The characteristic polynomial of a monodromy transformation attached to a family...

Lorenzini, Dino J.

pp. 111 - 137

Comment. Math. Helvetici **68** (1993) 111–137

0010–2571/93/010111–27$1.50 + 0.20/0

The characteristic polynomial of a monodromy transformation attached to a family of curves

DINO J. LORENZINI[1]

Let K be a complete field with respect to a discrete valuation v. Let $\mathcal{O}_K$ denote the ring of integers in K, and let k be the residue field. We assume that k is algebraically closed and we denote by $p \geq 0$ the residue characteristic. Let X/K be a curve of genus g having a K-rational point. Let A/K denote its jacobian. Let ℓ be a prime, $\ell \neq p$, and denote by $T_\ell(A)$, or simply by T_ℓ when no confusion may result, the Tate module of A/K. The Galois group $\mathrm{Gal}(\bar{K}/K)$ acts in a natural way on the module T_ℓ. In this paper, we describe the characteristic polynomial of a monodromy transformation attached to the action of $\mathrm{Gal}(\bar{K}/K)$ on the module T_ℓ in terms of the special fiber of a regular model $\mathcal{X}/\mathcal{O}_K$ of X/K.

In the first section of this paper, we introduce a polynomial $f_{X/K}(x)$ of degree $2g$ attached to the special fiber of a regular model of X/K. In the second section, we discuss the main result of this paper, Theorem 2.1: a homological interpretation of a factor $f^{(p)}_{X/K}(x)$ of the polynomial $f_{X/K}(x)$. In the third section, we give a description of the behavior of the polynomial $f_{X/K}(x)$ under base change, a description which is a key ingredient in the proof of Theorem 2.1. In the last section of this work, we use a variation on the proof of Theorem 2.1 to describe the characteristic polynomial of an automorphism of a curve acting on the first homology group of the curve.

In a forthcoming article, we will apply Theorem 2.1 to obtain a bound for the order of the p-part of the group of components of a jacobian variety.

1. The polynomial $f_{X/K}(x)$

In this paper, a scheme X/K is called a *curve* if it is a smooth, proper, geometrically irreducible scheme of dimension one, and if the following additional property holds. Let $\mathcal{X}/\mathcal{O}_K$ denote a regular model of X/K. Let $\mathcal{X}_k$ denote the special

---

[1] Research partially supported by a grant from the Swiss National Science Foundation.

fiber of $\mathscr{X}/\mathcal{O}_K$. The closed subscheme $\mathscr{X}_k$ is an effective Cartier divisor and, as such, we write it as

$$\mathscr{X}_k = \sum_{i=1}^{n} r_i C_i,$$

where r_i is the multiplicity of the irreducible component C_i. We include in our definition of a curve that

$$\gcd(r_1, \ldots, r_n) = 1.$$

This condition does not depend on the choice of $\mathscr{X}$. It holds, for instance, if X/K has a K-rational point.

We say that a regular model $\mathscr{X}/\mathcal{O}_K$ of X/K is a *good* model if the following conditions are satisfied:

- The components C_i are smooth curves of genus $g(C_i)$.
- Let $(C_i \cdot C_j)$ denote the intersection number of the components C_i and C_j. If $i \neq j$, then

$$(C_i \cdot C_j) \leq 1.$$

In particular, the reduced curve $(\mathscr{X}_k)_{red}$ has normal crossings.

1.1. Let $\mathscr{X}/\mathcal{O}_K$ be a normal model of X/K. Let $g(C_i)$ denote the geometric genus of the component C_i. We associate to the special fiber $\mathscr{X}_k$ a graph G defined as follows. Its vertices are the curves C_i and a vertex C_h is linked to a vertex C_j if and only if $C_h \cap C_j \neq \emptyset$. For each curve C_i, we define the *degree* of C_i in G to be the integer

$$d(C_i) := |C_i \cap (\overline{\mathscr{X}_k^{red} \setminus C_i})|.$$

When no confusion may result, we denote the integer $d(C_i)$ simply by d_i. When $\mathscr{X}$ is a good model, we find that

$$d(C_i) = \sum_{j \neq i} (C_i \cdot C_j).$$

Let

$$\beta(\mathscr{X}) := \text{first Betti number of } G.$$

One easily checks that

$$2\beta(\mathscr{X}) - 2 = \sum_{i=1}^{n} (d_i - 2).$$

Let

$$\alpha(\mathscr{X}) := \sum_{i=1}^{n} g(C_i).$$

Denote by $f_{\mathscr{X}/\mathscr{O}_K}(x)$ the following rational function:

$$f_{\mathscr{X}/\mathscr{O}_K}(x) := (x-1)^{2\alpha(\mathscr{X}) + 2\beta(\mathscr{X})} \cdot \prod_{i=1}^{n} \left(\frac{x^{r_i} - 1}{x - 1}\right)^{2g(C_i) + d_i - 2}.$$

PROPOSITION 1.2. *Let X/K be a curve of genus g and let $\mathscr{X}/\mathscr{O}_K$ be a good model of X/K.*

(i) *The rational function $f_{\mathscr{X}/\mathscr{O}_K}(x)$ is a polynomial of degree $2g$. It is independent of the choice of a good model for X/K. We denote this polynomial by $f_{X/K}(x)$.*

(ii) *The integers $\alpha(\mathscr{X})$ and $\beta(\mathscr{X})$ are independent of the choice of a good model for X/K. We denote these integers by $\alpha(X/K)$ and $\beta(X/K)$, respectively.*

(iii) *The polynomial $f_G(x) := \prod_{i=1}^{n} [(x^{r_i} - 1)/(x - 1)]^{d_i - 2}$ is independent of the choice of a good model of X/K.*

Proof. To show that $f_{\mathscr{X}/\mathscr{O}_K}(x)$ is a polynomial in $\mathbf{Z}[x]$, it is sufficient to show that

$$f_G(x) := \prod_{i=1}^{n} \left(\frac{x^{r_i} - 1}{x - 1}\right)^{d_i - 2}$$

is a polynomial. The fact that $f_G(x)$ is a polynomial is proved in [Lor], Theorem 3.1. The proof of Theorem 3.1 uses only the algebraic properties of the intersection matrix M. Note that it is by no means obvious that the rational function $f_G(x)$ is a polynomial, since a curve C_i could have multiplicity $r_i \geq 2$ while $d_i = 1$. Note also that, in general, $f_G(x)$ is not a polynomial if $\gcd(r_1, \ldots, r_n) > 1$.

To show that $\deg f_{\mathscr{X}/\mathscr{O}_K}(x) = 2g$, we use the following "adjunction formula":

$$2g - 2 = \mathscr{X}_k \cdot (\mathscr{X}_k + \mathscr{K}),$$

where $\mathscr{K}$ is the relative canonical sheaf of $\mathscr{X}/\mathscr{O}_K$. Recall that $\forall i = 1, \ldots, n$,

$$2g(C_i) - 2 = C_i \cdot (C_i + \mathscr{K}),$$

and

$$(C_i \cdot \mathscr{X}_k) = 0.$$

Hence,

$$\begin{aligned} 2g - 2 &= \mathscr{X}_k \cdot \mathscr{K} \\ &= \sum_i r_i (C_i \cdot \mathscr{K}) \\ &= \sum_i r_i (2g(C_i) - 2 - (C_i \cdot C_i)) \\ &= \sum_i r_i (2g(C_i) - 2) + \sum_i \left(\sum_{j \neq i} r_j (C_i \cdot C_j) \right) \\ &= \sum_i r_i (2g(C_i) - 2) + \sum_i r_i d_i \\ &= \sum_i 2g(C_i) + \sum_i (d_i - 2) + \sum_i (r_i - 1)(d_i - 2) + \sum_i (r_i - 1) 2g(C_i). \end{aligned}$$

As we already pointed out in 1.1, one easily checks that

$$2\beta(\mathscr{X}) - 2 = \sum_{i=1}^{n} (d_i - 2).$$

Hence, $\deg f_{\mathscr{X}/\mathscr{O}_K}(x) = 2g$.

