COMPLEX DYNAMICS AND INVARIANT FORMS MOD p

ALEXANDRU BUIUM

ABSTRACT. Complex dynamical systems on the Riemann sphere do not possess "invariant forms". However there exist non-trivial examples of dynamical systems, defined over number fields, satisfying the property that their reduction modulo $\wp$ possesses "invariant forms" for all but finitely many places $\wp$. The paper completely characterizes the dynamical systems possessing the latter property.

1. MOTIVATION AND STATEMENT OF THE THEOREM

Let k be an algebraically closed field; in our applications k will be either the complex field $\mathbf{C}$ or the algebraic closure of a finite field. Let $k(t)$ be the field of rational functions in the variable t and let $\sigma(t) \in k(t)$ be a non-constant rational function. By an *invariant form of weight* $\nu \in \mathbf{Z}$ for $\sigma(t)$ we mean a rational function $f(t) \in k(t)$ such that

$$(1.1) \qquad f(\sigma(t)) = \left(\frac{d\sigma}{dt}(t)\right)^{-\nu} \cdot f(t).$$

If we consider the $\nu-$tuple differential form $\omega := f(t) \cdot (dt)^{\nu}$ then Equation 1.1 can be written as $\sigma^{*}\omega = \omega$ which is actually what justifies our terminology. We shall sometimes refer to ω itself as being an *invariant form of weight* $\nu \in \mathbf{Z}$.

Our first remark is that if $k = \mathbf{C}$ and σ, viewed as a self map $\mathbf{P}^1 \to \mathbf{P}^1$ of the complex projective line, has degree ≥ 2 then there are no non-zero invariant forms for σ of non-zero weight. Indeed if Equation 1.1 holds for some $f \neq 0$ and $\nu \neq 0$ then the same equation holds with σ replaced by the $n-$th iterate σ^n for any n. Now this equation for the iterates implies that any finite non-parabolic periodic point of σ is either a zero or a pole of f; cf. [14], p. 99 for the definition of parabolic periodic points. On the other hand by [14], pp. 47 and 143, there are infinitely many non-parabolic periodic points, a contradiction.

Although invariant forms don't exist over the complex numbers there exist, nevertheless, interesting examples of complex rational functions with coefficients in number fields whose reduction mod (almost all) primes admit invariant forms. To explain this let $F \subset \mathbf{C}$ be a number field (always assumed of finite degree over the rationals) and let $\wp$ be a place of F (always assumed finite). Let $\mathcal{O}_{\wp}$ denote the valuation ring of $\wp$, let $\kappa_{\wp}$ be the residue field of $\mathcal{O}_{\wp}$ and let $k_{\wp} = \kappa_{\wp}^a$ be an algebraic closure of $\kappa_{\wp}$. Now if $\sigma(t) \in \mathbf{C}(t)$ has coefficients in F then for all except finitely many places $\wp$ of F we may consider the rational function $\bar{\sigma}_{\wp}(t) \in \kappa_{\wp}(t) \subset k_{\wp}(t)$ obtained by writing $\sigma(t) = P(t)/Q(t)$, $P(t), Q(t) \in \mathcal{O}_{\wp}[t]$, with $Q(t)$ primitive, and then reducing the coefficients of $P(t)$ and $Q(t)$ modulo the maximal ideal of $\mathcal{O}_{\wp}$. Below is a list of examples of $\sigma(t)$'s such that $\bar{\sigma}_{\wp}(t)$ has non-zero invariant forms of

non-zero weight for all but finitely many places $\wp$ of F. Our main result will then state that the examples below are *all* possible examples.

