main objects in the theory of ordinary hyperbolic curves, on projective smooth hyperelliptic curves in characteristic three. By means of an explicit computation of Cartier operators, we establish an explicit formula for the number of isomorphism classes of nilpotent ordinary indigenous bundles over a general projective smooth curve over an algebraically closed field of characteristic three. The present paper thereby reproduces, by an entirely different and elementary method, the number obtained via the theory of molecules, which had hitherto been available only through a degeneration procedure.

Contents

Introduction

The theory of ordinary hyperbolic curves initiated by S. Mochizuki [cf. [9], [10]] provides a p-adic and arithmetic analogue of the theory of uniformization of hyperbolic Riemann surfaces. One central object in this theory is the notion of an indigenous bundle. In the remainder of the present Introduction, let p be an odd prime number, k an algebraically closed field of characteristic p, and X a projective smooth curve of genus ≥ 2 over k. Then an *indigenous bundle* on X [cf. [9, Chapter I, Definition 2.2]] is defined to be a pair $(\pi\colon P \to X, \nabla_P)$ that consists of a $\mathbb{P}^1$-bundle $\pi\colon P \to X$ over X and a connection ∇_P on P relative to X/k [i.e., a PD-connection in the sense of [6, Definition 4.1, (iii)], [7, Definition 2.5]] such that the Kodaira–Spencer homomorphism arising from the Hodge section $\sigma\colon X \to P$ is an isomorphism. This notion was introduced by R. C. Gunning [cf. [2, §2]] and makes it possible to capture the uniformization of a Riemann surface in an algebro-geometric framework.

2020 Mathematics Subject Classification. — 14G17.
Key words and phrases. — hyperbolic ordinariness, p-adic Teichmüller theory, nilpotent ordinary indigenous bundle, hyperelliptic curve, Cartier operator.

Let $(\pi\colon P \to X, \nabla_P)$ be an indigenous bundle on X. Write $\mathcal{P}\colon \Phi^*\tau_{X/k} \to \pi_*\tau_{P/X}$ — where we write Φ for the relative Frobenius morphism of X/k and "$\tau_{(-)}$" for the tangent sheaf of "$(-)$" — for the *p-curvature homomorphism* determined by the connection ∇_P. Then we shall say that the indigenous bundle $(\pi\colon P \to X, \nabla_P)$ is

- *nilpotent* if the square of $\mathcal{P}$ is zero [cf. [9, Chapter II, Definition 2.4]];
- *admissible* if $\mathcal{P}$ has no zero [cf. [9, Chapter II, Definition 2.4]].

The *supersingular divisor* of a nilpotent admissible indigenous bundle — a fundamental invariant, defined as half of the zero divisor of the composite determined by the p-curvature homomorphism and the Hodge section [cf. [9, Chapter II, Proposition 2.6, (3)]] — in fact completely determines the isomorphism class of the indigenous bundle [cf. [9, Chapter II, Proposition 2.6, (4)]]. Moreover, we shall say that a nilpotent indigenous bundle is *ordinary* [cf. [9, Chapter II, Definition 3.1]] if the Frobenius induced on $H^1(X, \tau_{X/k})$ [cf. the discussion following [9, Chapter II, Lemma 2.11]] is an isomorphism.

We shall say that X is *hyperbolically ordinary* if X admits a nilpotent ordinary indigenous bundle [cf. [9, Chapter II, Definition 3.3]]. The hyperbolic ordinariness of a curve forms the point of departure of the theory of ordinary hyperbolic curves. Thus, the following problem [cf. [10, Introduction, §2.1, (1)]] lies at the foundation of p-adic Teichmüller theory: Is every hyperbolic curve in odd characteristic hyperbolically ordinary? Mochizuki has shown that a general curve of arbitrary type is hyperbolically ordinary [cf. [9, Chapter II, Corollary 3.8]].

With regard to this fundamental problem, affirmative results have been accumulated for individual types. In characteristic three, the author of the present paper characterized the supersingular divisors of the nilpotent admissible/ordinary indigenous bundles by means of Cartier operators [cf. [3, Theorem 5.2, (i), (ii)]], thereby opening the way to explicit computation. By means of this characterization, several curves of low type were shown to be hyperbolically ordinary [cf. [3], [4], [8]]. In particular, every projective smooth hyperelliptic curve of genus ≤ 5 in characteristic three was shown to be hyperbolically ordinary [cf. [5, Theorem A]]. On the other hand, with regard to the problem of counting the nilpotent ordinary indigenous bundles over a general curve, although the number, for an arbitrary genus g, has been determined in [10, Chapter V] by means of the combinatorics of "molecules", this number is given only through a degeneration procedure, and, moreover, formulae have been limited to low type [10, Chapter V, Corollary 1.3]. Even in characteristic three, no closed formula for the number of nilpotent ordinary indigenous bundles over a general curve of arbitrary genus has been known.

The main result of the present paper establishes an explicit formula for the number of nilpotent ordinary indigenous bundles over a general curve of arbitrary genus in characteristic three [cf. Corollary 5.3, Corollary 5.4]:

Theorem A. — *Let $g \geq 2$ be an integer, and let k be an algebraically closed field of characteristic three. Then there exists a projective smooth hyperelliptic curve X of genus g over k such that the number of isomorphism classes of nilpotent ordinary indigenous bundles over X/k is given by*

$$\frac{3^g - 1}{2} + (2^{2g} - 1) \cdot \frac{3^{g-1} - 1}{2}.$$

THEOREM B. — *Let $g \geq 2$ be an integer, and let k be an algebraically closed field of characteristic three. Then the number of isomorphism classes of nilpotent ordinary indigenous bundles over a general projective smooth curve of genus g over k is given by*

$$\frac{3^g - 1}{2} + (2^{2g} - 1) \cdot \frac{3^{g-1} - 1}{2}.$$

The key to the proof is the explicit computation of Cartier operators in characteristic three. Following [3], the nilpotent ordinary indigenous bundles are governed by the Cartier eigenforms possibly twisted by invertible sheaves of order two [cf. [3, Definition A.8, (ii)]], and the supersingular divisor appears as the zero divisor of the Cartier eigenform under discussion. Thus, counting the nilpotent ordinary indigenous bundles reduces to counting the Cartier eigenforms whose zero divisor is reduced. The hyperelliptic setting "$y^2 = f(x)$" makes it possible to write the Cartier operators down explicitly as a homomorphism in terms of the coordinates of the branch points — that is to say, as the image of a homomorphism that arises from products of polynomials. If one takes the branch locus to be general, then the polynomials that determine the Cartier eigenforms that appear are separable, hence the zero divisors reduced, and the number under consideration is determined. In this sense, hyperellipticity is merely a concrete scaffold that makes it possible to carry the computation of Cartier operators to completion and is not the conceptual core of the assertion itself.

The shape of the formula reflects the structure of the 2-torsion points of the Jacobian variety. The first term $(3^g - 1)/2 = \#\mathbb{P}^{g-1}(\mathbb{F}_3)$ is the contribution of the trivial invertible sheaf $\mathcal{O}_X$, and the second term is the sum, over the $2^{2g} - 1$ nontrivial invertible sheaves of order two, of the respective contributions $\#\mathbb{P}^{g-2}(\mathbb{F}_3)$; this decomposition arises from the even decompositions [cf. Definition 4.1, (iii)] of the $2g + 2$ branch points — equivalently [cf. Lemma 4.8, (ii)], from the connected finite étale coverings of X of degree two. The resulting number agrees with the count obtained from Mochizuki's theory of molecules. In the case where $g = 2$, the value 19 obtained above is none other than the value $p(2p^2+1)/3$ of [10, Chapter V, Corollary 1.3, (3)] at $p = 3$. The present paper reproduces, by the independent and elementary method of the direct computation of Cartier operators, as a uniform closed form, the number that [10, Chapter V] may give only through an algorithm via totally degenerate curves. In particular, Theorem B may be regarded as an explicit closed-form evaluation, in the case of characteristic three, of the number. It is, moreover, worthy of note that, although for $g \geq 3$ a projective smooth hyperelliptic curve is not general in the moduli of curves of genus g [indeed, the hyperelliptic locus is of codimension $g-2$], a general projective smooth hyperelliptic curve nevertheless achieves, as regards the number of nilpotent ordinary indigenous bundles, the same number as a general curve.

The present paper is organized as follows. In §1, we determine the dimension of the image of a k-linear homomorphism arising from products of polynomials [cf. Lemma 1.4], which forms the linear-algebraic core of the subsequent computations. In §2 and §3, we introduce, respectively, the notion of a CE-admissible element and that of a CE-admissible pair in characteristic three and also establish the separability and reducedness under consideration for a general branch locus. In §4, we translate these algebraic results into the language of the Cartier eigenforms on a projective smooth hyperelliptic curve and their zero divisors. Finally, in §5, we give a proof of the main results.

Acknowledgments

This research was supported by JSPS KAKENHI Grant Number 24K06668 and by the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University. This research was also supported by the CNRS France-Japan "Arithmetic and Homotopic Galois Theory" International Research Network.

1. The Image of a Homomorphism Arising from Products of Polynomials

In the present §1, we determine the dimension of the image of a certain k-linear homomorphism that arises from products of polynomials [cf. Lemma 1.4, (iv), below].

In the present §1, let

- p be an odd prime number,
- g a nonnegative integer, and
- k an algebraically closed field of characteristic p.

Definition 1.1. — Let i be a nonnegative integer, and let $f(z) \in k[z]$ be a polynomial in the variable z. Then we shall write $C_i^{[z]}(f(z)) \in k$ for the coefficient of z^i in $f(z)$.

Definition 1.2. — Let n be a nonnegative integer, and let $a = (a_1, \ldots, a_n)$ be an element of the direct product $k^{\times n}$ of n copies of k.

(i) We shall write

$$M_a(t) \stackrel{\text{def}}{=} a_1 + a_2 t + \cdots + a_n t^{n-1} + t^n,$$

$$P_a(t) \stackrel{\text{def}}{=} a_1 + a_2 t + \cdots + a_n t^{n-1} = M_a(t) - t^n \in k[t]$$

— where t is an indeterminate.

(ii) We define $P_{a,0}(t), \ldots, P_{a,p-1}(t) \in k[t]$ to be the polynomials uniquely determined by the equality

$$P_a(t) = \sum_{i=0}^{p-1} \big(t^i \cdot P_{a,i}(t^p)\big).$$

(iii) We define

$$G_a(t) \stackrel{\text{def}}{=} \gcd\big(P_{a,0}(t), \ldots, P_{a,p-1}(t)\big)$$

— where we normalize $G_a(t)$ so as to be monic [whenever $G_a(t)$ is nonzero].

(iv) Suppose that $G_a(t) \neq 0$. Then, for each $i \in \{0, 1, \ldots, p-1\}$, we define the polynomial $Q_{a,i}(t) \in k[t]$ that is uniquely determined by the equality

$$P_{a,i}(t) = G_a(t) \cdot Q_{a,i}(t).$$

Definition 1.3.

(i) We shall write

$$C \stackrel{\text{def}}{=} C(g) \stackrel{\text{def}}{=} k^{\times(2g+2)}, \quad D \stackrel{\text{def}}{=} D(g) \stackrel{\text{def}}{=} k^{\times g}, \quad F \stackrel{\text{def}}{=} F(g) \stackrel{\text{def}}{=} k^{\times g}.$$

(ii) We shall write

$$\phi\colon C \times D \longrightarrow F; \quad (c,d) \longmapsto \Big(C^{[t]}_{p-1}\big(M_c(t)\cdot P_d(t)\big), \ldots, C^{[t]}_{pg-1}\big(M_c(t)\cdot P_d(t)\big)\Big)$$

for the map that assigns to each element $(c,d) \in C \times D$ the element of F whose i-th component — where i is an element of $\{1, \ldots, g\}$ — is given by the coefficient of t^{pi-1} in the polynomial $M_c(t) \cdot P_d(t) \in k[t]$.

(iii) For each $d \in D$, we shall write

$$\phi_d\colon C \longrightarrow F$$

for the map given by $c \mapsto \phi(c,d)$ and

$$\psi_d\colon C \longrightarrow F$$

for the map [which is necessarily a k-linear homomorphism] given by $c \mapsto \phi(c,d) - \phi(0,d)$.

Lemma 1.4. — *Let d be a nonzero element of D. Then the following assertions hold:*

(i) *Let i be an element of $\{1, \ldots, g\}$, and let c be an element of C. Then the i-th component of $\psi_d(c)$ coincides with $C^{[t]}_{pi-1}(P_c(t) \cdot P_d(t))$.*

(ii) *The image of ψ_d coincides with the sub-k-space of F that consists of*

$$\left(C^{[t]}_0\left(\sum_{j=0}^{p-1}\big(h_j(t)\cdot P_{d,p-1-j}(t)\big)\right), \ldots, C^{[t]}_{g-1}\left(\sum_{j=0}^{p-1}\big(h_j(t)\cdot P_{d,p-1-j}(t)\big)\right)\right)$$

— where $h_j(t) \in k[t]$ ranges over the polynomials of degree $\leq \lfloor (2g+1-j)/p \rfloor$ for each $j \in \{0, \ldots, p-1\}$.

(iii) *The sub-k-space of $k[t]$ that consists of*

$$\sum_{j=0}^{p-1}\big(h_j(t)\cdot Q_{d,p-1-j}(t)\big)$$

— where $h_j(t) \in k[t]$ ranges over the polynomials of degree $\leq \lfloor (2g+1-j)/p \rfloor$ for each $j \in \{0, \ldots, p-1\}$ — coincides with the sub-k-space of $k[t]$ of polynomials of degree $\leq \lfloor (2g+2+\deg(P_d(t)))/p \rfloor - 1 - \deg(G_d(t))$.