1.3. We turn now to showing that $f_{\mathscr{X}/\mathscr{O}_K}(x)$ does not depend on the choice of a good model. Let $\mathscr{X}/\mathscr{O}_K$ be a good model of X/K and let $\mathscr{Y}_P$ be a model obtained from $\mathscr{X}$ by blowing up a closed point P of $\mathscr{X}_k$. We call the birational map $\pi : \mathscr{Y}_P \to \mathscr{X}$ an *elementary blow-up*. Let E denote the exceptional curve on $\mathscr{Y}_P$. Denote by $\tilde{C}_i$ the strict transform of $C_i \subset \mathscr{X}_k$ in $\mathscr{Y}_P$. Since E is a rational curve, and since $g(C_i) = g(\tilde{C}_i)$ for all $i = 1, \ldots, n$, it follows that

$$\alpha(\mathscr{Y}_P) = \alpha(\mathscr{X}).$$

Let (C_i, r_i) and (C_j, r_j) be two components of $\mathscr{X}_k$. Recall that, if $P \in (C_i, r_i)$ is a regular point of $\mathscr{X}_k$, then E has multiplicity r_i in $\mathscr{Y}_P$ and $(E \cdot \tilde{C}_i) = 1$. Recall also that, if $P = C_i \cap C_j$, then E has multiplicity $r_i + r_j$ in $\mathscr{Y}_P$, with $(E \cdot \tilde{C}_i) =$

$(E \cdot \tilde{C}_j) = 1$ and $(\tilde{C}_i \cdot \tilde{C}_j) = 0$. It follows immediately that $\mathscr{Y}_P$ is a good model of X/K. Using the formula $2\beta(\mathscr{X}) - 2 = \Sigma_{i=1}^{n} (d(C_i) - 2)$, one shows easily that

$$\beta(\mathscr{Y}_P) = \beta(\mathscr{X}).$$

Let G' denote the graph associated to the special fiber of $\mathscr{Y}_P$. If $P \in C_i \cap C_j$, then it is obvious that $f_{G'}(x) = f_G(x)$. If $P \in C_i$ is a regular point of $\mathscr{X}_k$, then the degree of $\tilde{C}_i$ in G' is equal to $d_i + 1$ while the degree of E in G' is equal to 1. Both components E and $\tilde{C}_i$ have multiplicity equal to r_i. Hence, $f_{G'}(x)$ equals $f_G(x)$ in this case also.

1.4. Let $\mathscr{X}_1$ and $\mathscr{X}_2$ denote two good models of $\mathscr{X}$. It is well known that there exists a third model $\mathscr{Y}$ of X and two maps

$$\pi_i : \mathscr{Y} \to \mathscr{X}_i \quad i = 1, 2$$

such that each map π_i is a composition of elementary blow-ups $\pi_{i,j}$:

$$\mathscr{Y} = \mathscr{X}_{i,s_i} \xrightarrow{\pi_{i,s_i}} \cdots \longrightarrow \mathscr{X}_{i,1} \xrightarrow{\pi_{i,1}} \mathscr{X}.$$

Therefore, we can apply 1.3 to each $\pi_{i,j}$ and deduce that $\mathscr{Y}$ is a good model of $\mathscr{X}$ such that

$$f_{\mathscr{X}_1/\mathscr{C}_K} = f_{\mathscr{Y}/\mathscr{C}_K} = f_{\mathscr{X}_2/\mathscr{C}_K},$$

and

$$f_{G(\mathscr{X}_1)}(x) = f_{G(\mathscr{X}_2)}(x).$$

It also follows from 1.3 that $\alpha(\mathscr{X}_1) = \alpha(\mathscr{Y}) = \alpha(\mathscr{X}_2)$ and $\beta(\mathscr{X}_1) = \beta(\mathscr{Y}) = \beta(\mathscr{X}_2)$. This concludes the proof of Proposition 1.2. □

15. Let q be any prime and let r be any integer. Let $r^{(q)}$ denote the largest prime-to-q integer dividing r. Let $\mathrm{ord}_q(r)$ be defined by the factorization

$$r = r^{(q)} \cdot q^{\mathrm{ord}_q(r)}.$$

We let

$$r^{(0)} := r,$$

so that the integer $r^{(p)}$ is defined for all possible values of the residual characteristic p.

Let

$$f^{(q)}_{X/K}(x) := (x-1)^{2\alpha(X)+2\beta(X)} \cdot \prod_{i=1}^{n} \left(\frac{x^{r_i^{(q)}} - 1}{x-1} \right)^{2g(C_i)+d_i-2}.$$

We let

$$f^{(0)}_{X/K}(x) := f_{X/K}(x),$$

so that the rational function $f^{(p)}_{X/K}(x)$ is also defined for all possible values of the residual characteristic p.

COROLLARY 1.6. *Let X/K be a curve. Let q be any prime. The rational function $f^{(q)}_{X/K}(x)$ is a polynomial with integer coefficients, and is independent of the choice of a good regular model for X/K.*

Proof. Let $\Phi_s(x)$ denote the minimal polynomial over $\mathbf{Z}$ of a primitive s^{th} root of unity. Recall that

$$(x^r - 1) = \prod_{s \mid r} \Phi_s(x).$$

Our corollary follows immediately from the fact that

$$\prod_{i=1}^{n} [(x^{r_i^{(q)}} - 1)/(x-1)]^{d_i - 2} = \prod_{\Phi_s(x) \mid f_G(x),\ q \nmid s} \Phi_s(x)^{\operatorname{ord}_{\Phi_s(x)}(f_G(x))}. \qquad \square$$

Remark 1.7. Let $f(x)$ be a product of cyclotomic polynomials. Let q be any prime. The prime-to-q part $f^{(q)}(x)$ of $f(x)$ is defined as follows:

$$f^{(q)}(x) := \prod_{\substack{\Phi_s(x) \mid f(x) \\ q \nmid s}} (\Phi_s(x))^{\operatorname{ord}_{\Phi_s(x)}(f(x))}.$$

It follows from this definition that the polynomial $f^{(q)}_{X/K}(x)$ is the prime-to-q part of the polynomial $f_{X/K}(x)$.

2. Homological Interpretation of $f^{(p)}_{X/K}(x)$

Let X/K be a curve and let A/K denote its jacobian. Let ℓ be a prime, $\ell \neq p$. Let $T_\ell(A)$ denote the Tate module of A/K. We denote $T_\ell(A)$ simply by T_ℓ when no

confusion may result. Fix a separable closure K^s of K. The free $\mathbf{Z}_\ell$-module T_ℓ is equipped with a natural action of the Galois group $\mathrm{Gal}(K^s/K)$. Note that, under our hypothesis on K, the group $\mathrm{Gal}(K^s/K)$ is equal to its inertia subgroup $I_K := I(K^s/K)$. Let P denote the pro-p-Sylow subgroup of I_K. The group I_K acts on $(T_\ell A)^P$ through its quotient

$$I_K/P \cong \prod_{\ell \neq p} \mathbf{Z}_\ell.$$

Let σ be a topological generator of I_K/P, and let σ_ℓ denote its image in $\mathrm{Aut}(T_\ell^P)$. We let $\mathrm{char}(\sigma_\ell)(x)$ denote the characteristic polynomial of σ_ℓ acting on $(T_\ell A)^P$.

When $p = 0$ and q is any prime, let Q denote the pro-q-Sylow subgroup of I_K. This subgroup Q is normal in I_K and, therefore, the module T_ℓ^Q is I_K-invariant. We denote by $\sigma_{\ell,Q}$ the image in $\mathrm{Aut}(T_\ell^Q)$ of a topological generator σ of I_K. We let $\mathrm{char}(\sigma_{\ell,Q})(x)$ denote the characteristic polynomial of $\sigma_{\ell,Q}$.

THEOREM 2.1. *Let X/K be a curve and let A/K denote its jacobian.*
(i) *The polynomials $f^{(p)}_{X/K}(x)$ and $\mathrm{char}(\sigma_\ell)(x)$ are equal.*
(ii) *If $p = 0$, and if q and ℓ are distinct primes, then $f^{(q)}_{X/K}(x) = \mathrm{char}(\sigma_{\ell,Q})(x)$.*

COROLLARY 2.2 (T. Saito, [Sai], Corollary 1.6). *Under the above hypothesis and notations,*

$$\mathrm{rank}_{\mathbf{Z}_\ell}(T_\ell A)^P = 2\alpha(X/K) + 2\beta(X/K) + \sum_{i=1}^{n} (r_i^{(p)} - 1)(d(C_i) - 2 + 2g(C_i)).$$

Remark 2.3. The automorphism σ_ℓ may be called a *monodromy transformation*, consistent with the terminology used in the complex case. Recall that in the "dictionary" between algebraic geometry and the theory of complex manifolds, our situation

$$\begin{array}{ccccc} X_{K^s} & \to & X & \subset & \mathscr{X} \\ \downarrow & & \downarrow \pi' & & \downarrow \pi \\ \mathrm{Spec}(K^s) & \to & \mathrm{Spec}(K) & \subset & \mathrm{Spec}(\mathscr{O}_K) \end{array}$$

corresponds to a situation

$$\begin{array}{ccccc} \mathbf{X}_\eta & \to & \mathbf{X}\backslash\mathbf{X}_0 & \subset & \mathbf{X} \\ \downarrow & & \downarrow p' & & \downarrow p \\ \eta & \hookrightarrow & \Delta^* & \subset & \Delta \end{array}$$

where Δ is a small disk in the plane centered at the origin, $\Delta^* := \Delta \setminus \{0\}$, and $\eta \in \Delta^*$. The natural action of $\pi_1(\Delta^*, \eta)$ on $H_1(\mathbf{X}_\eta, \mathbf{Z})$ corresponds to the action of $\mathrm{Gal}(K^s/K)$ on $T_\ell A$.