(iv) *The image of the k-linear homomorphism $\psi_d\colon C \to F$ is of dimension $\lfloor (2g+2+\deg(P_d(t)))/p \rfloor - \deg(G_d(t))$.*

Proof. — Assertion (i) follows immediately from the various definitions involved. Next, we verify assertion (ii). Let c be an element of C. Then since [it is immediate that] the equalities $P_c(t) = \sum_{i=0}^{p-1} t^i \cdot P_{c,i}(t^p)$ and $P_d(t) = \sum_{i=0}^{p-1} t^i \cdot P_{d,i}(t^p)$ hold, one verifies easily that the sum of the terms of $P_c(t) \cdot P_d(t)$ whose degrees are $\equiv p-1$ modulo p is given by

$$t^{p-1} \cdot \sum_{j=0}^{p-1} \bigl(P_{c,j}(t^p) \cdot P_{d,p-1-j}(t^p)\bigr).$$

In particular, the coefficient $C^{[t]}_{pi-1}(P_c(t) \cdot P_d(t))$ is given by

$$C^{[t]}_{i-1}\left(\sum_{j=0}^{p-1} \bigl(P_{c,j}(t) \cdot P_{d,p-1-j}(t)\bigr)\right).$$

Thus, since [one verifies easily that] the set

$$\{\, \bigl(P_{c,0}(t), \ldots, P_{c,p-1}(t)\bigr) \mid c \in C \,\}$$

coincides with the set that consists of

$$\bigl(h_0(t), \ldots, h_{p-1}(t)\bigr)$$

— where $h_j(t) \in k[t]$ ranges over the polynomials of degree $\leq \lfloor (2g+1-j)/p \rfloor$ for each $j \in \{0, \ldots, p-1\}$ — assertion (ii) follows from assertion (i). This completes the proof of assertion (ii). Assertion (iii) follows immediately from the [easily verified] equality $\gcd(Q_{d,0}(t), \ldots, Q_{d,p-1}(t)) = 1$, together with a comparison of the degrees of the various polynomials that appear in the argument.

Finally, we verify assertion (iv). Write e for the uniquely determined maximal nonnegative integer such that $G_d(t)$ is divisible by t^e. Then since [it is immediate that] $G_d(t)/t^e$ is invertible in $k[[t]]$, one concludes immediately from assertions (ii), (iii) that the dimension of the image of the k-linear homomorphism $\psi_d \colon C \to F$ is given by

$$\min\Bigl\{\, \Bigl\lfloor \Bigl(2g+2+\deg\bigl(P_d(t)\bigr)\Bigr)/p \Bigr\rfloor - \deg\bigl(G_d(t)\bigr), g-e \Bigr\}.$$

Next, observe that it is immediate that the inequalities $\deg(P_d(t)) \leq g-1$ and $p \geq 3$, hence the inequality $\lfloor (2g+2+\deg(P_d(t)))/p \rfloor \leq g$, hold. Thus, since [it is immediate that] the inequality $e \leq \deg(G_d(t))$ holds, the above minimum is given by $\lfloor (2g+2+\deg(P_d(t)))/p \rfloor - \deg(G_d(t))$, as desired. This completes the proof of assertion (iv), hence also Lemma 1.4. $\square$

2. A CE-admissible Element in Characteristic Three

In the present §2, we prove that if $p = 3$, then, for a suitably generic element c of C, every element d of D that is of CE-type with respect to c [cf. Definition 2.1, (i), below] determines a separable polynomial $P_d(t)$ of degree $g-1$ [cf. Lemma 2.9 below].

In the present §2, we maintain the notational conventions introduced at the beginning of the preceding §1. Suppose, moreover, that

$$p = 3.$$

In the remainder of the present paper, we regard every linear space over k as being equipped with the natural Zariski topology; in particular, we regard every linear space over k as the set of k-rational points of the corresponding affine variety over k.

Definition 2.1. — Let c be an element of C.

(i) Let d be an element of D. Then we shall say that d is *of CE-type* [where "CE" stands for "Cartier Eigenform" — cf. Lemma 4.6, (ii), below] with respect to c if the following two conditions are satisfied:

(1) The element d is nonzero.

(2) The equality $\phi(c, d) = (d_1^3, \ldots, d_g^3)$ holds.

(ii) We shall say that c is *CE-admissible* if, for every element d of D of CE-type with respect to c, the polynomial $P_d(t) \in k[t]$ is separable and of degree $g - 1$.

Lemma 2.2. — *Let c be an element of C. Write $D_{\mathrm{CE}} \subseteq D$ for the linear subspace of D over [not k but over] $\mathbb{F}_3$ obtained by forming the union of*

- *the set of elements of D of CE-type with respect to c and*
- *the set that consists of the zero element of D.*

Then the following assertions hold:

(i) *There exists a linear subspace $D_{\mathrm{nlp}} \subseteq D$ of D over k such that*

- *if D_{nlp} is nonzero, then the composite*

$$D_{\mathrm{nlp}} \hookrightarrow D \longrightarrow F$$

— where the first arrow is the natural inclusion, and the second arrow is the k-linear homomorphism $D \to F$ given by $d \mapsto \phi(c, d)$ — is not injective, and, moreover,

- *the natural inclusions D_{CE}, $D_{\mathrm{nlp}} \hookrightarrow D$ determine an isomorphism of linear spaces over k*

$$(D_{\mathrm{CE}} \otimes_{\mathbb{F}_3} k) \times D_{\mathrm{nlp}} \xrightarrow{\sim} D.$$

(ii) *The set of elements of D of CE-type with respect to c is finite.*

(iii) *The following three conditions are equivalent:*

(1) *The k-linear homomorphism $D \to F$ given by $d \mapsto \phi(c, d)$ is injective.*

(2) *The set of elements of D of CE-type with respect to c is of cardinality $3^g - 1$.*

(3) *The set of elements of D of CE-type with respect to c is of cardinality $\geq 3^g - 1$.*

Proof. — One may verify assertion (i) immediately by applying [12, Corollary, p. 143] to the homomorphism

$$D \longrightarrow F \longrightarrow F$$

obtained by forming the composite of the k-linear homomorphism $D \to F$ given by $d \mapsto \phi(c, d)$ and the endomorphism of F given by $(f_1, \ldots, f_g) \mapsto (f_1^{1/3}, \ldots, f_g^{1/3})$. Assertions (ii), (iii) are formal consequences of assertion (i). This completes the proof of Lemma 2.2. $\square$

Definition 2.3. — Let n be an integer. Then a *separation* $\mathbb{S}$ of n is defined to be a sequence $(s_1, \ldots, s_r)$ — where r is a positive integer — of positive integers that satisfies the following three conditions:

(1) If $i \in \{1, \ldots, r-1\}$, then the inequality $s_i \geq s_{i+1}$ holds.

(2) If $i \in \{1, \ldots, r\}$, then the inequality $s_i \geq 2$ holds.

(3) The inequality $\sum_{i=1}^{r} s_i \leq n$ holds.

In this situation, we define the *length* $\mathrm{lg}(\mathbb{S})$, *degree* $\deg(\mathbb{S})$ of the separation $\mathbb{S}$ of n to be r, $\sum_{i=1}^{r} \lfloor s_i/3 \rfloor$, respectively.

Definition 2.4. — Let n be a positive integer, $a = (a_1, \ldots, a_n)$ an element of $k^{\times n}$, and $\mathbb{S} = (s_1, \ldots, s_r)$ a separation of $n-1$. Then we shall say that a is *of type* $\mathbb{S}$ if $a_n \neq 0$, and, moreover, there exist distinct elements $b_1, \ldots, b_r \in k$ and a separable polynomial $\Phi(t) \in k[t]$ such that $b_1, \ldots, b_r$ are not roots of the polynomial $\Phi(t)$, and the equality $P_a(t) = (t - b_1)^{s_1} \cdots (t - b_r)^{s_r} \cdot \Phi(t)$ holds.

Lemma 2.5. — *Let n be a positive integer, and let $a = (a_1, \ldots, a_n)$ be an element of $k^{\times n}$. Then the following assertions hold:*

(i) *Suppose that a is nonzero. For each root ρ of the polynomial $P_a(t)$, write* mult_ρ *for the multiplicity of the root ρ. Then the equality* $\sum_\rho \lfloor \mathrm{mult}_\rho/3 \rfloor = \deg(G_a(t))$ *holds.*

(ii) *Let $\mathbb{S} = (s_1, \ldots, s_r)$ be a separation of $n-1$. Suppose that a is of type $\mathbb{S}$. Then the equality* $\deg(G_a(t)) = \deg(\mathbb{S})$ *holds.*

Proof. — First, we verify assertion (i). Observe that, since the field k is algebraically closed and of characteristic three, one verifies easily that the multiplicity of every root of the polynomial $G_a(t^3)$ is divisible by 3; moreover, one verifies immediately from the various definitions involved that the polynomial $Q_{a,0}(t^3) + t \cdot Q_{a,1}(t^3) + t^2 \cdot Q_{a,2}(t^3)$ does not have any root of multiplicity ≥ 3. Thus, since [it is immediate that] the polynomial $P_a(t)$, hence also the polynomial $G_a(t)$, is nonzero, and the equality $P_a(t) = G_a(t^3) \cdot (Q_{a,0}(t^3) + t \cdot Q_{a,1}(t^3) + t^2 \cdot Q_{a,2}(t^3))$ holds, one concludes immediately that the equality $\sum_\rho \lfloor \mathrm{mult}_\rho/3 \rfloor = \deg(G_a(t))$ holds, as desired. This completes the proof of assertion (i).

Next, we verify assertion (ii). First, observe that since a is of type $\mathbb{S}$, there exist distinct elements $b_1, \ldots, b_r \in k$ and a separable polynomial $\Phi(t) \in k[t]$ such that $b_1, \ldots, b_r$ are not roots of the polynomial $\Phi(t)$, and, moreover, the equality $P_a(t) = (t - b_1)^{s_1} \cdots (t - b_r)^{s_r} \cdot \Phi(t)$ holds. In particular, one concludes immediately that the equalities $\sum_\rho \lfloor \mathrm{mult}_\rho/3 \rfloor = \sum_{i=1}^{r} \lfloor s_i/3 \rfloor = \deg(\mathbb{S})$ hold. Thus, assertion (ii) follows from assertion (i). This completes the proof of Lemma 2.5. $\square$

Definition 2.6.

(i) We shall write

$$B \stackrel{\mathrm{def}}{=} k.$$

(ii) We shall write

$$V_\phi \stackrel{\mathrm{def}}{=} \{ (c, d, f) \in C \times D \times F \mid f = \phi(c, d) \}.$$

(iii) We shall write

$$V_{\mathrm{egn}} \stackrel{\mathrm{def}}{=} \{ (d, f) \in D \times F \mid d_i^3 = f_i \text{ for each } i \in \{1, \ldots, g\} \}$$

— where we write $d \stackrel{\text{def}}{=} (d_1, \ldots, d_g)$ and $f \stackrel{\text{def}}{=} (f_1, \ldots, f_g)$.

(iv) Let π, γ be nonnegative integers. Then we shall write

$$V_{\text{dgn}}(\pi, \gamma) \stackrel{\text{def}}{=} \{\, d \in D \mid d_g = 0, \deg\bigl(P_d(t)\bigr) = \pi, \deg\bigl(G_d(t)\bigr) = \gamma \,\}$$

— where we write $d \stackrel{\text{def}}{=} (d_1, \ldots, d_g)$.

(v) Let $\mathbb{S} = (s_1, \ldots, s_r)$ be a separation of $g-1$. Then we shall write

$$V_{\text{mlt}}(\mathbb{S}) \subseteq D \times B$$

for the subset of $D \times B$ that consists of $(d, b) \in D \times B$ such that the element d is of type $\mathbb{S}$, and, moreover, the element b is a root of the polynomial $P_d(t)$ of multiplicity $s_{\text{lg}(\mathbb{S})}$.

(vi) We shall write

$$\pi_\phi \colon C \times D \times F \times B \longrightarrow C \times D \times F, \quad \pi_{\text{egn}} \colon C \times D \times F \times B \longrightarrow D \times F,$$

$$\pi_{\text{dgn}} \colon C \times D \times F \times B \longrightarrow D, \quad \pi_{\text{mlt}} \colon C \times D \times F \times B \longrightarrow D \times B$$

for the respective natural projections.

Remark 2.6.1. — Note that one verifies easily that:

(i) The subsets $V_\phi \subseteq C \times D \times F$, $V_{\text{egn}} \subseteq D \times F$ are Zariski closed subsets.

(ii) For each pair of nonnegative integers π and γ, the subset $V_{\text{dgn}}(\pi, \gamma) \subseteq D$ is a Zariski constructible subset.

(iii) For each separation $\mathbb{S}$ of $g-1$, the subset $V_{\text{mlt}}(\mathbb{S}) \subseteq D \times B$ is a Zariski constructible subset.

Lemma 2.7. — *Let π, γ be nonnegative integers. Then the following assertions hold:*

(i) *The Zariski constructible subset $V_{\text{dgn}}(\pi, \gamma) \subseteq D$ of D [cf. Remark 2.6.1, (ii)] is of dimension $\leq \pi + 1 - 2\gamma$.*

(ii) *Let d be an element of $V_{\text{dgn}}(\pi, \gamma)$. Then the fiber at $d \in V_{\text{dgn}}(\pi, \gamma)$ of the map*

$$\pi_\phi^{-1}(V_\phi) \cap \pi_{\text{egn}}^{-1}(V_{\text{egn}}) \cap \pi_{\text{dgn}}^{-1}\bigl(V_{\text{dgn}}(\pi, \gamma)\bigr) \longrightarrow V_{\text{dgn}}(\pi, \gamma)$$

determined by π_{dgn} is either empty or of dimension $2g + 2 - \lfloor (2g + 2 + \pi)/3 \rfloor + \gamma + 1$.

(iii) *The Zariski constructible subset $\pi_\phi^{-1}(V_\phi) \cap \pi_{\text{egn}}^{-1}(V_{\text{egn}}) \cap \pi_{\text{dgn}}^{-1}(V_{\text{dgn}}(\pi, \gamma)) \subseteq C \times D \times F \times B$ of $C \times D \times F \times B$ [cf. Remark 2.6.1, (i), (ii)] is of dimension $\leq 2g + 2$.*

(iv) *The image of the composite*

$$\pi_\phi^{-1}(V_\phi) \cap \pi_{\text{egn}}^{-1}(V_{\text{egn}}) \cap \pi_{\text{dgn}}^{-1}\bigl(V_{\text{dgn}}(\pi, \gamma)\bigr) \hookrightarrow C \times D \times F \times B \longrightarrow C$$

— where the first arrow is the natural inclusion, and the second arrow is the projection onto the first factor — is not dense in C.

Proof. — First, we verify assertion (i). Observe that the subset of D that consists of $d \in D$ such that the equality $\deg(P_d(t)) = \pi$ holds is of dimension $\leq \pi + 1$. Thus, since [one verifies easily that] the condition that the three polynomials $P_{d,0}(t)$, $P_{d,1}(t)$, $P_{d,2}(t)$

have a common factor of degree γ is of codimension 2γ, one concludes that $V_{\mathrm{dgn}}(\pi,\gamma)$ is of dimension $\leq (\pi+1)-2\gamma$, as desired. This completes the proof of assertion (i). Assertion (ii) follows immediately from Lemma 1.4, (iv).

Next, we verify assertion (iii). First, observe that if $V_{\mathrm{dgn}}(\pi,\gamma)=\emptyset$, then assertion (iii) is immediate. Suppose that $V_{\mathrm{dgn}}(\pi,\gamma)\neq\emptyset$. In particular, since [we have assumed that] the equality $d_g=0$ holds for each $d\in V_{\mathrm{dgn}}(\pi,\gamma)$, the inequality $\pi\leq g-2$, hence the inequality

$$\pi+2\leq\lfloor(2g+2+\pi)/3\rfloor,$$

holds. Thus, it follows from assertions (i), (ii), that the Zariski constructible subset under consideration is of dimension

$$\leq(\pi+1-2\gamma)+\big(2g+2-\lfloor(2g+2+\pi)/3\rfloor+\gamma+1\big)$$

$$=2g+2-\gamma+\big(\pi+2-\lfloor(2g+2+\pi)/3\rfloor\big)\leq 2g+2,$$

as desired. This completes the proof of assertion (iii).

Finally, we verify assertion (iv). First, observe that one verifies immediately from the various definitions involved that the subset

$$\pi_\phi^{-1}(V_\phi)\cap\pi_{\mathrm{egn}}^{-1}(V_{\mathrm{egn}})\cap\pi_{\mathrm{dgn}}^{-1}\big(V_{\mathrm{dgn}}(\pi,\gamma)\big)\subseteq C\times D\times F\times B$$

may be written as the inverse image of some Zariski constructible subset of $C\times D\times F$. Thus, assertion (iv) is a formal consequence of assertion (iii). This completes the proof of assertion (iv), hence also of Lemma 2.7. $\square$

Lemma 2.8. — *Let $\mathbb{S}$ be a separation of $g-1$. Then the following assertions hold:*

(i) *Let b be an element of B. Then the fiber at $b\in B$ of the composite*

$$V_{\mathrm{mlt}}(\mathbb{S})\hookrightarrow D\times B\longrightarrow B$$

— where the first arrow is the natural inclusion, and the second arrow is the projection onto the second factor — may be naturally identified with the subset of D that consists of $d\in D$ such that d is of type $\mathbb{S}$, and, moreover, the element b is a root of the polynomial $P_d(t)$ of multiplicity $s_{\mathrm{lg}(\mathbb{S})}$. In particular, each fiber of the composite under consideration is a constructible subset of D of dimension $\leq g-\deg(\mathbb{S})-2$.

(ii) *The Zariski constructible subset $V_{\mathrm{mlt}}(\mathbb{S})\subseteq D\times B$ of $D\times B$ [cf. Remark 2.6.1, (iii)] is of dimension $\leq g-\deg(\mathbb{S})-1$.*

(iii) *The fiber at $(d,b)\in V_{\mathrm{mlt}}(\mathbb{S})$ of the map*

$$\pi_\phi^{-1}(V_\phi)\cap\pi_{\mathrm{egn}}^{-1}(V_{\mathrm{egn}})\cap\pi_{\mathrm{mlt}}^{-1}\big(V_{\mathrm{mlt}}(\mathbb{S})\big)\longrightarrow V_{\mathrm{mlt}}(\mathbb{S})$$

determined by π_{mlt} is of dimension $\leq g+\deg(\mathbb{S})+2$.

(iv) *The image of the composite*

$$\pi_\phi^{-1}(V_\phi)\cap\pi_{\mathrm{egn}}^{-1}(V_{\mathrm{egn}})\cap\pi_{\mathrm{mlt}}^{-1}\big(V_{\mathrm{mlt}}(\mathbb{S})\big)\hookrightarrow C\times D\times F\times B\longrightarrow C$$

— where the first arrow is the natural inclusion, and the second arrow is the projection onto the first factor — is not dense in C.

Proof. — Assertion (i) follows immediately from the various definitions involved. Assertion (ii) follows immediately from assertion (i). Assertion (iii) follows immediately from Lemma 1.4, (iv), and Lemma 2.5, (ii). Assertion (iv) follows immediately from assertions (ii), (iii). This completes the proof of Lemma 2.8. $\square$

Lemma 2.9. — *There exists a nonempty dense Zariski open subset of C such that if c is an element of this open subset of C, then c is CE-admissible, and, moreover, the polynomial $M_c(t) \in k[t]$ is separable.*

Proof. — First, observe that it is immediate that the subset of C that consists of $c \in C$ such that $M_c(t)$ is separable is a nonempty Zariski open subset of C. Thus, Lemma 2.9 follows immediately from Lemma 2.7, (iv), and Lemma 2.8, (iv). This completes the proof of Lemma 2.9. $\square$

Definition 2.10. — Let d be an element of D. Then we shall write

$$\Sigma(d) \stackrel{\text{def}}{=} \{\, a \in k \mid P_c(a) = 0 \text{ for every element } c \text{ of } \mathrm{Ker}(\psi_d)\,\}.$$

Lemma 2.11. — *Let d be a nonzero element of D. Then the following assertions hold:*

(i) *The inequality $\#\Sigma(d) \leq 2g+1$ holds.*

(ii) *The inequalities $\#\Sigma(d) \leq \dim(\mathrm{Im}(\psi_d)) \leq g$ hold.*

(iii) *Let b be an element of k. Then there is a unique element d' of D such that the equality $P_{d'}(t) = P_d(t+b)$ holds. Moreover, in this situation, the equality*

$$\Sigma(d') = \{\, a - b \mid a \in \Sigma(d)\,\}$$

holds.

Proof. — First, we verify assertion (i). Observe that, since [it is immediate that] the inequalities $\dim(\mathrm{Im}(\psi_d)) \leq \dim(F) = g < 2g+2 = \dim(C)$ hold, the kernel $\mathrm{Ker}(\psi_d)$ is nonzero. Thus, there exists a nonzero element c of C that is contained in $\mathrm{Ker}(\psi_d)$, which implies that the polynomial $P_c(t)$ is nonzero. In particular, since every element of $\Sigma(d)$ is a root of the polynomial $P_c(t)$, one concludes that the inequalities $\#\Sigma(d) \leq \deg(P_c(t)) \leq 2g+1$ hold, as desired. This completes the proof of assertion (i).

Next, we verify assertion (ii). Observe that since the image of ψ_d is a sub-k-space of $F = k^{\times g}$, the inequality $\dim(\mathrm{Im}(\psi_d)) \leq g$ holds. Thus, to verify assertion (ii), it suffices to verify the inequality $\#\Sigma(d) \leq \dim(\mathrm{Im}(\psi_d))$.

Next, observe that, by the definition of $\Sigma(d)$, the kernel $\mathrm{Ker}(\psi_d)$ is contained in the sub-k-space $V \subseteq C$ of C that consists of $c \in C$ such that $P_c(a) = 0$ for every element a of $\Sigma(d)$. On the other hand, since the assignment $c \mapsto P_c(t)$ determines an isomorphism of C with the linear space over k of polynomials of degree $\leq 2g+1$, one verifies easily from assertion (i) that the sub-k-space V is of dimension $2g+2-\#\Sigma(d)$. Thus, the inequality $\dim(\mathrm{Ker}(\psi_d)) \leq 2g+2-\#\Sigma(d)$, hence also the inequalities $\#\Sigma(d) \leq 2g+2-\dim(\mathrm{Ker}(\psi_d)) = \dim(\mathrm{Im}(\psi_d))$, holds. This completes the proof of assertion (ii).

Next, we verify assertion (iii). First, observe that, for each $c \in C$, since the inequality $\deg(P_c(t) \cdot P_d(t)) \leq 3g$ holds, it follows from Lemma 1.4, (i), that the equality $\psi_d(c) = 0$ holds if and only if the polynomial $P_c(t) \cdot P_d(t)$ has no term whose degree is $\equiv 2$ modulo

3. Moreover, one verifies easily that, for each $c \in C$ and each $b \in k$, the polynomial $P_c(t) \cdot P_d(t)$ has no term whose degree is $\equiv 2$ modulo 3 if and only if the polynomial $P_c(t+b) \cdot P_d(t+b)$ has no term whose degree is $\equiv 2$ modulo 3. Thus, assertion (iii) follows immediately from the various definitions involved. This completes the proof of Lemma 2.11. $\square$

Definition 2.12. — We shall write

$$I \overset{\text{def}}{=} I(g) \overset{\text{def}}{=} \{ (c, d) \in C \times D \mid d \text{ is of CE-type with respect to } c \}.$$

Remark 2.12.1.

(i) It is immediate from Lemma 2.2, (ii), that every fiber of the natural map $I \to C$ is finite.

(ii) One verifies easily that the subset $I \subseteq C \times D$ of $C \times D$ is a Zariski constructible subset.

Lemma 2.13. — *Let $J \subseteq I$ be an irreducible component of I [cf. Remark 2.12.1, (ii)] such that the image of the composite $J \hookrightarrow I \to C$ is dense. Then there is no nonempty open subspace of J on which the map*

$$J \longrightarrow B \qquad (c, d) \longmapsto C_{g-1}^{[t]}\big(P_d(t)\big)$$

[cf. Definition 1.1] is constant.

Proof. — Assume that there is a nonempty open subspace of J on which the map under consideration is constant. Then it is immediate that there exists an element $a \in k$ such that the image of the natural map $J \to D$ is contained in the subset of D that consists of the elements d that satisfy the equality $C_{g-1}^{[t]}(P_d(t)) = a$, which is of dimension $\leq g-1$. Thus, since $\dim(J) = \dim(C) = 2g+2$ [cf. Remark 2.12.1, (i)], one concludes that

(a) there exists a nonempty dense Zariski open subset of the image of the natural map $J \to D$ such that if d is an element of this open subset, then the fiber at d of the natural map $J \to D$ is of dimension $\geq 2g+2-(g-1) = g+3$.

On the other hand, it follows from the definition of I that, for each $d = (d_1, \ldots, d_g) \in D$, the fiber at $d \in D$ of the natural map $J \to D$ is contained in a set that may be naturally identified with the subset

$$\{ c \in C \mid \phi(c, d) = (d_1^3, \ldots, d_g^3) \}$$

of C, which is either empty or a coset of $\mathrm{Ker}(\psi_d)$, hence of dimension $2g+2-\dim(\mathrm{Im}(\psi_d))$. Thus, one concludes from (a) that

(b) there exists a nonempty dense Zariski open subset of the image of the natural map $J \to D$ such that if d is an element of this open subset, then the inequality $\dim(\mathrm{Im}(\psi_d)) \leq g-1$ holds.

On the other hand, since [we have assumed that] J dominates C, it follows from Lemma 2.9 that there exists a nonempty dense Zariski open subset of J such that if (c, d) is an element of this open subset of J, then the element c is CE-admissible, which implies that the polynomial $P_d(t)$ is separable of degree $g-1$. Thus, since [one verifies easily from Lemma 2.5, (i), that] the equality $\deg(G_d(t)) = 0$ holds, one concludes from Lemma 1.4, (iv), that there exists a nonempty dense Zariski open subset of J such that if (c,d) is an element of this open subset of J, then the equality $\dim(\mathrm{Im}(\psi_d)) = \lfloor (2g+2+(g-1))/3 \rfloor = g$ holds — in contradiction to (b). This completes the verification of Lemma 2.13. $\square$

3. A CE-admissible Pair in Characteristic Three

In the present §3, we prove that a suitably generic element of $C_1 \times C_2$ is CE-admissible [cf. Definition 3.3 below] and also satisfies certain additional genericity conditions [cf. Lemma 3.11 below]. In the present §3, let

- g_1, g_2 be nonnegative integers, and let
- k be an algebraically closed field of characteristic three.

Definition 3.1. For each $i \in \{1,2\}$, we shall write

$$C_i \overset{\text{def}}{=} C(g_i), \quad D_i \overset{\text{def}}{=} D(g_i), \quad F_i \overset{\text{def}}{=} F(g_i), \quad I_i \overset{\text{def}}{=} I(g_i) \subseteq C_i \times D_i$$

[cf. Definition 1.3, (i); Definition 2.12].

Definition 3.2. — For each $i \in \{1,2\}$, let c_i be an element of C_i, and let d_i be an element of D_i. Then we shall write

$$P_{(c_1,c_2,d_1,d_2)}(t) \overset{\text{def}}{=} P_{d_1}(t)^2 \cdot M_{c_2}(t) + P_{d_2}(t)^2 \cdot M_{c_1}(t) \in k[t]$$

[cf. Definition 1.2, (i)].

Definition 3.3. — Let (c_1,c_2) be an element of $C_1 \times C_2$. Then we shall say that the pair (c_1,c_2) is *CE-admissible* if, for elements d_1, d_2 of D_1, D_2 of CE-type with respect to c_1, c_2 [cf. Definition 2.1, (i)], respectively, the polynomials $P_{d_1}(t)$, $P_{d_2}(t)$, $P_{(c_1,c_2,d_1,d_2)}(t) \in k[t]$ are separable and, moreover, of degree g_1-1, g_2-1, $2g_1+2g_2$, respectively.

Definition 3.4. — Let $F(t)$, $G(t)$ be elements of $k[t]$. Then we shall write

$$\mathrm{Wr}\big(F(t), G(t)\big) \overset{\text{def}}{=} \frac{dF(t)}{dt} \cdot G(t) - F(t) \cdot \frac{dG(t)}{dt} \in k[t]$$

for the *Wronskian* of $F(t)$ and $G(t)$.

Lemma 3.5. — *Let $F(t)$, $G(t)$ be nonzero elements of $k[t]$. Then the following assertions hold:*

(i) *Suppose that the polynomial $F(t)$ is not divisible by the cube of any nonconstant polynomial. Let $H(t)$ be an element of $k[t]$. Then the following two conditions are equivalent:*

(1) *The equality* $\mathrm{Wr}(F(t) \cdot G(t)^3, H(t)) = 0$ *holds.*

(2) *The polynomial* $H(t)$ *may be written as the product of* $F(t)$ *and a cube of some element of* $k[t]$.