Let $\rho : \pi_1 \to \mathrm{Aut}(M)$ be a representation of a fundamental group π_1 on a module M. In the classical terminology, the elements of $\rho(\pi_1)$ are called *monodromy transformations*. The interested reader will have no difficulty in adapting the proof of our theorem to the complex case. Steenbrink has informed us that the analogue of our result in the complex case can be proven using the tools and methods introduced in his paper [Ste].

Remark 2.4. Let K be a field of equicharacteristic zero and let X/K be a curve of genus g. If the special fiber of a good model of X/K is reduced, then X/K has semistable reduction ([D–M], 2.2), and

$$f_{X/K}(x) = (x-1)^{2g}.$$

The semistable reduction theorem for curves ([D–M], 2.4, and [Gro], IX, 3.5) states that the curve has semistable reduction if and only if the inertia group I_K acts on $T_\ell A$ in a unipotent way. Therefore, when the special fiber of a good model of X/K is reduced,

$$\mathrm{char}(\sigma_\ell)(x) = (x-1)^{2g}.$$

Hence, in this case, $f_{X/K}(x) = \mathrm{char}(\sigma_\ell)(x)$.

The two main ingredients in the proof of our theorem are the semistable reduction theorem and the following explicit description of the behavior of $f_{X/K}(x)$ under base extension.

2.5. Let $\Phi_u(x)$ denote the minimal polynomial over $\mathbf{Z}$ of a primitive u^{th} root of unity. Let q be any prime. Define

$$\Gamma_q(\Phi_u(x)) := \begin{cases} \Phi_u(x) & \text{if } q \nmid u. \\ [\Phi_{u/q}(x)]^{q-1} & \text{if } q \mid u,\ q^2 \nmid u. \\ [\Phi_{u/q}(x)]^q & \text{if } q^2 \mid u. \end{cases}$$

When $f(x) = \prod_i \Phi_{u_i}(x)$ is a product of cyclotomic polynomials, let

$$\Gamma_q(f(x)) = \prod_i \Gamma_q(\Phi_{u_i}(x)).$$

Let $d = q_1^{a_1} \cdots q_k^{a_k}$ be any integer. Define

$$\Gamma_d := (\Gamma_{q_1})^{a_1} \circ \cdots \circ (\Gamma_{q_k})^{a_k}.$$

Note that, if the characteristic polynomial $\mathrm{char}_\tau(x)$ of an automorphism τ of $\mathbf{Z}^{2g}$ is equal to a product of cyclotomic polynomials, then the characteristic polynomial of τ^d is equal to $\Gamma_d(\mathrm{char}_\tau(x))$.

PROPOSITION 2.6. *Let X/K be a curve. Let d be any integer prime to p. Let K_d/K denote the unique (cyclic) extension of K of degree d. Then*

$$f_{X_{K_d}/K_d}(x) = \Gamma_d(f_{X/K}(x)).$$

We postpone the proof of this proposition to the next section and turn now to the proof of Theorem 2.1. We need to recall some standard facts about abelian varieties and their Néron models. Let A/K be an abelian variety and let $\mathscr{A}/\mathscr{O}_K$ denote its Néron model. The connected component of zero of the special fiber of $\mathscr{A}$, denoted by $\mathscr{A}_k^0/k$, is a smooth connected group scheme. As such, it can be described by an exact sequence

$$0 \to \mathscr{U} \times \mathscr{T} \to \mathscr{A}_k^0 \to \mathscr{B} \to 0$$

of smooth group schemes over k, where $\mathscr{U}$ is unipotent of dimension u_K, $\mathscr{T}$ is a torus of dimension t_K, and $\mathscr{B}$ is an abelian variety of dimension a_K.

2.7. Raynaud has shown in [Ray] (see also [BLR], Theorem 4 on page 267 and Propositions 9 and 10 on pages 248–249) that, if X/K is a curve and A/K denotes its jacobian, then

$$\alpha(X/K) = a_K$$

and

$$\beta(X/K) = t_K.$$

2.8. Fix a prime $\ell \neq p$ and fix a polarization of A/K. Associated to this polarization is a Galois invariant skew-symmetric separating pairing:

$$\langle\ ,\ \rangle : T_\ell A \times T_\ell A \to T_\ell \mathbf{G}_m \cong \mathbf{Z}_\ell.$$

When $X \subseteq T_\ell$ is any submodule, we let $X^\perp$ denote the orthogonal complement of X under the pairing $\langle\ ,\ \rangle$. When M/K is any finite extension, we let

$$W_{\ell,M} := T_\ell^{I_M} \cap (T_\ell^{I_M})^\perp.$$

We refer the reader to [Gro], IX, §2 and §3, for a proof of the following facts:

- $\operatorname{rank}_{\mathbf{Z}_\ell}(W_{\ell,K}) = t_K$.
- $\operatorname{rank}_{\mathbf{Z}_\ell}(T_\ell^{I_K}) = 2a_K + t_K$.
- There exists a finite extension L/K, minimal with the property that

$$(W_{\ell,L})^\perp = T_\ell^{I_L}.$$

2.9. Let $q = p$ or, when $p = 0$, let q be any prime. Let Q denote the pro-q-Sylow subgroup of I_K. If $\ell \neq q$, then the image Q_0 of Q in $\operatorname{Aut}(T_\ell A)$ is a *finite* group, and $|Q_0|$ is invertible in $\mathbf{Z}_\ell$. Therefore, the averaging map

$$T_\ell A \to (T_\ell A)^Q$$

$$x \to 1/|Q_0| \cdot \sum_{\tau \in Q_0} \tau(x)$$

is well defined. The above map is a section to the inclusion $(T_\ell A)^Q \subseteq T_\ell A$. Hence, the functor which associates to a module X its module of Q-invariants X^Q is exact. It is easy to check (see for instance [L–O], 1.1, when $Q = P$) that the pairing $\langle\ ,\ \rangle$ restricts to a nondegenerate pairing on T_ℓ^Q, denoted again by

$$\langle\ ,\ \rangle : T_\ell^Q \times T_\ell^Q \to \mathbf{Z}_\ell.$$

When $Y \subseteq T_\ell^Q$ is any submodule, we let $Y^\S$ denote the orthogonal complement of Y under the restricted pairing. If $X \subseteq T_\ell$ is any submodule, then

$$(X^Q)^\S = (X^\perp)^Q.$$

2.10. Let us now show that the characteristic polynomial $\operatorname{char}(\sigma_\ell)(x)$ of σ_ℓ acting on T_ℓ^P has integer coefficients. The proof of this claim presented here will also show that the polynomial $\operatorname{char}(\sigma_\ell)(x)$ is independent of ℓ ($\ell \neq p$), but this fact will not be used in the proof of Theorem 2.1.

Let L/K again denote the extension of K minimal with the property that $(W_{\ell,L})^\perp = T_\ell^{I_L}$. Let L_0 denote the maximal tame extension of K in L. Consider the inclusions

$$W_{\ell,L_0} \subseteq T_\ell^{I_{L_0}} \subseteq T_\ell^P.$$

Let $f_{W_{\ell,L_0}}(x)$ and $f_{T_\ell^{I_{L_0}}}(x)$ denote the characteristic polynomials of σ_ℓ restricted respectively to W_{ℓ,L_0} and $T_\ell^{I_{L_0}}$. Since

$T_\ell^P / T_\ell^{I_{L_0}}$ is isomorphic to W_{ℓ,L_0},

it follows that, in order to prove our claim, we need only to show that the polynomials $f_{W_{\ell,L_0}}(x)$ and $f_{T_\ell^{I_{L_0}}}(x)$ have integer coefficients and are independent of ℓ ($\ell \neq p$). Grothendieck showed, in [Gro], IX, Théorème 4.3, that the characteristic polynomial of any element τ of I_K acting on T_ℓ has integer coefficients. His proof can be modified to give a proof of our claim, as we shall now sketch for the convenience of the reader.