(ii) *Suppose that the inequality* $\deg(G(t)) < \deg(F(t))$ *holds, and that the equality* $\mathrm{Wr}(F(t), G(t)) = 0$ *holds. Then the polynomial* $F(t)$ *is divisible by the cube of some nonconstant polynomial.*

Proof. — First, we verify assertion (i). Observe that, since the field k is of characteristic three [which implies that the derivative of $G(t)^3$ is zero], the equality

$$\mathrm{Wr}\big(F(t) \cdot G(t)^3, H(t)\big) = G(t)^3 \cdot \mathrm{Wr}\big(F(t), H(t)\big)$$

holds. In particular, since [we have assumed that] $G(t)$ is nonzero, one concludes that condition (1) is satisfied if and only if the equality $\mathrm{Wr}(F(t), H(t)) = 0$ holds.

Now we verify the implication (1) $\Rightarrow$ (2). Suppose that condition (1) is satisfied, which implies [cf. the conclusion of the first paragraph of the present proof] that the equality $\mathrm{Wr}(F(t), H(t)) = 0$ holds. If $H(t) = 0$, then condition (2) is satisfied. Suppose that $H(t)$ is nonzero. Then it follows from the equality $\mathrm{Wr}(F(t), H(t)) = 0$ that the derivative of the rational function $H(t)/F(t)$ is zero. Thus, since the field k is algebraically closed and of characteristic three, one verifies easily that there exist elements $P(t)$, $Q(t)$ of $k[t]$ such that the equalities $\gcd(P(t), Q(t)) = 1$ and $H(t)/F(t) = (P(t)/Q(t))^3$ hold. In particular, one concludes that $Q(t)^3$ divides $F(t)$. Thus, since $F(t)$ is not divisible by the cube of any nonconstant polynomial, the polynomial $Q(t)$ is a nonzero constant. In particular, it follows from the equality $H(t)/F(t) = (P(t)/Q(t))^3$ that condition (2) is satisfied, as desired. This completes the proof of the implication (1) $\Rightarrow$ (2).

Next, we verify the implication (2) $\Rightarrow$ (1). Suppose that condition (2) is satisfied, i.e., that there exists an element $R(t)$ of $k[t]$ such that the equality $H(t) = F(t) \cdot R(t)^3$ holds. Then since the field k is of characteristic three [which implies that the derivative of $R(t)^3$ is zero], one verifies easily that the equality $\mathrm{Wr}(F(t), H(t)) = 0$ holds. Thus, it follows from the conclusion of the first paragraph of the present proof that condition (1) is satisfied, as desired. This completes the proof of the implication (2) $\Rightarrow$ (1), hence also of assertion (i).

Next, we verify assertion (ii). Assume that $F(t)$ is not divisible by the cube of any nonconstant polynomial. Then, by applying the implication (1) $\Rightarrow$ (2) of assertion (i) — where we take the "$(F(t), G(t), H(t))$" of assertion (i) to be $(F(t), 1, G(t))$ — one concludes from the equality $\mathrm{Wr}(F(t), G(t)) = 0$ that there exists an element $R(t)$ of $k[t]$ such that the equality $G(t) = F(t) \cdot R(t)^3$ holds. On the other hand, since $G(t)$ is nonzero, the polynomial $R(t)$ is nonzero, so that the inequality $\deg(F(t)) \leq \deg(G(t))$ holds. Thus, since [we have assumed that] the inequality $\deg(G(t)) < \deg(F(t))$ holds, we obtain a contradiction. This completes the proof of assertion (ii), hence of Lemma 3.5. □

Lemma 3.6. — *For each* $i \in \{1, 2\}$, *let* c_i *be an element of* C_i, *and let* d_i *be a nonzero element of* D_i. *Suppose that the polynomial* $P_{(c_1,c_2,d_1,d_2)}(t)$ *is nonzero. Then there exists an element* c_1' *of* $\mathrm{Ker}(\psi_{d_1})$ *such that the polynomial* $\mathrm{Wr}(P_{(c_1,c_2,d_1,d_2)}(t), P_{d_2}(t)^2 \cdot P_{c_1'}(t))$ *is nonzero.*

Proof. — Assume that, for every element c_1' of $\mathrm{Ker}(\psi_{d_1})$, the equality

$$\mathrm{Wr}\big(P_{(c_1,c_2,d_1,d_2)}(t), P_{d_2}(t)^2 \cdot P_{c_1'}(t)\big) = 0$$

holds. Then observe that since [we have assumed that] the polynomial $P_{(c_1,c_2,d_1,d_2)}(t)$ is nonzero, it is immediate that there exist elements $F(t)$, $G(t)$ of $k[t]$ such that $F(t)$ is not divisible by the cube of any nonconstant polynomial, and, moreover, the equality $P_{(c_1,c_2,d_1,d_2)}(t) = F(t) \cdot G(t)^3$ holds. Thus, by applying the implication (1) $\Rightarrow$ (2) of Lemma 3.5, (i) — where we take the "$(F(t), G(t), H(t))$" of Lemma 3.5, (i), to be $(F(t), G(t), P_{d_2}(t)^2 \cdot P_{c_1'}(t))$ — one concludes that, for each element c_1' of $\mathrm{Ker}(\psi_{d_1})$, the polynomial $P_{d_2}(t)^2 \cdot P_{c_1'}(t)$ may be written as the product of $F(t)$ and a cube of some element of $k[t]$. In particular, it follows from the implication (2) $\Rightarrow$ (1) of Lemma 3.5, (i), that, for elements c_1', c_1'' of $\mathrm{Ker}(\psi_{d_1})$, the equality

$$\mathrm{Wr}\big(P_{d_2}(t)^2 \cdot P_{c_1'}(t), P_{d_2}(t)^2 \cdot P_{c_1''}(t)\big) = 0$$

holds. On the other hand, since [one verifies easily that] the equality

$$\mathrm{Wr}\big(P_{d_2}(t)^2 \cdot P_{c_1'}(t), P_{d_2}(t)^2 \cdot P_{c_1''}(t)\big) = P_{d_2}(t)^4 \cdot \mathrm{Wr}(P_{c_1'}(t), P_{c_1''}(t))$$

holds, and the polynomial $P_{d_2}(t)$ is nonzero, one concludes that

(a) the equality $\mathrm{Wr}(P_{c_1'}(t), P_{c_1''}(t)) = 0$ holds for all elements c_1', c_1'' of $\mathrm{Ker}(\psi_{d_1})$.

Next, observe that since the inequality $\dim(\mathrm{Im}(\psi_{d_1})) \leq g_1$ holds [cf. Lemma 2.11, (ii)], the inequality $\dim(\mathrm{Ker}(\psi_{d_1})) = 2g_1+2-\dim(\mathrm{Im}(\psi_{d_1})) \geq g_1+2$ holds. In particular, there exists a nonzero element ${}_0c_1$ of $\mathrm{Ker}(\psi_{d_1})$. Then since the polynomial $P_{{}_0c_1}(t)$ is nonzero, there exist elements ${}_0F(t)$, ${}_0G(t)$ of $k[t]$ such that ${}_0F(t)$ is not divisible by the cube of any nonconstant polynomial, and, moreover, the equality $P_{{}_0c_1}(t) = {}_0F(t) \cdot {}_0G(t)^3$ holds. Thus, since [it follows from (a) that] the equality $\mathrm{Wr}(P_{{}_0c_1}(t), P_{c_1'}(t)) = 0$ holds for every element c_1' of $\mathrm{Ker}(\psi_{d_1})$, by applying the implication (1) $\Rightarrow$ (2) of Lemma 3.5, (i) — where we take the "$(F(t), G(t), H(t))$" of Lemma 3.5, (i), to be $({}_0F(t), {}_0G(t), P_{c_1'}(t))$ — one concludes that,

(b) for each element c_1' of $\mathrm{Ker}(\psi_{d_1})$, the polynomial $P_{c_1'}(t)$ may be written as the product of ${}_0F(t)$ and a cube of some element of $k[t]$.

Next, observe that, since the field k is algebraically closed and of characteristic three, the cubes of the elements of $k[t]$ are precisely the elements of $k[t^3]$. Write $V \subseteq k[t]$ for the sub-k-space of $k[t]$ that consists of the elements of ${}_0F(t) \cdot k[t^3]$ of degree $\leq 2g_1 + 1$. Then it follows immediately from (b) that the subset $\{ P_{c_1'}(t) \mid c_1' \in \mathrm{Ker}(\psi_{d_1}) \}$ is contained in V. Moreover, since [it is immediate that] the assignment $c_1' \mapsto P_{c_1'}(t)$ is injective, this subset is a sub-k-space of $k[t]$ of dimension $\dim(\mathrm{Ker}(\psi_{d_1})) \geq g_1 + 2$, which implies that the inequality $g_1 + 2 \leq \dim(V)$ holds. On the other hand, since [one verifies easily that] the inequalities $\dim(V) \leq \lfloor (2g_1 + 1)/3 \rfloor + 1 < g_1 + 2$ hold, we obtain a contradiction, as desired. This completes the proof of Lemma 3.6. $\square$

Lemma 3.7. — *Let $J \subseteq I_1 \times I_2$ be an irreducible component of $I_1 \times I_2$ [cf. Remark 2.12.1, (ii)] such that the image of the composite $J \hookrightarrow I_1 \times I_2 \to C_1 \times C_2$ is dense. Then there exists a nonempty dense Zariski open subset of J such that every point $(c_1, d_1, c_2, d_2) \in J$ of this open subset of J satisfies the following three conditions:*

(1) *For each $i \in \{1, 2\}$, the polynomials $M_{c_i}(t)$, $P_{d_i}(t)$ are separable, and, moreover, the polynomial $P_{d_i}(t)$ is of degree $g_i - 1$.*

(2) *The equalities*

$$k[t] = M_{c_i}(t) \cdot k[t] + P_{d_i}(t) \cdot k[t]$$

$$= M_{c_1}(t) \cdot k[t] + M_{c_2}(t) \cdot k[t] = P_{d_1}(t) \cdot k[t] + P_{d_2}(t) \cdot k[t]$$

— where i is an element of $\{1, 2\}$ — hold.

(3) *The element $C^{[t]}_{g_1-1}(P_{d_1}(t))^2 + C^{[t]}_{g_2-1}(P_{d_2}(t))^2$ [cf. Definition 1.1] of k is nonzero.*

PROOF. — Observe that one verifies immediately from Lemma 2.9, together with the various definitions involved, that the subset of $I_1 \times I_2$ that consists of the elements that satisfy conditions (1), (2) that appear in the statement of the present Lemma 3.7 is dense in $I_1 \times I_2$. Next, observe that it is immediate from the various definitions involved that there exist irreducible components $J_1 \subseteq I_1$, $J_2 \subseteq I_2$ of I_1, I_2 such that the equality $J_1 \times J_2 = J$ holds. In particular, since [one verifies easily that] the map "$J \to B$" that appears in the statement of Lemma 2.13 is algebraic, if the subset of J that consists of the elements that satisfy condition (3) of Lemma 3.7 is not dense in J, then, for each $i \in \{1, 2\}$, there is a nonempty open subspace of J_i on which the map $J_i \to k$ defined by $(c_i, d_i) \mapsto C^{[t]}_{g_i-1}(P_{d_i}(t))$ is constant. Therefore, one concludes from Lemma 2.13 that Lemma 3.7 holds. This completes the proof of Lemma 3.7. □

LEMMA 3.8. — *There exists a nonempty dense Zariski open subset of $C_1 \times C_2$ such that if $(c_1, c_2) \in C_1 \times C_2$ is an element of this open subset of $C_1 \times C_2$, then, for elements d_1, d_2 of D_1, D_2 of CE-type with respect to c_1, c_2, respectively, the following two conditions are satisfied:*

(1) *The polynomial $P_{(c_1,c_2,d_1,d_2)}(t)$ is of degree $2g_1 + 2g_2$.*

(2) *Let $a \in k$ be such that $P_{(c_1,c_2,d_1,d_2)}(a) = 0$. Then $M_{c_1}(a) \cdot M_{c_2}(a) \cdot P_{d_1}(a) \cdot P_{d_2}(a)$ is nonzero.*

PROOF. — First, observe that it follows immediately from Remark 2.12.1, (i), and Lemma 3.7 that, to verify Lemma 3.8, it suffices to verify that, for each element (c_1, d_1, c_2, d_2) of $I_1 \times I_2$, if the element (c_1, d_1, c_2, d_2) satisfies conditions (1), (2), (3) that appear in the statement of Lemma 3.7, then the element (c_1, d_1, c_2, d_2) satisfies conditions (1), (2) that appear in the statement of the present Lemma 3.8. To this end, let (c_1, d_1, c_2, d_2) be an element of $I_1 \times I_2$ that satisfies conditions (1), (2), (3) that appear in the statement of Lemma 3.7.

Now we verify the assertion that $(c_1, d_1, c_2, d_2) \in I_1 \times I_2$ satisfies condition (1). First, recall from condition (1) of Lemma 3.7 that, for each $i \in \{1, 2\}$, the polynomial $M_{c_i}(t)$ is monic of degree $2g_i + 2$, and the polynomial $P_{d_i}(t)$ is of degree $g_i - 1$. Thus, the equality

$$C^{[t]}_{2g_1+2g_2}\big(P_{(c_1,c_2,d_1,d_2)}(t)\big) = C^{[t]}_{g_1-1}\big(P_{d_1}(t)\big)^2 + C^{[t]}_{g_2-1}\big(P_{d_2}(t)\big)^2$$

holds. In particular, it follows from condition (3) of Lemma 3.7 that $(c_1, d_1, c_2, d_2) \in I_1 \times I_2$ satisfies condition (1), as desired. This completes the proof of the assertion that $(c_1, d_1, c_2, d_2) \in I_1 \times I_2$ satisfies condition (1).

Next, we verify the assertion that $(c_1, d_1, c_2, d_2) \in I_1 \times I_2$ satisfies condition (2). To this end, let $a \in k$ be such that $P_{(c_1,c_2,d_1,d_2)}(a) = 0$. Now we claim that $M_{c_1}(a) \cdot M_{c_2}(a) \neq 0$. To this end, assume that the equality $M_{c_2}(a) = 0$, hence also the equality $P_{(c_1,c_2,d_1,d_2)}(a) = P_{d_2}(a)^2 \cdot M_{c_1}(a)$, holds. Then it follows from condition (2) of Lemma 3.7 that $P_{d_2}(a) \neq 0$ and $M_{c_1}(a) \neq 0$, which implies that $P_{(c_1,c_2,d_1,d_2)}(a) \neq 0$ — in contradiction to our assumption that $P_{(c_1,c_2,d_1,d_2)}(a) = 0$. Thus, the inequality $M_{c_2}(a) \neq 0$ holds; a similar argument — where we interchange the roles of the indices 1 and 2 — shows that $M_{c_1}(a) \neq 0$. This completes the proof of the claim that $M_{c_1}(a) \cdot M_{c_2}(a) \neq 0$.