Let $\mathscr{A}_{L_0}$ denote the Néron model of A_{L_0}/L_0. Let $\mathscr{A}^0_{L_0,k}$ denote the connected component of zero in the special fiber of $\mathscr{A}_{L_0}$. The smooth group scheme $\mathscr{A}^0_{L_0,k}$ is an extension of an abelian variety $\mathscr{B}$ by the product of a torus $\mathscr{T}$ and a unipotent group $\mathscr{U}$:

$$0 \to \mathscr{U} \times \mathscr{T} \to A^0_{L_0,k} \to \mathscr{B} \to 0.$$

Any element σ of I_K induces two automorphisms

$$\sigma_{\mathscr{T}} : \mathscr{T} \to \mathscr{T}$$

and

$$\sigma_{\mathscr{B}} : \mathscr{B} \to \mathscr{B}.$$

Both automorphisms, σ_T and $\sigma_{\mathscr{B}}$, induce automorphisms of the corresponding Tate modules,

$$\sigma_{\mathscr{T}} : T_\ell(\mathscr{T}) \to T_\ell(\mathscr{T})$$

and

$$\sigma_{\mathscr{B}} : T_\ell(\mathscr{B}) \to T_\ell(\mathscr{B}).$$

Grothendieck shows in [Gro], IX, 4.2, that $T_\ell(\mathscr{T})$ and W_{ℓ,L_0} are isomorphic I_K-modules. He also shows that $T_\ell(\mathscr{B})$ and $T_\ell^{I_{L_0}}/W_{\ell,L_0}$ are isomorphic I_K-modules. It was proven by Weil (see [Mil], 12.9) that the characteristic polynomial of $\sigma_{\mathscr{B}}$ acting on $T_\ell(\mathscr{B})$ has integer coefficients and is independent of $\ell \neq p$. Grothendieck shows in the proof of Théorème 4.3 of [Gro], IX, that the characteristic polynomial of $\sigma_{\mathscr{T}}$ on $T_\ell(\mathscr{T})$ has integer coefficients and is independent of $\ell \neq p$. Therefore, our claim is proved.

2.11. *Proof of Theorem* 2.1, *Part* (*i*). We proceed by induction on the integer $\lambda(X/K)$ defined below. Let $\mathscr{X}/\mathscr{O}_K$ be a normal model of X/K. Write $\mathscr{X}_k^{red} = \bigcup C_i$,

where C_i is an irreducible component of multiplicity r_i and genus $g(C_i)$. Let $d(C_i)$ denote the degree of the vertex C_i in the associated graph $G(\mathscr{X})$. Set

$$\lambda_{\mathscr{X}/\mathscr{O}_K} := \operatorname{lcm}\,(r_i^{(p)} \mid g(C_i) > 0 \text{ or } d(C_i) > 2).$$

Let

$$\lambda(X/K) := \min\,\{\lambda_{\mathscr{X}/\mathscr{O}_K} \mid \mathscr{X}/\mathscr{O}_K \text{ is a regular good model of } X/K\}.$$

The properties of $\lambda(X/K)$ needed in the proof of our theorem are summarized in the following proposition, whose proof is postponed to the next section.

PROPOSITION 2.12. *Let X/K be a curve. Let d be any integer prime to p and let K_d/K denote the unique extension of K of degree d. Then*

(i) *$\lambda(X_{K_d}/K_d)$ divides $\lambda(X/K)$ and, if d divides $\lambda(X/K)$, then $\lambda(X_{K_d}/K_d)$ divides $d^{-1}\lambda(X/K)$.*

(ii) *If $\lambda(X/K) = 1$, then $\alpha(X_{K_d}/K_d) = \alpha(X/K)$ and $\beta(X_{K_d}/K_d) = \beta(X/K)$.*

2.13. Assume now that $\lambda(X/K) = 1$, so that $f_{X/K}^{(p)}(x) = (x-1)^{2\alpha(X/K)+2\beta(X/K)}$. We claim that in order to prove Theorem 2.1 under this assumption, it is sufficient to show that

$$W_{\ell,K}^{\S} = T_\ell^{I_K}.$$

Indeed, the automorphism σ_ℓ acts trivially on $T_\ell^{I_K}$ and on $W_{\ell,K}$. Hence, when $W_{\ell,K}^{\S} = T_\ell^{I_K}$, it also acts trivially on

$$T_\ell^P/T_\ell^{I_K} = T_\ell^P/W_{\ell,K}^{\S} \cong W_{\ell,K}.$$

Therefore, all the eigenvalues of σ_ℓ on T_ℓ^P are equal to one and the characteristic polynomial of σ_ℓ is equal to

$$(x-1)^{2a_K+2t_K}.$$

Raynaud's result quoted in 2.7 implies that $a_K = \alpha(X/K)$ and that $t_K = \beta(X/K)$, which proves our claim.

Let us now show that $W_{\ell,K}^{\S} = T_\ell^{I_K}$ when $\lambda(X/K) = 1$. Let $L_0 \subseteq L$ denote the extension of K corresponding to the inertia group $I_{L_0} := I_L \cdot P$. The extension L_0/K is tame and cyclic. Therefore, Proposition 2.12 implies that

$$\lambda(X_{L_0}/L_0) = \lambda(X/K) = 1,$$

and that

$$a_{L_0} = \alpha(X_{L_0}/L_0) = \alpha(X/K) = a_K,$$

and that

$$t_{L_0} = \beta(X_{L_0}/L_0) = \beta(X/K) = t_K.$$

Hence, $T_\ell^{I_K}$ and $T_\ell^{I_{L_0}}$ have the same rank. Since $T_\ell^{I_{L_0}}$ contains $T_\ell^{I_K}$, the group $T_\ell^{I_{L_0}}/T_\ell^{I_K}$ is finite, from which one easily deduces that

$$T_\ell^{I_K} = T_\ell^{I_{L_0}}.$$

In particular,

$$W_{\ell,K} = W_{\ell,L_0}.$$

Note that, by definition of L_0, the group P is equal to the pro-p-Sylow subgroup of I_{L_0}. Hence, the operation $(-)^{\S}$ is the same for both ground fields K and L_0. Therefore, to prove that $W_{\ell,K}^{\S} = T_\ell^{I_K}$, it is sufficient to show that

$$W_{\ell,L_0}^{\S} = T^{I_{L_0}}.$$

Note that

$$\begin{aligned}(W_{\ell,L})^P &= [T_\ell^{I_L} \cap (T_\ell^{I_L})^\perp]^P \\ &= (T_\ell^{I_L})^P \cap [(T_\ell^{I_L})^P]^{\S} \\ &= T_\ell^{I_{L_0}} \cap (T_\ell^{I_{L_0}})^{\S} \\ &= T_\ell^{I_{L_0}} \cap (T_\ell^{I_{L_0}})^\perp \\ &= W_{\ell,L_0}.\end{aligned}$$

Therefore,

$$\begin{aligned}(W_{\ell,L_0})^{\S} &= [(W_{\ell,L})^P]^{\S} \\ &= [(W_{\ell,L})^\perp]^P \\ &= (T^{I_L})^P = T^{I_{L_0}}.\end{aligned}$$

This concludes the proof of our theorem when $\lambda(X/K) = 1$.

2.14. The proof of our theorem in general, by induction on the integer $\lambda(X/K)$, proceeds as follows. If d divides $\lambda := \lambda(X/K)$, then

σ^d is a topological generator of I_{K_d}/P.

By construction,

$$\mathrm{char}(\sigma_\ell^d) = \Gamma_d(\mathrm{char}(\sigma_\ell)).$$

Proposition 2.6 implies that, if d divides λ, then

$$f^{(p)}_{X_{K_d}/K_d}(x) = \Gamma_d(f^{(p)}_{X/K}(x)).$$

Proposition 2.12 implies that, if d divides λ and $d \neq 1$, then $\lambda(X_{K_d}/K_d)$ strictly divides $\lambda(X/K)$. Hence, by induction,

$$f^{(p)}_{X_{K_d}/K_d}(x) = \mathrm{char}(\sigma_\ell^d)(x)$$

for all $d \mid \lambda$, $d \neq 1$. It also follows from Proposition 2.12 that $\lambda(X_{K_\lambda}/K_\lambda) = 1$. Therefore, by induction, it follows that

$$f^{(p)}_{X_{K_\lambda}/K_\lambda}(x) = (x-1)^{\mathrm{rank}_{\mathbf{Z}_\ell}(T_\ell^P)} = \mathrm{char}(\sigma_\ell^\lambda)(x).$$

Lenstra and Oort have shown in [L–O], 1.3, that the multiplicity of the integer one as eigenvalue of σ_ℓ on T_ℓ^P is equal to $2a_K + 2t_K$. Raynaud's Theorem quoted in 2.7 implies that $2a_K + 2t_K$ is equal to $2\alpha(X/K) + 2\beta(X/K)$. Therefore, it follows from the definitions of $f^{(p)}_{X/K}(x)$ and $\mathrm{char}(\sigma_\ell)(x)$ that the multiplicity of $(x-1)$ in $f^{(p)}_{X/K}(x)$ is equal to the multiplicity of $(x-1)$ in $\mathrm{char}(\sigma_\ell)(x)$. Hence, in order to conclude the proof of Theorem 2.1, we need only to prove the following lemma.