Next, we claim that $P_{d_1}(a) \cdot P_{d_2}(a) \neq 0$. To this end, assume that $P_{d_2}(a) = 0$. Then since $0 = P_{(c_1,c_2,d_1,d_2)}(a) = P_{d_1}(a)^2 \cdot M_{c_2}(a)$ and $M_{c_2}(a) \neq 0$ [cf. the discussion of the preceding paragraph], one concludes that $P_{d_1}(a) = 0$ — in contradiction to condition (2) of Lemma 3.7. Thus, one also concludes that $P_{d_2}(a) \neq 0$; a similar argument — where we interchange the roles of the indices 1 and 2 — shows that $P_{d_1}(a) \neq 0$. This completes the proof of the claim that $P_{d_1}(a) \cdot P_{d_2}(a) \neq 0$, hence also of Lemma 3.8. $\square$

Lemma 3.9. — *Let $J \subseteq I_1 \times I_2$ be an irreducible component of $I_1 \times I_2$ such that the image of the composite $J \hookrightarrow I_1 \times I_2 \to C_1 \times C_2$ is dense. Let us recall that it follows from Lemma* 3.8*, together with the various definitions involved, that there exists a nonempty dense Zariski open subset $U_J \subseteq J$ of J that satisfies the following two conditions:*

(a) *For every element (c_1, d_1, c_2, d_2) of U_J, the polynomial $P_{(c_1,c_2,d_1,d_2)}(t)$ is of degree $2g_1 + 2g_2$.*

(b) *For every element (c_1, d_1, c_2, d_2) of U_J and every element $a \in k$, if the equality $P_{(c_1,c_2,d_1,d_2)}(a) = 0$ holds, then $M_{c_1}(a) \cdot M_{c_2}(a) \cdot P_{d_1}(a) \cdot P_{d_2}(a)$ is nonzero.*

Write, moreover, $V_J \subseteq J$ for the [necessarily nonempty dense Zariski open] subset of J that consists of the elements of J that are not contained in the closure, in $I_1 \times I_2$, of the complement of J in $I_1 \times I_2$. Suppose that, for every $(c_1, d_1, c_2, d_2) \in J$, the polynomial $P_{(c_1,c_2,d_1,d_2)}(t)$ is not separable. Let (c_1, d_1, c_2, d_2) be an element of $U_J \cap V_J$. Write

$$V_{\mathrm{Wr}} \stackrel{\text{def}}{=} \{\, c \in \operatorname{Ker}(\psi_{d_1}) \mid \operatorname{Wr}\big(P_{(c_1,c_2,d_1,d_2)}(t), P_{d_2}(t)^2 \cdot P_c(t)\big) = 0 \,\}.$$

[Note that since — one verifies easily from the various definitions involved that — the assignment $c \mapsto \operatorname{Wr}(P_{(c_1,c_2,d_1,d_2)}(t), P_{d_2}(t)^2 \cdot P_c(t))$ is k-linear, the subset V_{Wr} is a sub-k-space of $\operatorname{Ker}(\psi_{d_1})$.] Let c'_1 be an element of $\operatorname{Ker}(\psi_{d_1})$ that is not contained in V_{Wr}. [Note that it follows from Lemma 3.6 *that such an element always exists.] For each $s \in k$, write*

$$L_s(t) \stackrel{\text{def}}{=} P_{(c_1+sc'_1,c_2,d_1,d_2)}(t) = P_{(c_1,c_2,d_1,d_2)}(t) + s \cdot P_{d_2}(t)^2 \cdot P_{c'_1}(t).$$

Write, moreover,

$$W_{c'_1}(t) \stackrel{\text{def}}{=} \operatorname{Wr}\big(P_{(c_1,c_2,d_1,d_2)}(t), P_{d_2}(t)^2 \cdot P_{c'_1}(t)\big).$$

Then the following assertions hold:

(i) *For all but finitely many $s \in k$, the polynomial $L_s(t)$ is of degree $2g_1 + 2g_2$ and not separable.*

(ii) *The subset of k that consists of multiple roots of the polynomial $L_s(t)$ for some $s \in k^\times$ is contained in the set of roots of the polynomial $W_{c'_1}(t)$.*

(iii) *There exists an element $a_1 \in k$ such that the equalities $P_{(c_1,c_2,d_1,d_2)}(a_1) = P_{c'_1}(a_1) = 0$ hold.*

(iv) *There exists an element of $\Sigma(d_1)$ that is a root of the polynomial $P_{(c_1,c_2,d_1,d_2)}(t)$.*

(v) *There exists an element c'_2 of $\operatorname{Ker}(\psi_{d_2})$ such that no root of the polynomial $P_{c'_2}(t)$ is contained in $\Sigma(d_1) \setminus \Sigma(d_2)$.*

(vi) *In the situation of* (v)*, for each $s \in k$, write*

$$R_s(t) \stackrel{\text{def}}{=} P_{(c_1,c_2+sc'_2,d_1,d_2)}(t) = P_{(c_1,c_2,d_1,d_2)}(t) + s \cdot P_{d_1}(t)^2 \cdot P_{c'_2}(t).$$

Then, for all but finitely many $s \in k$, no root of the polynomial $R_s(t)$ is contained in $\Sigma(d_1) \setminus \Sigma(d_2)$.

(vii) *The intersection $\Sigma(d_1) \cap \Sigma(d_2)$ is nonempty.*

Proof. — First, we verify assertion (i). Observe that one verifies easily from the various definitions involved that, for every $s \in k$, the element d_1 is of CE-type with respect to $c_1 + sc'_1$, which implies that $(c_1 + sc'_1, d_1, c_2, d_2)$ is an element of $I_1 \times I_2$. Moreover, since [we have assumed that] the element (c_1, d_1, c_2, d_2) is contained in V_J, one concludes that the subset

$$\{ (c_1 + sc'_1, d_1, c_2, d_2) \mid s \in k \} \subseteq I_1 \times I_2$$

is contained in J, which implies [cf. our assumption that, "for every $(c_1, d_1, c_2, d_2) \in J$, the polynomial $P_{(c_1,c_2,d_1,d_2)}(t)$ is not separable"] that, for each $s \in k$, the polynomial $L_s(t)$ is not separable, as desired. Moreover, since [one verifies easily that] the inequalities $\deg(P_{d_2}(t)^2 \cdot P_{c'_1}(t)) \leq 2(g_2 - 1) + 2g_1 + 1 < 2g_1 + 2g_2$ hold, it follows from (a) that, for all but finitely many $s \in k$, the polynomial $L_s(t)$ is of degree $2g_1 + 2g_2$, as desired. This completes the proof of assertion (i).

Next, we verify assertion (ii). Let s be an element of $k^\times$. First, observe that if an element a of k is a multiple root of the polynomial $L_s(t)$, then the equalities $L_s(t)(a) = 0$ and $(dL_s(t)/dt)(a) = 0$ hold. Thus, since $L_s(t) = P_{(c_1,c_2,d_1,d_2)}(t) + s \cdot P_{d_2}(t)^2 \cdot P_{c'_1}(t)$, and

$$W_{c'_1}(t) = \frac{d}{dt}\big(P_{(c_1,c_2,d_1,d_2)}(t)\big) \cdot \big(P_{d_2}(t)^2 \cdot P_{c'_1}(t)\big) - \big(P_{(c_1,c_2,d_1,d_2)}(t)\big) \cdot \frac{d}{dt}\big(P_{d_2}(t)^2 \cdot P_{c'_1}(t)\big),$$

one concludes immediately that a is a root of the polynomial $W_{c'_1}(t)$, as desired. This completes the proof of assertion (ii).

Next, we verify assertion (iii). First, observe that since the polynomial $W_{c'_1}(t)$ is nonzero [cf. the definition of V_{Wr}], it follows from assertion (ii) that the subset of k that consists of multiple roots of the polynomial $L_s(t)$ [cf. (i)] for some $s \in k^\times$ is finite. In particular, since [we have assumed that] the field k is algebraically closed, it follows from assertion (i) that there exists an element a_1 of k that is a multiple root of the polynomial $L_s(t)$ for infinitely many $s \in k$. For such an element a_1, since the equality $L_s(a_1) = 0$ holds for infinitely many $s \in k$, one concludes immediately from the definition of $L_s(t)$ that the equalities

$$P_{(c_1,c_2,d_1,d_2)}(a_1) = P_{d_2}(a_1)^2 \cdot P_{c'_1}(a_1) = 0$$

hold. In particular, since $P_{(c_1,c_2,d_1,d_2)}(a_1) = 0$, which implies [cf. (b)] that $P_{d_2}(a_1) \neq 0$, one concludes that the equality $P_{c'_1}(a_1) = 0$ holds. This completes the proof of assertion (iii).

Next, we verify assertion (iv). Write $S_{(c_1,c_2,d_1,d_2)} \subseteq k$ for the set of roots of the polynomial $P_{(c_1,c_2,d_1,d_2)}(t)$. Then one concludes from assertion (iii) that the equality

$$\mathrm{Ker}(\psi_{d_1}) = V_{\mathrm{Wr}} \cup \bigcup_{a \in S_{(c_1,c_2,d_1,d_2)}} \{ c \in \mathrm{Ker}(\psi_{d_1}) \mid P_c(a) = 0 \}$$

holds. Now recall that $S_{(c_1,c_2,d_1,d_2)}$ is finite [cf. (a)], and that $V_{\mathrm{Wr}} \neq \mathrm{Ker}(\psi_{d_1})$ [cf. Lemma 3.6]. On the other hand, since the field k is infinite, the linear space $\mathrm{Ker}(\psi_{d_1})$ over k may not be written as the union of finitely many proper sub-k-spaces. Thus, one concludes that, for some $a \in S_{(c_1,c_2,d_1,d_2)}$, the equality

$$\mathrm{Ker}(\psi_{d_1}) = \{ c \in \mathrm{Ker}(\psi_{d_1}) \mid P_c(a) = 0 \}$$

holds. In particular, assertion (iv) holds. This completes the proof of assertion (iv).

Next, we verify assertion (v). Observe that it follows from Lemma 2.11, (ii), that the set $\Sigma(d_1)$ is finite. Moreover, it is immediate that, for each element a of $\Sigma(d_1) \setminus \Sigma(d_2)$, the sub-$k$-space $\{ c \in \mathrm{Ker}(\psi_{d_2}) \mid P_c(a) = 0 \}$ is a proper sub-k-space of $\mathrm{Ker}(\psi_{d_2})$. In particular, since the field k is infinite, the linear space $\mathrm{Ker}(\psi_{d_2})$ over k may not be written as the union of finitely many proper sub-k-spaces. Thus, one concludes that there exists an element c_2' of $\mathrm{Ker}(\psi_{d_2})$ such that $P_{c_2'}(a) \neq 0$ for every element a of $\Sigma(d_1) \setminus \Sigma(d_2)$. This completes the proof of assertion (v).

Next, we verify assertion (vi). Observe that since $c_2' \in \mathrm{Ker}(\psi_{d_2})$, one verifies easily from the various definitions involved that, for every $s \in k$, the element d_2 is of CE-type with respect to $c_2 + sc_2'$, which implies that $(c_1, d_1, c_2 + sc_2', d_2)$ is an element of $I_1 \times I_2$. Moreover, since [we have assumed that] the element (c_1, d_1, c_2, d_2) is contained in V_J, one concludes that the subset

$$\{ (c_1, d_1, c_2 + sc_2', d_2) \mid s \in k \} \subseteq I_1 \times I_2$$

is contained in J.

To verify assertion (vi), assume that, for infinitely many $s \in k$, there is an element of $\Sigma(d_1) \setminus \Sigma(d_2)$ that is a root of the polynomial $R_s(t)$. Then since $\Sigma(d_1)$ is finite [cf. Lemma 2.11, (ii)], there is an element a_2 of $\Sigma(d_1) \setminus \Sigma(d_2)$ that is a root of the polynomial $R_s(t)$ for infinitely many $s \in k$. Thus, one concludes immediately from the definition of $R_s(t)$ that the equalities

$$P_{(c_1,c_2,d_1,d_2)}(a_2) = P_{d_1}(a_2)^2 \cdot P_{c_2'}(a_2) = 0$$

hold. In particular, since $P_{(c_1,c_2,d_1,d_2)}(a_2) = 0$, which implies [cf. (b)] that $P_{d_1}(a_2) \neq 0$, the equality $P_{c_2'}(a_2) = 0$ holds — in contradiction to assertion (v). This completes the proof of assertion (vi).

Next, we verify assertion (vii). Let $c_2' \in \mathrm{Ker}(\psi_{d_2})$ be as in assertion (v). Thus, since the field k is infinite, it follows immediately from assertion (vi) that there exists an element $s \in k$ such that $(c_1, d_1, c_2 + sc_2', d_2)$ is contained in $U_J \cap V_J$ [cf. the discussion in the proof of assertion (vi)], and, moreover, no root of the polynomial $R_s(t)$ is contained in $\Sigma(d_1) \setminus \Sigma(d_2)$. Fix such an element $s \in k$. Then it follows from assertion (iv) — where we take the "(c_1, d_1, c_2, d_2)" of assertion (iv) to be $(c_1, d_1, c_2 + sc_2', d_2)$ — that there exists a root $a \in k$ of the polynomial $R_s(t)$ that is contained in $\Sigma(d_1)$. Then it follows from our choice of s that a is not contained in $\Sigma(d_1) \setminus \Sigma(d_2)$, which implies that the intersection $\Sigma(d_1) \cap \Sigma(d_2)$ is nonempty, as desired. This completes the proof of assertion (vii), hence also of Lemma 3.9. □

Lemma 3.10. — *Let $J \subseteq I_1 \times I_2$ be an irreducible component of $I_1 \times I_2$ such that the image of the composite $J \hookrightarrow I_1 \times I_2 \to C_1 \times C_2$ is dense. Then the subset of J that consists of $(c_1, d_1, c_2, d_2) \in J$ such that the polynomial $P_{(c_1,c_2,d_1,d_2)}(t)$ is not separable is not dense in J.*

Proof. — Assume that, for every element (c_1, d_1, c_2, d_2) of J, the polynomial $P_{(c_1,c_2,d_1,d_2)}(t)$ is not separable. In particular, it follows from Lemma 3.9, (vii), that

(a) for every element (c_1, d_1, c_2, d_2) of $U_J \cap V_J$ [cf. the statement of Lemma 3.9], the intersection $\Sigma(d_1) \cap \Sigma(d_2)$ is nonempty.