LEMMA 2.15. *Let $f(x)$ and $g(x)$ be two polynomials in $\mathbf{Z}[x]$ whose roots are roots of unity of order dividing λ. Suppose that*

(i) *If d divides λ and $d \neq 1$, then $\Gamma_d(f(x)) = \Gamma_d(g(x))$.*

(ii) *The multiplicity of the integer one as root of $f(x)$ is equal to the multiplicity of the integer one as root of $g(x)$.*

Then $f(x) = g(x)$.

Proof. Without loss of generality, we may assume that λ is minimal with the property that

$$\Gamma_\lambda(f(x)) = (x-1)^{\deg f}.$$

Let $B_r(f)$ (resp. $B_r(g)$) denote the set of roots of $f(x)$ (resp. of $g(x)$) having order dividing r. By hypothesis,

$$B_1(f) = B_1(g),$$

and, if $r \neq 1$, then

$$B_r(f) = \text{multiplicity of } (x-1) \text{ in } \Gamma_r(f) = B_r(g).$$

Let $P_r(f)$ (resp. $P_r(g)$) denote the set of primitive r-th roots of unity in $B_r(f)$ (resp. in $B_r(g)$). Clearly,

$$|B_r(f)| = \sum_{d \mid r} |P_d(f)|.$$

Applying the Möbius inversion formula, we find that

$$|P_r(f)| = \sum_{d \mid r} \mu(d) |B_{r/d}(f)|.$$

It follows that

$$|P_r(f)| = |P_r(g)|, \quad \forall r \mid \lambda.$$

Since $f(x)$ and $g(x)$ have integer coefficients, we conclude that the multiplicity of $\Phi_r(x)$ in $f(x)$ is equal to

$$|P_r(f)|/\deg \Phi_r(x).$$

Therefore, the multiplicity of $\Phi_r(x)$ in $f(x)$ is equal to the multiplicity of $\Phi_r(x)$ in $g(x)$. □

2.16. *Proof of Theorem* 2.1, *Part* (*ii*). Assume that $p = 0$, and let q be any prime. One can prove Part (ii) in virtually the same way as Part (i), proceeding by induction on the integer $\mu(X/K)$ defined as follows. Let

$$\mu(\mathscr{X}/\mathscr{O}_K) := \text{lcm } (r_i^{(q)} \mid g(C_i) > 0 \text{ or } d(C_i) > 2),$$

and define

$$\mu(X/K) := \min \{\mu(\mathscr{X}/\mathscr{O}_K) \mid \mathscr{X}/\mathscr{O}_K \text{ is a regular good model of } X/K\}.$$

We leave the details of such a proof to the reader and turn now to a different proof of Part (ii). We will show that, in fact, Part (ii) follows from Part (i).

We need to show that

$$\mathrm{char}(\sigma_{\ell,Q})(x) = f^{(q)}_{X/K}.$$

Recall that, in the terminology of Remark 1.7, the polynomial $f^{(q)}_{X/K}(x)$ is equal to the prime-to-q part of the polynomial $f_{X/K}(x)$. Recall also that Part (i) implies that $f_{X/K}(x) = \mathrm{char}(\sigma_\ell)(x)$. Therefore, we need only to show that

$$\mathrm{char}(\sigma_{\ell,Q})(x) = \text{prime-to-}q \text{ part of } \mathrm{char}(\sigma_\ell)(x).$$

Let L/K denote the extension of K minimal with the property that A_L/L has semistable reduction. Let L_q/K denote the unique subfield of L such that

$$[L : L_q] = q^{\mathrm{ord}_q([L:K])}.$$

Consider the inclusions

$$W_{\ell,L} \subseteq T_\ell^{I_L} \subseteq T.$$

Taking the Q-invariant submodules of these modules, we obtain

$$W_{\ell,L_q} \subseteq T_\ell^{I_{L_q}} \subseteq T^Q.$$

Let $g_{W_{\ell,L}}(x)$ and $g(x)$ denote respectively the characteristic polynomial of σ_ℓ restricted to $W_{\ell,L}$ and to $T_\ell^{I_L}/W_{\ell,L}$. Similarly, let $h_{W_{\ell,L_q}}(x)$ and $h(x)$ denote respectively the characteristic polynomial of σ_ℓ restricted to $W_{\ell,L_q} = (W_{\ell,L})^Q$ and to $T_\ell^{I_{L_q}}/W_{\ell,L_q} = (T_\ell^{I_L}/W_{\ell,L})^Q$. Note that, as in the proof of Part (i), one can show that

$$W^{\S}_{\ell,L_q} = T^{I_{L_q}}.$$

Therefore,

$$\mathrm{char}(\sigma_{\ell,Q})(x) = (h_{W_{\ell,L_q}}(x))^2 \cdot h(x).$$

Hence, to prove Part (ii), it is sufficient to show that

$$h_{W_{\ell,L_q}}(x) = g^{(q)}_{W_{\ell,L}}(x)$$

and

$$h(x) = g^{(q)}(x).$$

Since I_K acts on the modules $W_{\ell,L}$ and $T_\ell^{I_L}/W_{\ell,L}$ through the finite cyclic quotient I_K/I_L, our claim follows from our next lemma.

LEMMA 2.17. *Let G be a cylic group of order m generated by an element τ. Let q be a prime and denote by G_q the q-Sylow subgroup of G. Let X be a free $\mathbf{Z}_\ell$-module on which τ acts and assume that the characteristic polynomial of τ has integer coefficients. Then the characteristic polynomial of τ restricted to X^{G_q} has integer coefficients and is equal to the prime-to-q part of the characteristic polynomial of τ on X.*

Proof. Let a and b be two integers such that $am^{(q)} + bq^{\mathrm{ord}_q(m)} = 1$. Clearly, $\gcd(q, a) = 1 = \gcd(b, m^{(q)})$. Let

$$\gamma := (\tau^{m^{(q)}})^a \quad \text{and} \quad \delta = (\tau^{q^{\mathrm{ord}_q(m)}})^b.$$

We find that $\tau = \gamma \cdot \delta$. Let F be an algebraic closure of $\mathbf{Q}_\ell$. Since γ and δ commute, we can find a basis for $X^{G_q} \otimes_{\mathbf{Z}_\ell} F$ such that both γ and δ are in diagonal form in that basis. Similarly, we can find a basis for $(X/X^{G_q}) \otimes_{\mathbf{Z}_\ell} F$ such that both γ and δ are in diagonal form in that basis. Since γ is a generator of G_q, the operator γ has no eigenvalues equal to 1 when restricted to X/X^{G_q}. Therefore, the eigenvalues of the characteristic polynomial of $\gamma\delta$ restricted to X/X^{G_q} are roots of unity of order divisible by q. Since γ is the identity when restricted to X^{G_q} and since the eigenvalues of δ restricted to X^{G_q} are roots of unity of order prime to q, we conclude that the characteristic polynomial of τ restricted to X^{G_q} has integer coefficients and that it is equal to the prime-to-q part of the characteristic polynomial of τ.

3. Behavior of $f_{X/K}(x)$ under base change

Let $\mathscr{X}/\mathscr{O}_K$ be a good model of X/K. Fix a prime $q \neq p$. Let K_q/K denote the unique extension of K of degree q. In order to prove Proposition 2.6 and Proposition 2.12, we need to recall how to obtain a good model $\mathscr{Z}/\mathscr{O}_{K_q}$ of X_{K_q}/K_q from a good model of X/K. The assumption that the extension K_q/K is tame is essential in this section.

Let $\mathscr{Y}/\mathscr{O}_{K_q}$ denote the normalization of the scheme

$$\mathscr{X} \times_{\mathrm{Spec}(\mathscr{O}_K)} \mathrm{Spec}(\mathscr{O}_{K_q}).$$

Let $\pi : \mathscr{Y} \to \mathscr{X}$ denote the composition of the natural maps

$$\mathscr{Y} \to \mathscr{X} \times_{\mathrm{Spec}\,(\mathcal{O}_K)} \mathrm{Spec}\,(\mathcal{O}_{K_q}) \to \mathscr{X}.$$

Let

$$p : \mathscr{Z} \to \mathscr{Y}$$

denote the minimal desingularization of $\mathscr{Y}$. To recall the descriptions of the maps p and π, we need the following definition. Let $\mathscr{X}/\mathcal{O}_K$ be any regular model of X/K. Let $C_1, \ldots, C_m$ be irreducible components of the special fiber $\mathscr{X}_k$. The divisor

$$C = \sum_{i=1}^{m} C_i$$

is said to be a *Hirzebruch–Young string* if:

- $g(C_i) = 0 \quad \forall i = 1, \ldots, m.$
- $(C_i \cdot C_i) \leq -2 \quad \forall i = 1, \ldots, m.$
- $(C_i \cdot C_j) = 1 \quad \text{if } |i-j| = 1.$
- $(C_i \cdot C_j) = 0 \quad \text{if } |i-j| > 1.$

We state the following well known facts without proof (see for instance [BPV], Theorem 5.2, when $\mathscr{X}/\mathbf{C}$ is a surface).

Facts 3.1. Let $\mathscr{X}/\mathcal{O}_K$ be a good model of X/K and q be a prime, $q \neq p$.

- The map $\pi : \mathscr{Y} \to \mathscr{X}$ is ramified over the divisor

  $$R := \sum_{\gcd(q, r_i) = 1} C_i.$$

  In particular, $R \subset \mathscr{X}$ has normal crossings. A point $P \in \mathscr{Y}$ is singular if and only if $\pi(P)$ is a singular point of R.
- If $P \in \mathscr{Y}$ is a singular point, then the divisor $p^{-1}(P) := \Sigma_{i=1}^{m(P)} E_i$ is a Hirzebruch–Young string. Let $P \in D_i \cap D_j$, where D_i and D_j are irreducible components of $\mathscr{Y}_k$. Write $\tilde{D}_i$ for the strict transform of D_i in $\mathscr{Z}$. Then:

  $$(p^{-1}(P) \cdot \tilde{D}_i) = (E_1 \cdot \tilde{D}_i) = 1 = (E_{m(P)} \cdot \tilde{D}_j) = (p^{-1}(P) \cdot \tilde{D}_j).$$

  Moreover, if D is an irreducible component of $\mathscr{Z}_k$ and $D \neq \tilde{D}_i$ or $\tilde{D}_j$, then

  $$(p^{-1}(P) \cdot D) = 0.$$

Using the facts recalled in 3.1, one easily proves the following proposition. The integer $\lambda_{\mathscr{X}/\mathscr{O}_{K_q}}$ is defined as in 2.11.

PROPOSITION 3.2. *If $\mathscr{X}/\mathscr{O}_K$ is a good model for X/K, then $\mathscr{X}/\mathscr{O}_{K_q}$ is a good model for X_{K_q}/K_q. Moreover, the following invariants attached to $\mathscr{X}$ can be computed on $\mathscr{Y}$:*

(i) $\alpha(\mathscr{X}) = \alpha(\mathscr{Y})$ *and* $\beta(\mathscr{X}) = \beta(\mathscr{Y})$,

(ii) $f_{\mathscr{X}/\mathscr{O}_{K_q}}(x) = f_{X_{K_q}/K_q}(x) = f_{\mathscr{Y}/\mathscr{O}_{K_q}}(x)$, *and*

(iii) $\lambda_{\mathscr{X}/\mathscr{O}_{K_q}} = \lambda_{\mathscr{Y}/\mathscr{O}_{K_q}}$.

Facts 3.3. Let $\mathscr{X}/\mathscr{O}_K$ be a good model of X/K and let $q \neq p$ be a prime. Let C_i be any component of $\mathscr{X}_k$ having multiplicity r_i and degree d_i. Let $b(C_i) = b_i$ denote the number of components C_j adjacent to C_i, and such that $\gcd(r_i, r_j)$ is prime to q.

- Assume that $q \nmid r_i$. Then $D_i := \pi^{-1}(C_i)$ is irreducible and the restricted map

  $$\pi_{|D_i} : D_i \to C_i$$

  is an isomorphism. The multiplicity of D_i in $\mathscr{Y}$ is equal to r_i. The degree of D_i in $G(\mathscr{Y})$ is equal to $d_i = d(C_i)$.
- Assume that $q \mid r_i$ and $b_i > 0$. Then $D_i := \pi^{-1}(C)$ is irreducible. The restricted map

  $$\pi_{|D_i} : D_i \to C_i$$

  has degree q and is ramified over b_i points of C_i. The degree of D_i in $G(\mathscr{Y})$ is equal to $b_i + q(d_i - b_i)$. The genus $g(D_i)$ of D_i is given by the formula

  $$2g(D_i) = 2g(C_i) \cdot q + (q-1)(b_i - 2),$$

  obtained using the Riemann–Hurwitz formula. The curve D_i has multiplicity r_i/q in $\mathscr{Y}$.
- Assume that $q \mid r_i$ and $b_i = 0$. Then either $D_i := \pi^{-1}(C_i)$ is irreducible and

  $$\pi_{|D_i} : D_i \to C_i$$

  is an étale map, or else $\pi^{-1}(C_i)$ is equal to the disjoint union of q curves D_j and each restricted map

  $$\pi_{|D_j} : D_j \to C_i$$

is an isomorphism. In either case, each irreducible component of $\pi^{-1}(C_i)$ has multiplicity r_i/q in $\mathcal{Y}_k$.

The following lemmas follow immediately from the facts recalled above.

LEMMA 3.4. *If q divides r_i, then*

$$\sum_{D_j \subseteq \pi^{-1}(C_i)} (2g(D_j) + d(D_j) - 2) = q(2g(C_i) + d(C_i) - 2).$$

LEMMA 3.5. *Let D_j be an irreducible component of $\pi^{-1}(C_i)$. If $g(C_i) = 0$ and $d(C_i) \leq 2$, then $g(D_j) = 0$ and $d(D_j) = d(C_i)$.*

Remark 3.6. The integer $(2g(C_i) + d(C_i) - 2)$ is equal to the "topological" Euler–Poincaré characteristic $\mathrm{EP}(C_i')$ of the open curve

$$C_i' := C_i \backslash (C_i \cap \overline{\mathcal{X}_k \backslash C_i}).$$

Let

$$D_i' := \pi^{-1}(C_i) \backslash (\pi^{-1}(C_i) \cap \overline{\mathcal{Y}_k \backslash \pi^{-1}(C_i)}).$$

Since the restricted map $\pi : D_i' \to C_i'$ is étale of degree q prime to p, Lemma 3.4 simply states that

$$\mathrm{EP}(D_i') = q\ \mathrm{EP}(C_i').$$

Proof of Proposition 2.6. We want to prove that

$$\Gamma_q(f_{X/K}(x)) = f_{X_{K_q}/K_q}(x).$$

Let us first check that the multiplicity of the factor $(x-1)$ is the same in both polynomials. We keep the notations introduced in 3.3. It follows from the definitions of Γ_q and of $f_{X/K}(x)$ that

$$\mathrm{ord}_{(x-1)}(\Gamma_q(f_{X/K}(x))) = 2\alpha(X) + 2\beta(X) + \sum_{q \mid r_i} (q-1)(2g(C_i) + d_i - 2).$$

It follows from the definition of $f_{X_{K_q}/K_q}(x)$ that

$$\mathrm{ord}_{(x-1)}(f_{X_{K_q}/K_q}(x)) = 2\alpha(X_{K_q}) + 2\beta(X_{K_q}).$$

Recall that Part (i) of Proposition 3.2 shows that $\alpha(X_{K_q}) = \alpha(\mathcal{Y})$ and $\beta(X_{K_q}) = \beta(\mathcal{Y})$. Recall also the following formula for the Betti number of a graph G:

$$2\beta(G) - 2 = \sum_{i=1}^{n} (d(C_i) - 2).$$

Therefore,

$$2\alpha(X_{K_q}) + (2\beta(X_{K_q}) - 2) = \sum_{D_j \subseteq \pi^{-1}(C_i)} 2g(D_j) + d(D_j) - 2.$$

It follows immediately from Lemma 3.4 that

$$2\alpha(X_{K_q}) + 2\beta(X_{K_q}) - 2 = 2\alpha(X) + 2\beta(X) - 2 + \sum_{q \mid r_i} (q-1)(2g(C_i) + d_i - 2).$$

Hence,

$$\mathrm{ord}_{(x^r-1)}(f_{X_{K_q}/K_q}(x)) = \mathrm{ord}_{(x^r-1)}(\Gamma_q(f_{X/K}(x))).$$

Let $d > 1$ be any integer. To finish the proof of Proposition 2.6, we need to show that

$$\mathrm{ord}_{\Phi_d(x)}(\Gamma_q(f_{X/K}(x))) = \mathrm{ord}_{\Phi_d(x)}(f_{X_{K_q}/K_q}(x)).$$

Let us first state a lemma.