Next, observe that, since every fiber of the natural map $I_i \to C_i$ is finite for each $i \in \{1, 2\}$ [cf. Remark 2.12.1, (i)], every fiber of the natural map $I_1 \times I_2 \to C_1 \times C_2$ is finite; in particular, the inequality $\dim(I_1 \times I_2) \leq \dim(C_1 \times C_2) = 2g_1 + 2g_2 + 4$ holds. Thus, since [we have assumed that] J has dense image in $C_1 \times C_2$, one verifies immediately from the [easily verified] equality $\dim(J) = 2g_1 + 2g_2 + 4$ that there exists a nonempty Zariski open subset $U_{C_2} \subseteq C_2$ of C_2 such that

(b) the composite $J \hookrightarrow I_1 \times I_2 \to C_2$ is a dominant morphism whose fiber at an element of $U_{C_2} \subseteq C_2$ is of dimension $2g_1 + 2$, and, moreover,

(c) the fiber at an element of $U_{C_2} \subseteq C_2$ of the composite $J \hookrightarrow I_1 \times I_2 \to C_2$ has dense image in C_1.

Fix an element c_2 of U_{C_2} and write $F_{c_2} \subseteq J$ for the fiber at c_2 of the composite $J \hookrightarrow I_1 \times I_2 \to C_2$. Recall from Remark 2.12.1, (i), that every fiber of the natural map $I_2 \to C_2$ is finite. Thus, one concludes from Lemma 2.11, (i), that

(d) the subset $S \subseteq k$ that consists of the elements of $\Sigma(d_2)$ — where d_2 ranges over the elements of D_2 such that (c_2, d_2) occurs as the third and fourth factors of some element of F_{c_2} — is finite.

Next, observe that it follows from (a) that, for every element (c_1, d_1, c_2, d_2) of $F_{c_2} \cap U_J \cap V_J$, the intersection $\Sigma(d_1) \cap S$ is nonempty. Thus, since [one verifies easily that] $F_{c_2} \cap U_J \cap V_J$ is dense in F_{c_2}, one verifies immediately from (b), (d) that there exists an element a of S such that

(e) the [necessarily closed] subset

$$F'_{c_2} \stackrel{\text{def}}{=} \{ (c_1, d_1, c_2, d_2) \in F_{c_2} \mid a \in \Sigma(d_1) \}$$

of F_{c_2} is of dimension $2g_1 + 2$, hence [cf. (b), (c)] has dense image in C_1.

Next, write $W \subseteq I_1$ for the subset of I_1 that consists of the elements $(c_1, d_1) \in I_1$ such that $a \in \Sigma(d_1)$. Observe that, for a nonzero element d_1 of D_1 and an element b of k, it follows from Lemma 2.11, (iii), that there exists a unique element d'_1 of D_1 such that the equalities $P_{d'_1}(t) = P_{d_1}(t + b)$ and $\Sigma(d'_1) = \{ a' - b \mid a' \in \Sigma(d_1) \}$ hold. In particular, the condition $a \in \Sigma(d'_1)$ holds if and only if the condition $a + b \in \Sigma(d_1)$ holds. Thus, since $\Sigma(d_1)$ is finite [cf. Lemma 2.11, (i)], and the field k is infinite, one concludes that the [necessarily closed] subset $\{ d_1 \in D_1 \mid a \in \Sigma(d_1) \}$ of D_1 is a proper subset of D_1, hence of dimension $\leq g_1 - 1$.

Next, let π, γ be nonnegative integers such that the inequality $\pi \leq g_1 - 1$ holds. Then it follows from Lemma 1.4, (iv), that, for each nonzero element d_1 of D_1 such that the equalities $\deg(P_{d_1}(t)) = \pi$ and $\deg(G_{d_1}(t)) = \gamma$ hold, the fiber of the natural map $I_1 \to D_1$ at d_1 is either empty or of dimension $2g_1 + 2 - \lfloor (2g_1 + 2 + \pi)/3 \rfloor + \gamma$. Thus, if the equalities $\pi = g_1 - 1$ and $\gamma = 0$ hold, then this fiber is of dimension $g_1 + 2$, which implies that the subset of W that lies over such elements is of dimension $\leq (g_1 - 1) + (g_1 + 2) = 2g_1 + 1$. On the other hand, if either $\pi \leq g_1 - 2$ or $\gamma \geq 1$ holds, then since the subset of D_1 that consists of such elements is of dimension $\leq \pi + 1 - 2\gamma$ [cf. the proof of Lemma 2.7, (i)], one verifies easily that the corresponding subset of W is of dimension $\leq 2g_1 + 1$. In particular, the inequality $\dim(W) \leq 2g_1 + 1$ holds. Thus, since every fiber of the natural map $W \to C_1$ is finite [cf. Remark 2.12.1, (i)], the subset $W \subseteq I_1$ does not have dense image in C_1. On the other hand, it is immediate that the image of the closed subset $F'_{c_2} \subseteq F_{c_2}$ of F_{c_2} under the natural projection $I_1 \times I_2 \to I_1$ is contained in W, which implies [cf. (e)] that $W \subseteq I_1$ has dense image in C_1. Thus, we obtain a contradiction. This completes the proof of Lemma 3.10. $\square$

Lemma 3.11. — *There exists a nonempty dense Zariski open subset of $C_1 \times C_2$ such that if (c_1, c_2) is an element of this open subset of $C_1 \times C_2$, then the following four conditions are satisfied:*

(1) *The pair (c_1, c_2) is CE-admissible.*

(2) *The polynomials $M_{c_1}(t)$, $M_{c_2}(t) \in k[t]$ are separable.*

(3) *Let d_1, d_2 be elements of D_1, D_2 that are of CE-type with respect to c_1, c_2, respectively, and let $a \in k$ be such that $P_{(c_1,c_2,d_1,d_2)}(a) = 0$. Then $M_{c_1}(a) \cdot M_{c_2}(a) \cdot P_{d_1}(a) \cdot P_{d_2}(a)$ is nonzero.*

(4) *For each $i \in \{1, 2\}$ and each element $d \in D_i$ of CE-type with respect to c_i, the polynomials $P_d(t)$ and $M_{c_{3-i}}(t)$ have no common root.*

Proof. — This assertion follows immediately from Remark 2.12.1, (i); Lemma 2.9; Lemma 3.8; Lemma 3.10, together with the various definitions involved. □

4. Cartier Eigenforms on a Hyperelliptic Curve in Characteristic Three

In the present §4, we recall some basic facts concerning hyperelliptic curves in characteristic three. In the present §4, let

- $g \geq 2$ be an integer, and let
- k be an algebraically closed field of characteristic three.

Write

$$\mathbb{A}^1_k$$

for the affine line over k and

$$\mathbb{P}^1_k$$

for the smooth compactification of $\mathbb{A}^1_k$, i.e., the projective line over k. Thus, there exists a regular function $t \in \Gamma(\mathbb{A}^1_k, \mathcal{O}_{\mathbb{A}^1_k})$ on $\mathbb{A}^1_k$ that determines an isomorphism of k-algebras

$$k[t] \xrightarrow{\sim} \Gamma(\mathbb{A}^1_k, \mathcal{O}_{\mathbb{A}^1_k}).$$

Moreover, one verifies easily that this regular function $t \in \Gamma(\mathbb{A}^1_k, \mathcal{O}_{\mathbb{A}^1_k})$ on $\mathbb{A}^1_k$ determines a bijective map between the set of closed points of $\mathbb{A}^1_k$ (respectively, $\mathbb{P}^1_k$) and the set k (respectively, $k \sqcup \{\infty\}$). In the remainder of the present paper, let us fix such a regular function $t \in \Gamma(\mathbb{A}^1_k, \mathcal{O}_{\mathbb{A}^1_k})$ on $\mathbb{A}^1_k$ and identify the set of closed points of $\mathbb{A}^1_k$ (respectively, $\mathbb{P}^1_k$) and the set k (respectively, $k \sqcup \{\infty\}$) by means of the bijective map determined by this fixed regular function t.

In the present §4, let

- $A \subseteq \mathbb{A}^1_k$ be a closed subset of $\mathbb{A}^1_k$ of cardinality $2g + 2$.

In particular, the set A may be regarded as a subset of k of cardinality $2g + 2$.

Definition 4.1.

(i) We shall write

$$C_A \stackrel{\text{def}}{=} C(g), \quad D_A \stackrel{\text{def}}{=} D(g), \quad F_A \stackrel{\text{def}}{=} F(g)$$

[cf. Definition 1.3, (i)].

(ii) We shall write

$$c_A \in C_A$$

for the unique element of C_A such that

$$M_{c_A}(t) = \prod_{a \in A}(t-a) \in k[t]$$

[cf. Definition 1.2, (i)].

(iii) We shall refer to a(n) [unordered] pair $\{A_1, A_2\}$ of two nonempty subsets A_1, $A_2 \subseteq A$ of A that satisfies the following three conditions as an *even decomposition* of A:

- The equality $A_1 \cup A_2 = A$ holds.
- The equality $A_1 \cap A_2 = \emptyset$ holds.
- The set A_1, hence also A_2, is of even cardinality.

Definition 4.2. — We shall write

$$\xi_A \colon X_A \longrightarrow \mathbb{P}^1_k$$

for the [uniquely determined] connected finite flat covering of degree two whose branch locus coincides with the reduced closed subscheme of $\mathbb{P}^1_k$ determined by A,

$$\iota_A \in \mathrm{Gal}(X_A/\mathbb{P}^1_k)$$

for the [uniquely determined] nontrivial automorphism of X_A over $\mathbb{P}^1_k$, and

$$\omega_A \stackrel{\mathrm{def}}{=} \omega_{X_A/k}$$

for the cotangent sheaf of X_A/k.

Remark 4.2.1. — It follows from the Riemann-Hurwitz formula that X_A is a projective smooth curve of genus g.

Definition 4.3. — One verifies easily that there exists an open immersion over $\mathbb{P}^1_k$ from the affine scheme

$$\mathrm{Spec}\Big(k[s,t]/\big(s^2 - M_{c_A}(t)\big)\Big)$$

into X_A. Let us fix such an open immersion by means of which we regard the above affine scheme as an open subscheme of X_A. We shall write

$$U_A \subseteq X_A$$

for the [uniquely determined] maximal open subscheme [of the resulting affine open subscheme] of X_A on which the regular function s is invertible [which implies that we have an identification $\mathrm{Spec}(k[s,s^{-1},t]/(s^2 - M_{c_A}(t))) = U_A$ of affine schemes].

LEMMA 4.4. — *The restriction homomorphism*

$$\Gamma(X_A, \omega_A) \longrightarrow \Gamma(U_A, \omega_A)$$

determines an isomorphism of linear spaces over k

$$\Gamma(X_A, \omega_A) \xrightarrow{\sim} \left\{ \frac{P_d(t)dt}{s} \in \Gamma(U_A, \omega_A) \,\middle|\, d \in D_A \right\}$$

[*cf. Definition* 1.2, (i)].

PROOF. — This assertion may be verified by straightforward computation. □

DEFINITION 4.5. — For each $d \in D_A$, we shall write

$$\omega_d \in \Gamma(X_A, \omega_A)$$

for the global section of ω_A that corresponds, via the isomorphism of Lemma 4.4, to

$$\frac{P_d(t)dt}{s} \in \Gamma(U_A, \omega_A).$$

In particular, it follows from Lemma 4.4 that we have an isomorphism of linear spaces over k

$$D_A \xrightarrow{\sim} \Gamma(X_A, \omega_A); \qquad d \longmapsto \omega_d.$$

LEMMA 4.6. — *Let d be a nonzero element of D_A. Then the following assertions hold:*

(i) *Since* [*we have assumed that*] *the field k is algebraically closed, there exist a non-negative integer r and elements a, $a_1, \ldots, a_r$ of k such that the equality*

$$P_d(t) = a \cdot \prod_{i=1}^{r}(t - a_i)$$

holds. Then the zero divisor of the nonzero global section ω_d of ω_A is given by the pull-back, via ξ_A, of the divisor on $\mathbb{P}^1_k$

$$(g - 1 - r)[\infty] + \sum_{i=1}^{r}[a_i]$$

— where we write "$[-]$" for the prime divisor on $\mathbb{P}^1_k$ determined by the closed point of $\mathbb{P}^1_k$ that corresponds to "$(-)$".

(ii) *The following two conditions are equivalent:*

(1) *The nonzero global section ω_d of ω_A is a Cartier eigenform associated to $\mathcal{O}_{X_A}$* [*cf.* [3, Definition A.8, (ii)]].

(2) *The element $d \in D_A$ is a $k^\times$-multiple of an element of D_A of CE-type with respect to c_A* [*cf. Definition* 2.1, (i)].

PROOF. — Assertion (i) follows immediately from the definition of the global section ω_d [cf. Definition 4.5]. Assertion (ii) is a formal consequence of [5, Lemma 3.1, (i)]. This completes the proof of Lemma 4.6. □

Definition 4.7. — Let $\{A_1, A_2\}$ be an even decomposition of A. Then we shall write

$$X_{A_1,A_2} \stackrel{\text{def}}{=} X_{A_1} \times_{\mathbb{P}^1_k} X_{A_2}$$

for the fiber product of ξ_{A_1} and ξ_{A_2} [cf. Definition 4.2],

$$\iota_{A_1,A_2} \stackrel{\text{def}}{=} (\iota_{A_1}, \iota_{A_2}) \in \mathrm{Gal}(X_{A_1,A_2}/\mathbb{P}^1_k)$$

[cf. Definition 4.2] for the automorphism of X_{A_1,A_2} over $\mathbb{P}^1_k$ [necessarily of order two] determined by the automorphisms ι_{A_1} and ι_{A_2}, and

$$\omega_{A_1,A_2} \stackrel{\text{def}}{=} \omega_{X_{A_1,A_2}/k}$$

for the cotangent sheaf of $X_{A_1,A_2}/k$.