LEMMA 3.7. *Let q be prime, and let d and r be any integers. Then*

$$\mathrm{ord}_{\Phi_d(x)}(\Gamma_q(x^r - 1)) = \begin{cases} 0 & \text{if and only if } d \nmid r \text{ or } q \mid d \mid r,\ dq \nmid r. \\ 1 & \text{if and only if } d \mid r,\ q \nmid r. \\ q & \text{if and only if } dq \mid r. \end{cases}$$

Proof. The first two cases are obvious and we leave them to the reader. With regard to the third case, let us note that if $dq \mid r$, then $\Phi_d \cdot \Phi_{dq}$ divides $(x^r - 1)$. Therefore, when $q^2 \mid dq$, then $\Gamma_q(\Phi_{dq}) = (\Phi_d)^q$ and when $q \nmid d$, then $\Gamma_q(\Phi_d \cdot \Phi_{dq}) = \Phi_d(\Phi_d)^{q-1}$. □

Using the above lemma and the definition of $f_{X/K}(x)$, we can write:

$$\mathrm{ord}_{\Phi_d(x)}(\Gamma_q(f_{X/K}(x))) = \sum_{\substack{d \mid r_i \\ q \nmid r_i}} (2g(C_i) + d(C_i) - 2) + \sum_{dq \mid r_i} q(2g(C_i) + d(C_i) - 2).$$

On the other hand,

$$\operatorname{ord}_{\Phi_d(x)}(f_{X_{K_q}/K_q}(x)) = \sum_{\substack{D_j \subseteq \pi^{-1}(C_i) \\ d \mid r_i,\ q \nmid r_i}} (2g(D_j) + d(D_j) - 2) + \sum_{\substack{D_j \subseteq \pi^{-1}(C_i) \\ dq \mid r_i}} (2g(D_j) + d(D_j) - 2).$$

It is then easy to check, using the facts recalled in 3.3 and Lemma 3.4, that

$$\operatorname{ord}_{\Phi_d(x)}(\Gamma_q(f_{X/K}(x))) = \operatorname{ord}_{\Phi_d(x)}(f_{X_{K_q}/K_q}(x)).$$

This concludes the proof of Proposition 2.6. □

Proof of Proposition 2.12. Let q be a prime, $q \neq p$. Part (i) of Proposition 2.12 states that $\lambda(X_{K_q}/K_q)$ divides $\lambda(X/K)$ and that, if q divides $\lambda(X/K)$, then $\lambda(X_{K_q}/K_q)$ divides $q^{-1}\lambda(X/K)$. Choose a good model $\mathscr{X}/\mathscr{O}_K$ of X/K such that

$$\lambda_{\mathscr{X}/\mathscr{O}_K} = \lambda(X/K).$$

Let $\mathscr{Y}$ denote the normalization of $\mathscr{X} \times_{\operatorname{Spec}(\mathscr{O}_K)} \operatorname{Spec}(\mathscr{O}_{K_q})$ and let $\mathscr{Z}$ denote the minimal desingularization of $\mathscr{Y}$. Proposition 3.2 shows that

$$\lambda_{\mathscr{X}/\mathscr{O}_{K_q}} = \lambda_{\mathscr{Y}/\mathscr{O}_{K_q}}.$$

Therefore, in order to prove Part (i) of Proposition 2.12, we need only to show that

$\lambda_{\mathscr{Y}/\mathscr{O}_{K_q}}$ divides $\lambda_{\mathscr{X}/\mathscr{O}_K}$

and that

$\lambda_{\mathscr{Y}/\mathscr{O}_{K_q}}$ divides $q^{-1}\lambda_{\mathscr{X}/\mathscr{O}_K}$ if q divides $\lambda_{\mathscr{X}/\mathscr{O}_K}$.

These two facts follow immediately from the facts recalled in 3.3 and from Lemma 3.5.

Part (ii) of Proposition 2.12 states that, if $\lambda(X/K) = 1$, then $\alpha(X_{K_d}/K_d) = \alpha(X/K)$ and $\beta(X_{K_d}/K_d) = \beta(X/K)$. Choose a good model $\mathscr{X}/\mathscr{O}_K$ of X/K such that $\lambda(X/K) = \lambda_{\mathscr{X}/\mathscr{O}_K} = 1$. Let q be a prime. Proposition 3.2 shows that

$$\alpha(X_{K_q}/K_q) = \alpha(\mathscr{Z}/\mathscr{O}_{K_q}) = \alpha(\mathscr{Y}/\mathscr{O}_{K_q}),$$

and that

$$\beta(X_{K_q}/K_q) = \beta(\mathscr{X}/\mathscr{O}_{K_q}) = \beta(\mathscr{Y}/\mathscr{O}_{K_q}).$$

Let us now show that $\alpha(\mathscr{Y}/\mathscr{O}_{K_q}) = \alpha(\mathscr{X}/\mathscr{O}_K)$. Let C_i be a component of $\mathscr{X}$. If $d(C_i) > 2$ or $g(C_i) > 0$, then, by hypothesis, $r_i^{(p)} = 1$. Therefore, C_i is in the ramification locus of

$$\pi : \mathscr{Y} \to \mathscr{X}.$$

Hence, $\pi^{-1}(C_i) =: D_i$ is irreducible and

$$\pi_{|D_i} : D_i \to C_i$$

is an isomorphism. In particular, $g(D_i) = g(C_i)$. If $d(C_i) \leq 2$ and $g(C_i) = 0$, then Lemma 3.5 implies that

$$g(D_j) = 0 \quad \text{if } D_j \in \pi^{-1}(C_i).$$

Therefore, $\alpha(\mathscr{X}) = \alpha(\mathscr{Y})$. To show that $\beta(\mathscr{Y}/\mathscr{O}_{K_q}) = \beta(\mathscr{X}/\mathscr{O}_K)$, let us first recall that

$$2\beta(\mathscr{X}) - 2 = \sum_{i=1}^{n} (d(C_i) - 2) = \sum_{q \mid r_i} (d(C_i) - 2) + \sum_{q \nmid r_i} (d(C_i) - 2).$$

We claim that if q divides r_i, then $d(C_i) = 2$ and $g(C_i) = 0$. Certainly we must have $g(C_i) = 0$ and $d(C_i) \leq 2$ since $\lambda_{\mathscr{X}/\mathscr{O}_K} = 1$. Let us assume, ab absurdo, that C_i is such that q divides r_i and $d(C_i) = 1$. Recall that a vertex C of G is called a node if $d(C) > 2$. Since $\gcd(r_1, \ldots, r_n) = 1$, the existence of C_i with $q \mid r_i$ implies the existence of a node in G. It is then easy to check that q must divide the multiplicity of the node C of G closest to C_i (we assume that an edge of G has unit length). This is a contradiction since our assumption $\lambda_{\mathscr{X}/\mathscr{O}_K} = 1$ implies that all nodes have multiplicity prime to q. Therefore, $d(C_i) = 2$ if q divides r_i. Hence, the above formula for $\beta(\mathscr{X})$ simplifies and reads:

$$2\beta(\mathscr{X}) - 2 = \sum_{q \nmid r_i} (d(C_i) - 2).$$

We can compute $2\beta(\mathscr{Y}) - 2$ in the same way:

$$2\beta(\mathscr{Y}) - 2 = \sum_{D_j \in \pi^{-1}(C_i),\ q \nmid r_i} (d(D_j) - 2) + \sum_{D_j \in \pi^{-1}(C_i),\ q \mid r_i} (d(D_j) - 2).$$

As we have shown above, if q divides r_i, then $g(C_i) = 0$ and $d(C_i) = 2$. Therefore, we can apply Lemma 3.5 to C_i and conclude that $d(D_j) = 2$ if $D_j \in \pi^{-1}(C_i)$. Hence,

$$2\beta(\mathscr{Y}) - 2 = \sum_{D_j \in \pi^{-1}(C_i),\ q \nmid r_i} (d(D_j) - 2) = \sum_{q \nmid r_i} (d(C_i) - 2) = 2\beta(\mathscr{X}) - 2.$$

This concludes the proof of Proposition 2.12. □

4. The characteristic polynomial of an automorphism

Let σ be an automorphism of order r of a compact Riemann surface X of genus $g(X)$. Let Y denote the quotient of X by the cyclic group $\langle \sigma \rangle$ generated by σ. Let

$$\pi : X \to Y$$

denote the quotient map and let $B \subset Y$ denote the branch locus of π. The Riemann–Hurwitz formula applied to π reads:

$$2g(X) - 2 = r(2g(Y) - 2) + \sum_{P \in B} |\pi^{-1}(P)|(r/|\pi^{-1}(P)| - 1).$$

To motivate our next theorem, let us rewrite this formula in the following form:

$$2g(X) = 2g(Y) + (2g(Y) + |B| - 2)(r - 1) - \sum_{P \in B} (|\pi^{-1}(P)| - 1).$$

Let

$$f_\sigma(x) := (x - 1)^{2g(Y)} \cdot \left(\frac{x^r - 1}{x - 1}\right)^{2g(Y) + |B| - 2} \cdot \prod_{P \in B} \left(\frac{x^{|\pi^{-1}(P)|} - 1}{x - 1}\right)^{-1}.$$

THEOREM 4.1. *Let X be a compact Riemann surface and let σ be an automorphism of order r. Assume that* $\gcd(|\pi^{-1}(P)|, P \in B) = 1$. *Then the rational function $f_\sigma(x)$ is a polynomial of degree $2g(X)$ and this polynomial is equal to the characteristic polynomial* $\mathrm{char}(\sigma)(x)$ *of σ acting on $H_1(X, \mathbf{Z})$.*

Remark 4.2. Much has been written on automorphisms of curves. This theorem may well follow from the Lefshetz trace formula. We did not, however, find it stated in the literature. Our proof is a variation of the proof of Theorem 2.1. It uses

little more than the Riemann–Hurwitz formula. Note that the assumption $\gcd(|\pi^{-1}(P)|, P \in B) = 1$ holds when σ has a fixed point.

LEMMA 4.3. *Assume that* $\gcd(|\pi^{-1}(P)|, P \in B) = 1$. *Then the rational function* $f_\sigma(x)$ *is a polynomial of degree* $2g(X)$.

Proof. Our lemma will follow from Theorem 3.1 in [Lor]. To be able to apply Theorem 3.1, we need to associate an arithmetical graph G to the integers r and $|\pi^{-1}(P)|$, $P \in B$. We proceed as follows. Let R be the ramification locus of π and fix $\xi \in X \backslash R$. Let $\eta = \pi(\xi)$. Then

$$\pi : X \backslash R \to Y \backslash B$$

is étale and we have an exact sequence of fundamental groups

$$0 \to \pi_1(X \backslash R, \xi) \to \pi_1(Y \backslash B, \eta) \xrightarrow{p} \langle \sigma \rangle \to 0.$$

Let $B := \{P_1, \ldots, P_{|B|}\}$ and set $s_i := |\pi^{-1}(P_i)|$. Let μ_i be a "loop around P_i" passing through η, and such that

$$\mu_i^{r/s_i} \text{ can be lifted to } X \backslash R.$$

In particular, there exist $|B|$ integers m_i, with the property that $\gcd(m_i, r/s_i) = 1$, and such that

$$p(\mu_i) = \sigma^{s_i m_i}.$$

The path $\mu_1 \cdots \mu_{|B|}$ is equal to a product of commutators in $\pi_1(Y \backslash B, \eta)$. Therefore, its image in the abelian group $\langle \sigma \rangle$ is trivial:

$$p(\mu_1 \cdots \mu_{|B|}) = \mathrm{id} = \sigma^{\sum s_i m_i}.$$

In particular,

$$r \text{ divides } \sum s_i m_i.$$

Let $r_i := s_i m_i$, with $\gcd(r, r_i) = s_i$. For each pair (r, r_i), we can construct a terminal chain T_i of an arithmetical graph using Euclid's algorithm as in 2.4 of [Lor]. The terminal vertex on the terminal chain T_i has multiplicity s_i. The graph G needed to

apply Theorem 3.1 of [Lor] is obtained by attaching the terminal chains T_i, $i = 1, \ldots, |B|$, to a single vertex C, given multiplicity r. The "self-intersection" of C in G is then equal to

$$(C \cdot C) = -\left(\sum_{i=1}^{|B|} r_i\right) \Big/ r.$$

Since $\gcd(s_1, \ldots, s_{|B|}) = 1$, we can apply Theorem 3.1 in [Lor] to show that

$$f_G(x) := \left(\frac{x^r - 1}{x - 1}\right)^{|B|-2} \cdot \prod_{i=1}^{|B|} \left(\frac{x^{s_i} - 1}{x - 1}\right)^{-1}$$

is a polynomial. Since

$$f_\sigma(x) = (x-1)^{2g(Y)} \cdot [(x^r - 1)/(x - 1)]^{2g(Y)} \cdot f_G(x),$$

our lemma follows. □

Proof of Theorem 4.1. The proof of Theorem 4.1 is a variation on the proof of Theorem 2.1. We proceed by induction on the integer r. If $r = 1$, our claim is obviously true. Therefore, we may assume by induction that, if d divides r and $d < r$, then

$$f_{\sigma^d}(x) = \mathrm{char}(\sigma^d)(x).$$

Theorem 4.1 will follow from Lemma 2.15 once we have proven Lemma 4.4 and Lemma 4.5 below. Indeed, Lemma 4.4 shows that

$$\mathrm{ord}_{(x-1)}(f_\sigma(x)) = \mathrm{ord}_{(x-1)}(\mathrm{char}(\sigma)(x)).$$

Therefore, to apply Lemma 2.15 to our situation, we need only to know that $\Gamma_q(f_\sigma(x)) = f_{\sigma^q}(x)$. This is the statement of Lemma 4.5.

LEMMA 4.4. *The kernel of the map*

$$\sigma - \mathrm{id} : H_1(X, \mathbf{Z}) \to H_1(X, \mathbf{Z})$$

has rank equal to $2g(Y)$.

Proof. This lemma is certainly well known. It follows for instance from V.2.2.3 in [F–K], where it is shown that the kernel of

$$\sigma - \mathrm{id} : H^0(X, \Omega_X) \to H^0(X, \Omega_X)$$

has dimension $g(Y)$. □

LEMMA 4.5. *Let q be any divisor of r. Then $\Gamma_q(f_\sigma(x)) = f_{\sigma^q}(x)$.*

Proof. The proof is straightforward but rather tedious. We leave it to the reader. □

REFERENCES

[BPV] W. BARTH, C. PETERS, and A. VAN DE VEN, *Compact Complex Surfaces*, Springer Verlag (1984).

[BLR] S. BOSCH, W. LÜTKEBOHMERT, and M. RAYNAUD, *Néron Models*, Springer Verlag, (1990).

[D–M] P. DELIGNE and D. MUMFORD, *The irreducibility of the space of curves of given genus*, Publ. Inst. Hautes Etudes Sci. *36* (1969), 75–109.

[F–K] M. FARKAS and I. KRA, *Riemann Surfaces*, Springer Verlag (1980).

[Gro] A. GROTHENDIECK, *Séminaire de géométrie algébrique* SGA 7, I, Lect. Notes Math. *288*, Springer Verlag (1970).

[L–O] H. LENSTRA and F. OORT, *Abelian varieties having purely additive reduction*, J. Pure and Applied Alg. *36* (1985), 281–298.

[Lor] D. LORENZINI, *Jacobians with potentially good ℓ-reduction*, J. reine angew. Math. *430* (1992), 151–177.

[Mil] J. MILNE, *Abelian varieties*, in Arithmetic Geometry, G. Cornell and J. Silverman, editors, Springer Verlag (1986).

[Ray] M. RAYNAUD, *Spécialisation du foncteur de Picard*, Publ. Inst. Hautes Etudes Sci. *38* (1970), 27–76.

[Sai] T. SAITO, *Vanishing cycles and the geometry of curves over a discrete valuation ring*, Am. J. of Math. *109* (1987), 1043–1085.

[Ste] J. STEENBRINK, *Mixed Hodge structure on the vanishing cohomology*, in the Proceedings of the Nordic Summer School on Real and Complex Singularities, Oslo, August 1976, P. Holm, editor, Sijthoff & Noordhoff International Publishers (1977).

Present address:
Department of Mathematics
University of Georgia
Athens, Georgia 30602

Received March 24, 1992