Lemma 4.8. — *The following assertions hold:*

(i) *Let $\{A_1, A_2\}$ be an even decomposition of A. Then X_{A_1,A_2} is a projective smooth curve of genus $2g-1$. Moreover, there exists a finite étale morphism of degree two over $\mathbb{P}^1_k$*

$$\xi_{A_1,A_2} \colon X_{A_1,A_2} \longrightarrow X_A$$

such that the Galois group $\mathrm{Gal}(X_{A_1,A_2}/X_A)$ *of ξ_{A_1,A_2} is generated by the automorphism $\iota_{A_1,A_2} \in \mathrm{Gal}(X_{A_1,A_2}/\mathbb{P}^1_k)$.*

(ii) *There exists a uniquely determined bijective map between*

- *the set of isomorphism classes of invertible sheaves on X_A of order two and*
- *the set of even decompositions of A*

that satisfies the following condition: Let $\mathcal{L}$ be an invertible sheaf on X_A of order two. Write $\{A_1, A_2\}$ for the even decomposition of A that corresponds, via the bijective map under consideration, to the isomorphism class of $\mathcal{L}$. Then the invertible sheaf $\xi^*_{A_1,A_2}\mathcal{L}$ [cf. (i)*] on X_{A_1,A_2} is trivial.*

Proof. — These assertions follow immediately from the discussion given in [11, p. 346]. □

Lemma 4.9. — *Let $\mathcal{L}$ be an invertible sheaf on X_A of order two. Write $\{A_1, A_2\}$ for the even decomposition of A that corresponds, via the bijective map of Lemma* 4.8, (ii)*, to the isomorphism class of $\mathcal{L}$. Then the following assertions hold:*

(i) *For each $i \in \{1, 2\}$, the natural morphism $X_{A_1,A_2} \to X_{A_i}$ determines a homomorphism*

$$\Gamma(X_{A_i}, \omega_{A_i}) \longrightarrow \Gamma(X_{A_1,A_2}, \omega_{A_1,A_2}).$$

Moreover, let us fix a trivialization Θ of $\xi^*_{A_1,A_2}\mathcal{L}$ [cf. Lemma 4.8, (i), (ii)*]. Thus, the finite étale morphism ξ_{A_1,A_2}, together with Θ, determines homomorphisms*

$$\Gamma(X_A, \mathcal{L} \otimes_{\mathcal{O}_{X_A}} \omega_A) \longrightarrow \Gamma\big(X_{A_1,A_2}, (\xi^*_{A_1,A_2}\mathcal{L}) \otimes_{\mathcal{O}_{X_{A_1,A_2}}} \omega_{A_1,A_2}\big) \xrightarrow[\Theta]{\sim} \Gamma(X_{A_1,A_2}, \omega_{A_1,A_2}).$$

Then these homomorphisms determine an isomorphism of linear spaces over k

$$\Gamma(X_{A_1}, \omega_{A_1}) \times \Gamma(X_{A_2}, \omega_{A_2}) \xrightarrow{\sim} \Gamma(X_A, \mathcal{L} \otimes_{\mathcal{O}_{X_A}} \omega_A),$$

hence [cf. the final portion of Definition 4.5] an isomorphism of linear spaces over k

$$D_{A_1} \times D_{A_2} \xrightarrow{\sim} \Gamma(X_A, \mathcal{L} \otimes_{\mathcal{O}_{X_A}} \omega_A)$$

[cf. Definition 4.1, (i)].

(ii) *Let $\Theta_{\mathcal{L}}$ be a trivialization of the square of $\mathcal{L}$. Then there exists an element λ of $k^\times$ that satisfies the following condition: Let i be an element of $\{1, 2\}$. Write X_A^F, ω_A^F, $\mathcal{L}^F$, $X_{A_i}^F$, $\omega_{A_i}^F$ for the respective base-changes of X_A, ω_A, $\mathcal{L}$, X_{A_i}, ω_{A_i} by the Frobenius automorphism of k. Then the diagram of modules*

$$\begin{array}{ccc} \Gamma(X_{A_i}, \omega_{A_i}) & \hookrightarrow & \Gamma(X_A, \mathcal{L} \otimes_{\mathcal{O}_{X_A}} \omega_A) \\ \downarrow & & \downarrow \\ \Gamma(X_{A_i}^F, \omega_{A_i}^F) & \hookrightarrow & \Gamma(X_A^F, \mathcal{L}^F \otimes_{\mathcal{O}_{X_A^F}} \omega_A^F) \end{array}$$

— where the horizontal arrows are the [necessarily injective] homomorphisms discussed in (i)*, and the left-hand, right-hand vertical arrows are the Cartier operators associated to $(\mathcal{O}_{X_{A_i}}, \mathrm{id}_{\mathcal{O}_{X_{A_i}}})$, $(\mathcal{L}, \Theta_{\mathcal{L}})$ [cf.* [3, Definition A.4]*], respectively — commutes up to multiplication by $\lambda \in k^\times$.*

(iii) *Let (d_1, d_2) be a nonzero element of $D_{A_1} \times D_{A_2}$. Then since [we have assumed that] the field k is algebraically closed, there exist a nonnegative integer r and elements a, $a_1, \ldots, a_r$ of k such that the equality*

$$P_{(c_{A_1}, c_{A_2}, d_1, d_2)}(t) = a \cdot \prod_{i=1}^{r} (t - a_i)$$

holds. Then the trace with respect to the connected finite flat covering $\xi_A \colon X_A \to \mathbb{P}_k^1$ of degree two [i.e., "$\mathrm{id}_{X_A}^* + \iota_A^*$"] of the zero divisor of the nonzero global section of $\mathcal{L} \otimes_{\mathcal{O}_{X_A}} \omega_A$ determined — by the final isomorphism of (i) *— by $(d_1, d_2) \in D_{A_1} \times D_{A_2}$ is given by the pull-back, via ξ_A, of the divisor on $\mathbb{P}_k^1$*

$$(2g - 2 - r)[\infty] + \sum_{i=1}^{r} [a_i]$$

— where we write "$[-]$" for the prime divisor on $\mathbb{P}_k^1$ determined by the closed point of $\mathbb{P}_k^1$ that corresponds to "$(-)$".

(iv) *Let (d_1, d_2) be a nonzero element of $D_{A_1} \times D_{A_2}$. Then the following two conditions are equivalent:*

(1) *The nonzero global section of $\mathcal{L} \otimes_{\mathcal{O}_{X_A}} \omega_A$ discussed in* (iii) *[i.e., determined by (d_1, d_2)] is a Cartier eigenform associated to $\mathcal{L}$ [cf.* [3, Definition A.8, (ii)]*].*

(2) *There exists an element μ of $k^\times$ such that, for each $i \in \{1, 2\}$, the element μd_i is either zero or of CE-type [cf. Definition 2.1, (i)] with respect to $c_{A_i} \in C_{A_i}$ [cf. Definition 4.1, (i), (ii)].*

PROOF. — Assertions (i), (ii) follow immediately from the discussion given in [11, p. 346]. Next, we verify assertion (iii). First, we verify that $P_{(c_{A_1}, c_{A_2}, d_1, d_2)}(t)$ is nonzero. Assume that $P_{(c_{A_1}, c_{A_2}, d_1, d_2)}(t) = 0$. Then since $A_1 \cap A_2 = \emptyset$, the polynomials $M_{c_{A_1}}(t)$ and $M_{c_{A_2}}(t)$ have no common root. Thus, if $d_1 \neq 0$, it follows from the definition of

$P_{(c_{A_1},c_{A_2},d_1,d_2)}(t)$ that $M_{c_{A_1}}(t)$ divides $P_{d_1}(t)^2$ — in contradiction to the [easily verified] inequalities $\deg(P_{d_1}(t)^2) \leq 2g_{A_1}-2 < 2g_{A_1}+2 = \deg(M_{c_{A_1}}(t))$. In particular, the equality $d_1 = 0$ holds. Thus, since [we have assumed that] the equality $P_{(c_{A_1},c_{A_2},d_1,d_2)}(t) = 0$ holds, one concludes the equality $P_{d_2}(t)^2 \cdot M_{c_{A_1}}(t) = 0$. In particular, the equality $d_2 = 0$ holds — in contradiction to our assumption that (d_1, d_2) is nonzero. This completes the verification of the assertion that $P_{(c_{A_1},c_{A_2},d_1,d_2)}(t)$ is nonzero.

Write u for the nonzero global section of $\mathcal{L} \otimes_{\mathcal{O}_{X_A}} \omega_A$ determined — by the final isomorphism of (i) — by $(d_1, d_2) \in D_{A_1} \times D_{A_2}$ and E for the zero divisor of u. Then since $\mathcal{L}$ is of degree zero, the divisor E is of degree $2g - 2$. Next, observe that since [one verifies easily that] the invertible sheaf $\iota_A^*\mathcal{L}$ is isomorphic to the invertible sheaf $\mathcal{L}$, the element $u \otimes \iota_A^* u$ determines a global section of $\omega_A^{\otimes 2}$ whose zero divisor is $E + \iota_A^* E$. Moreover, one verifies easily from the various definitions involved that this global section of $\omega_A^{\otimes 2}$ coincides, up to a $k^\times$-multiple, with $P_{(c_{A_1},c_{A_2},d_1,d_2)}(t) \cdot (dt/s)^{\otimes 2}$. Thus, since [one verifies immediately that] the zero divisor of the rational function $P_{(c_{A_1},c_{A_2},d_1,d_2)}(t)$ on X_A is given by $\xi_A^*\bigl(\sum_{i=1}^r [a_i] - r[\infty]\bigr)$, and the zero divisor of $dt/s \in \Gamma(X_A, \omega_A)$ is given by $(g-1) \cdot \xi_A^*[\infty]$, one concludes that

$$E + \iota_A^* E = \xi_A^*\Bigl((2g-2-r)[\infty] + \sum_{i=1}^r [a_i]\Bigr),$$

as desired. This completes the proof of assertion (iii). Assertion (iv) follows immediately from assertion (ii) and Lemma 4.6, (ii), together with the various definitions involved. This completes the proof of Lemma 4.9. □

Lemma 4.10. — *Let X be a projective smooth curve of genus ≥ 2 over k and $\xi\colon X \to \mathbb{P}^1_k$ a finite flat covering of degree two. Let ω be a Cartier eigenform on X associated to $\mathcal{O}_X$* [*cf.* [3, Definition A.8, (ii)]], *and let x be a point of X at which ξ is not étale. Suppose that ω is of order ≥ 1 at x. Then ω is of order ≥ 4 at x.*

Proof. — This assertion follows immediately from [3, Proposition 3.2] and [3, Lemma 3.5], together with the various definitions involved. □

5. The Generic Number of Nilpotent Ordinary Indigenous Bundles

In the present §5, we give a proof of the main result of the present paper, i.e., the assertion that there exists a projective smooth hyperelliptic curve in characteristic three that satisfies various ordinariness conditions and an additional condition concerning the Cartier eigenforms [cf. Theorem 5.2 below]. We then compute the number of nilpotent ordinary indigenous bundles over a general curve in characteristic three [cf. Corollary 5.3 below].

Lemma 5.1. — *Let $g \geq 2$ be an integer, and let k be an algebraically closed field of characteristic three. Write*

$$R^+ \overset{\text{def}}{=} k[x_1, \ldots, x_{2g+2}]$$

— *where* $x_1, \ldots, x_{2g+2}$ *are indeterminates* — *and*

$$R \stackrel{\text{def}}{=} R^+ \left[\frac{1}{x_i - x_j} \middle| i, j \in \{1, \ldots, 2g+2\} \text{ such that } i \neq j \right].$$

Write, moreover,

$$\mathcal{X} \longrightarrow \operatorname{Spec}(R)$$

for the projective smooth curve over R *obtained by forming the smooth compactification of the smooth curve over* R

$$\operatorname{Spec}\left(R[s,t]/\big(s^2 - \prod_{i=1}^{2g+2}(t - x_i)\big) \right) \longrightarrow \operatorname{Spec}(R)$$

— *where* s *and* t *are indeterminates. Then the following assertions hold:*

(i) *There exists a nonempty open subscheme* $U \subseteq \operatorname{Spec}(R)$ *of* $\operatorname{Spec}(R)$ *such that the projective smooth curve* $\mathcal{X} \times_{\operatorname{Spec}(R)} U$ *over* U *is parabolically ordinary* [*cf.* [3, Definition A.5, (i)]].

(ii) *Let* $\mathcal{Y} \to \operatorname{Spec}(R)$ *be a projective smooth curve over* R, *and let* $\mathcal{Y} \to \mathcal{X}$ *be a finite étale covering of* $\mathcal{X}$ *of degree two over* R. *Then there exists a nonempty open subscheme* $U_{\mathcal{Y}} \subseteq \operatorname{Spec}(R)$ *of* $\operatorname{Spec}(R)$ *such that the finite étale covering* $\mathcal{Y} \times_{\operatorname{Spec}(R)} U_{\mathcal{Y}} \to \mathcal{X} \times_{\operatorname{Spec}(R)} U_{\mathcal{Y}}$ *over* $U_{\mathcal{Y}}$ *is parabolically new-ordinary* [*cf.* [3, Definition A.5, (ii)]].

Proof. — Assertion (i) follows from [1, Theorem 1]. Assertion (ii) follows immediately from assertion (i), together with Lemma 4.8, (ii), and Lemma 4.9, (ii). This completes the proof of Lemma 5.1. □

Theorem 5.2. — *Let* $g \geq 2$ *be an integer, and let* k *be an algebraically closed field of characteristic three. Then there exists a projective smooth hyperelliptic curve* X *of genus* g *over* k *that satisfies the following three conditions:*

(1) *The projective smooth curve* X *over* k *is parabolically ordinary.*

(2) *Every connected finite étale covering of* X *of degree two is parabolically new-ordinary.*

(3) *Let* $\mathcal{L}$ *be an invertible sheaf on* X *whose square is trivial. Then the zero divisor of every Cartier eigenform associated to* $\mathcal{L}$ *is reduced.*

Proof. — First, observe that it follows immediately from Lemma 2.9, Lemma 3.11, and Lemma 5.1 — together with the [easily verified] fact that there exist only finitely many even decompositions [cf. Definition 4.1, (iii)] of a set of cardinality $2g+2$ — that there exists a subset $A \subseteq k$ of k of cardinality $2g+2$ that satisfies the following four conditions:

(a) The element $c_A \in C(g)$ [cf. Definition 1.3, (i); Definition 4.1, (ii)] is CE-admissible [cf. Definition 2.1, (ii)].

(b) Let $\{A_1, A_2\}$ be an even decomposition of A. Then the pair $(c_{A_1}, c_{A_2}) \in C(\#A_1/2 - 1) \times C(\#A_2/2 - 1)$ [cf. Definition 1.3, (i); Definition 4.1, (ii)] satisfies the following four conditions:

(b-1) For each $i \in \{1, 2\}$, the element $c_{A_i} \in C(\#A_i/2 - 1)$ is CE-admissible.

(b-2) The pair (c_{A_1}, c_{A_2}) is CE-admissible [cf. Definition 3.3].

(b-3) Let d_1, d_2 be elements of $D(\#A_1/2-1)$, $D(\#A_2/2-1)$ [cf. Definition 1.3, (i)] of CE-type with respect to c_{A_1}, c_{A_2}, respectively, and let $a \in k$ be such that $P_{(c_{A_1},c_{A_2},d_1,d_2)}(a) = 0$ [cf. Definition 3.2]. Then $M_{c_{A_1}}(a) \cdot M_{c_{A_2}}(a) \cdot P_{d_1}(a) \cdot P_{d_2}(a)$ [cf. Definition 1.2, (i)] is nonzero.

(b-4) For each $i \in \{1,2\}$ and each element $d \in D(\#A_i/2-1)$ of CE-type with respect to c_{A_i}, no element of A_{3-i} is a root of the polynomial $P_d(t)$.

(c) The projective smooth [necessarily hyperelliptic] curve X_A over k [cf. Definition 4.2] is parabolically ordinary.

(d) Every connected finite étale covering of X_A of degree two is parabolically new-ordinary.

Observe that it follows from Remark 4.2.1 that the projective smooth curve X_A is of genus g. Then conditions (1), (2) that appear in the statement of Theorem 5.2 are none other than conditions (c), (d). Thus, to complete the proof of Theorem 5.2, it suffices to verify condition (3) that appears in the statement of Theorem 5.2. To this end, let $\mathcal{L}$ be an invertible sheaf on X_A whose square is trivial, and let ω be a Cartier eigenform associated to $\mathcal{L}$. Write E for the zero divisor of ω.

First, suppose that $\mathcal{L}$ is trivial. Then it follows from Lemma 4.6, (ii), that ω is a $k^\times$-multiple of ω_d for some element $d \in D(g)$ [cf. Definition 1.3, (i)] of CE-type with respect to c_A [cf. Definition 2.1, (i)]. Now observe that since c_A is CE-admissible [cf. (a)], the polynomial $P_d(t)$ is separable and of degree $g-1$. Thus, it follows from Lemma 4.6, (i), that E coincides with the pull-back, via ξ_A, of the reduced effective divisor $\sum_{i=1}^{g-1}[a_i]$ on $\mathbb{P}^1_k$ — where $a_1, \ldots, a_{g-1}$ are the distinct roots of the polynomial $P_d(t)$. Now observe that since $P_d(t)$ is separable, it follows from Lemma 4.10 that none of $a_1, \ldots, a_{g-1}$ lies in A. Thus, one concludes that E is reduced, as desired.

Next, suppose that $\mathcal{L}$ is nontrivial. Write $\{A_1, A_2\}$ for the even decomposition of A that corresponds — via the bijective map of Lemma 4.8, (ii) — to the isomorphism class of $\mathcal{L}$. Then it follows from Lemma 4.9, (iv), that ω is an element of $\Gamma(X_A, \mathcal{L} \otimes_{\mathcal{O}_{X_A}} \omega_A)$ that corresponds — via the isomorphism of Lemma 4.9, (i) — to $(d_1, d_2) \in D(\#A_1/2-1) \times D(\#A_2/2-1)$, where one of d_1 and d_2 is nonzero, and, moreover, there exists an element μ of $k^\times$ such that, for each $i \in \{1,2\}$, the element μd_i is either zero or of CE-type with respect to c_{A_i}. Now observe that, since the isomorphism of Lemma 4.9, (i), is k-linear, the element of $\Gamma(X_A, \mathcal{L} \otimes_{\mathcal{O}_{X_A}} \omega_A)$ that corresponds to $(\mu d_1, \mu d_2)$ coincides with $\mu\omega$, whose zero divisor coincides with E. Thus, we may assume without loss of generality, by replacing ω by $\mu\omega$ if necessary, that, for each $i \in \{1,2\}$, the element d_i is either zero or of CE-type with respect to c_{A_i}.

Next, suppose that at least one of d_1 and d_2 is zero. Then we may assume without loss of generality, by replacing $(1,2)$ by $(2,1)$ if necessary, that $d_2 = 0$, which implies that $d_1 \neq 0$. Now observe that since c_{A_1} is CE-admissible [cf. (b-1)], the polynomial $P_{d_1}(t)$ is separable and of degree $\#A_1/2-2$. Write $a_1, \ldots, a_{\#A_1/2-2}$ for the distinct roots of the polynomial $P_{d_1}(t)$. Then it follows from Lemma 4.9, (iii), that

$$E + \iota_A^* E = \xi_A^*\Big(2\sum_{i=1}^{\#A_1/2-2}[a_i] + \sum_{a \in A_2}[a]\Big).$$

On the other hand, since [one verifies immediately that] a $k^\times$-multiple of $\xi_{A_1,A_2}^*\omega$ coincides with the pull-back of ω_{d_1} by the natural morphism $X_{A_1,A_2} \to X_{A_1}$, and the equality $\iota_{A_1}^*\omega_{d_1} = -\omega_{d_1}$ holds, one concludes that $\iota_A^*\omega$ is a $k^\times$-multiple of ω, which implies that

$\iota_A^* E = E$. Thus, the equality

$$E = \xi_A^* \Big(\sum_{i=1}^{\#A_1/2-2} [a_i] \Big) + \xi_A^{-1}(A_2)_{\mathrm{red}}$$

— where $\xi_A^{-1}(A_2)_{\mathrm{red}}$ denotes the reduced effective divisor on X_A whose support is $\xi_A^{-1}(A_2)$ — holds. Next, observe that it follows immediately from Lemma 4.10 [cf. also Lemma 4.6, (ii)] that none of $a_1, \ldots, a_{\#A_1/2-2}$ lies in A_1; moreover, it follows from (b-4) that none of $a_1, \ldots, a_{\#A_1/2-2}$ lies in A_2. Thus, none of $a_1, \ldots, a_{\#A_1/2-2}$ lies in A. In particular, the divisor E is reduced, as desired.

Next, suppose that both d_1 and d_2 are nonzero. Then since (c_{A_1}, c_{A_2}) is CE-admissible [cf. (b-2)], the polynomials $P_{d_1}(t)$, $P_{d_2}(t)$, $P_{(c_{A_1}, c_{A_2}, d_1, d_2)}(t) \in k[t]$ are separable and, moreover, of degree $\#A_1/2 - 2$, $\#A_2/2 - 2$, $2g - 2$, respectively. Thus, it follows from Lemma 4.9, (iii), that $E + \iota_A^* E$ coincides with the pull-back, via ξ_A, of the reduced effective divisor $\sum_{i=1}^{2g-2} [a_i]$ on $\mathbb{P}_k^1$ — where $a_1, \ldots, a_{2g-2}$ are the distinct roots of the polynomial $P_{(c_{A_1}, c_{A_2}, d_1, d_2)}(t)$. Moreover, observe that it follows from (b-3) that none of $a_1, \ldots, a_{2g-2}$ lies in A. Thus, one concludes that E is reduced, as desired. This completes the proof of Theorem 5.2. $\square$

Corollary 5.3. — *Let $g \geq 2$ be an integer, and let k be an algebraically closed field of characteristic three. Then there exists a projective smooth hyperelliptic curve X of genus g over k such that the number of isomorphism classes of nilpotent ordinary indigenous bundles* [*cf.* [9, Chapter I, Definition 2.2], [9, Chapter II, Definition 2.4], [9, Chapter II, Definition 3.1]] *over X/k is given by*

$$\frac{3^g - 1}{2} + (2^{2g} - 1) \cdot \frac{3^{g-1} - 1}{2}.$$

Proof. — This assertion is a formal consequence of Theorem 5.2, [3, Theorem 5.2, (ii)], and [3, Corollary 5.3, (ii)]. $\square$

Remark 5.3.1.

(i) The number

$$\frac{3^g - 1}{2} + (2^{2g} - 1) \cdot \frac{3^{g-1} - 1}{2} = \#\mathbb{P}^{g-1}(\mathbb{F}_3) + (2^{2g} - 1) \cdot \#\mathbb{P}^{g-2}(\mathbb{F}_3)$$

that appears in the statement of Corollary 5.3 coincides with the number "$n_{g,0}^{\mathrm{ord}}$" that was discussed in [10, Chapter V] — i.e., the number of isomorphism classes of nilpotent ordinary indigenous bundles over a general projective smooth curve of genus g, which, if $g \geq 3$, is not hyperelliptic. This number is computed in [10, Chapter V] by an entirely different method — that is to say, by means of degeneration to totally degenerate curves and the resulting combinatorics of "molecules" [cf. [10, Chapter V]] — and is given there, for general g, only as a sum over such molecules. Indeed, the number of isomorphism classes of nilpotent ordinary indigenous bundles over a projective smooth curve of genus g takes the value $n_{g,0}^{\mathrm{ord}}$ for every projective smooth curve of genus g that satisfies conditions (1), (2), (3) of Theorem 5.2 — in particular, for the hyperelliptic curve X of Corollary 5.3.

Thus, Corollary 5.3 may be regarded as an explicit closed-form evaluation, in the case of characteristic three, of this number.

(ii) For instance, in the case where $g = 2$, this molecule-theoretic count may be carried out explicitly as follows. Consider a totally degenerate proper curve of genus two whose dual graph is the "theta graph", i.e., the graph consisting of two vertices joined by three edges. The associated molecules are parametrized by the assignments of a radius $\rho_e \in \{0,1\}$ to each of the three edges; a molecule with precisely k toral edges [i.e., edges e with $\rho_e = 1$] contributes 2^k to the count [as the two vertices carry the same radius data, each toral edge is aphilial, so that the weight $2^{n_{\mathrm{aph}}}$ equals 2^k] with the sole exception of the molecule all of whose edges are toral, which is dormant and hence contributes nothing. Thus, one concludes the equalities

$$n^{\mathrm{ord}}_{2,0} = \sum_{k=0}^{2} \binom{3}{k} 2^k = 1 + 6 + 12 = 19 \quad \left(= 3^3 - 2^3\right),$$

which coincides both with the value $p(2p^2+1)/3$ of [10, Chapter V, Corollary 1.3, (3)] and with the case where $g = 2$ of the number displayed above [the same value is necessarily obtained from any other totally degenerate curve of genus two, e.g., the one whose dual graph is the "dumbbell graph", since $n^{\mathrm{ord}}_{2,0}$ does not depend on the choice of degeneration].

(iii) Moreover, the decomposition displayed above — into the contribution $\#\mathbb{P}^{g-1}(\mathbb{F}_3)$ of the trivial invertible sheaf $\mathcal{O}_X$ and the contributions, each equal to $\#\mathbb{P}^{g-2}(\mathbb{F}_3)$, of the $2^{2g} - 1$ nontrivial invertible sheaves whose square is trivial [cf. [3, Theorem 5.2, (ii)], [3, Corollary 5.3, (ii)]] — corresponds to the decomposition of the molecule-theoretic count of [10] according to the associated defect data. Finally, we note that [10, Chapter V, §1, the final Remark] observes that the equality of the numbers obtained from distinct totally degenerate models yields various nontrivial combinatorial identities, the whose significance remains to be clarified. The closed form obtained in Corollary 5.3 endows one side of such an identity with a transparent interpretation in terms of projective spaces over $\mathbb{F}_3$.

Corollary 5.4. — *Let $g \geq 2$ be an integer, and let k be an algebraically closed field of characteristic three. Then the number of isomorphism classes of nilpotent ordinary indigenous bundles over a general projective smooth curve of genus g over k is given by*

$$\frac{3^g - 1}{2} + (2^{2g} - 1) \cdot \frac{3^{g-1} - 1}{2}.$$

Proof. — This assertion is a formal consequence of Corollary 5.3 and [3, Corollary 5.3, (ii)]. □

References

[1] D. Glass and R. Pries, Hyperelliptic curves with prescribed p-torsion, *Manuscripta Math.* **117** (2005), no. 3, 299–317.

[2] R. C. Gunning, Special coordinate coverings of Riemann surfaces, *Math. Ann.* **170** (1967), 67–86.

[3] Y. Hoshi, Nilpotent admissible indigenous bundles via Cartier operators in characteristic three, *Kodai Math. J.* **38** (2015), no. 3, 690–731.

[4] Y. Hoshi, On the supersingular divisors of nilpotent admissible indigenous bundles, *Kodai Math. J.* **42** (2019), no. 1, 1–47.

[5] Y. Hoshi, Hyperbolic ordinariness of hyperelliptic curves of lower genus in characteristic three, *Kyushu J. Math.* **73** (2019), no. 2, 317–335.

[6] Y. Hoshi, *Integrable connections I: two fundamental correspondences*, RIMS Preprint **1902** (July 2019).

[7] Y. Hoshi, *Integrable connections II: divided power stratifications*, RIMS Preprint **1903** (July 2019).

[8] Y. Hoshi, *On indigenous bundles in characteristic three*, RIMS Preprint **1918** (June 2020).

[9] S. Mochizuki, A theory of ordinary p-adic curves, *Publ. Res. Inst. Math. Sci.* **32** (1996), no. 6, 957–1152.

[10] S. Mochizuki, *Foundations of p-adic Teichmüller theory*, AMS/IP Stud. Adv. Math. **11**, Amer. Math. Soc./Int. Press, 1999.

[11] D. Mumford, Prym varieties. I. *Contributions to analysis* (a collection of papers dedicated to Lipman Bers), pp. 325–350 Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1974.

[12] D. Mumford, *Abelian varieties*, Tata Inst. Fund. Res. Stud. Math. **5**, Tata Inst. Fund. Res./Hindustan Book Agency, 2008.

(Yuichiro Hoshi) Research Institute for Mathematical Sciences, Kyoto University, Kyoto 606-8502, JAPAN

Email address: yuichiro@kurims.kyoto-u.ac.jp