Examples 1.1. 1) *Multiplicative functions.* Let $F = \mathbf{Q}$ and let $\sigma(t) = t^{\pm d}$ where d is a positive integer. Then for all prime integers p not dividing d the rational function $\bar{\sigma}_p(t) \in \mathbf{F}_p^a[t]$ possesses a non-zero invariant form of weight $p - 1$,

$$\omega_p = \left(\frac{dt}{t}\right)^{p-1}.$$

2) *Chebyshev polynomials.* Let $F = \mathbf{Q}$ and let $Cheb_d(t) \in \mathbf{C}[t]$ be the Chebyshev polynomial of degree d, i.e. the unique polynomial in $\mathbf{C}[t]$ such that $Cheb_d(t+t^{-1}) = t^d + t^{-d}$. Clearly $Cheb_d$ has integer coefficients. Let $\sigma(t) = \pm Cheb_d(t)$. Then for all odd prime integers p not dividing d the polynomial $\bar{\sigma}_p(t) \in \mathbf{F}_p^a[t]$ possesses a non-zero invariant form of weight $p - 1$,

$$\omega_p = \frac{(dt)^{p-1}}{(t^2 - 4)^{(p-1)/2}}.$$

3) *Lattès functions* [11], [14]. A rational function $\sigma(t) \in \mathbf{C}(t)$, $\sigma : \mathbf{P}^1 \to \mathbf{P}^1$, will be called a *Lattès function* if σ is obtained as follows. One starts with an elliptic curve E over $\mathbf{C}$ with affine plane equation $y^2 = x^3 + ax + b$. One then considers an algebraic group endomorphism $\tau_0 : E \to E$, a non-trivial algebraic group automorphism $\gamma_0 : E \to E$, and a fixed point P_0 of γ_0. Note that γ_0 has order $2, 4, 3$ or 6 and, correspondingly, one has: $\gamma_0(x, y) = (x, -y)$ or $b = 0$, $\gamma_0(x, y) = (-x, iy)$, or $a = 0$, $\gamma_0(x, y) = (\zeta_3 x, y)$, or $a = 0$, $\gamma_0(x, y) = (\zeta_3 x, -y)$. One considers the morphism $\tau : E \to E$, $\tau(P) = \tau_0(P) + P_0$ and one considers the map $\sigma : E/\Gamma \to E/\Gamma$ induced by τ, where $\Gamma := \langle \gamma_0 \rangle$ and E/Γ is identified with $\mathbf{P}^1 = Proj\ \mathbf{C}[x_0, x_1]$ via the isomorphism that sends $t = x_1/x_0$ into x, x^2, y, or y^2 according as $ord(\gamma_0)$ is $2, 4, 3$ or 6. We denote by Lat_d any Lattès function of degree d. The original examples of Lattès, cf. [14], are given by the above construction with $ord(\gamma_0) = 2$.

We claim that if $\sigma(t)$ is a Lattès function with E defined over a number field F then $\bar{\sigma}_\wp(t)$ has a non-zero invariant form of non-zero weight for all but finitely many places $\wp$ of F. Indeed if ω_E is a non-zero global $1-$ form on E defined over F and $e = ord(\gamma_0)$ then $\omega_E^e = \pi^* \omega$ where $\pi : E \to E/\langle \gamma_0 \rangle$ is the canonical projection and $\omega \in F(t) \cdot (dt)^e$. Now

$$\pi^* \sigma^* \omega = \tau^* \pi^* \omega = (\tau^* \omega_E)^e = \lambda \omega_E^e = \pi^* (\lambda \omega)$$

for some $\lambda \in F^\times$. Hence $\sigma^* \omega = \lambda \omega$ hence

$$\bar{\sigma}_\wp^* \bar{\omega}_\wp^{q_\wp - 1} = \bar{\omega}_\wp^{q_\wp - 1}$$

for all but finitely many $\wp$'s, where $\bar{\omega}_\wp$ is the reduction mod $\wp$ of ω and $q_\wp$ is the size of the residue field $\kappa_\wp$.

4) *Flat functions.* It is convenient to introduce terminology that "puts together" all the above Examples. First let us say that two rational functions $\sigma_1, \sigma_2 \in \mathbf{C}(t)$ are *conjugate* if there exists $\varphi \in \mathbf{C}(t)$ of degree 1 such that $\sigma_2 = \varphi \circ \sigma_1 \circ \varphi^{-1}$; if this is the case write $\sigma_1 \sim \sigma_2$. Say that $\sigma(t) \in \mathbf{C}(t)$ is *flat* if either $\sigma(t) \sim t^{\pm d}$ or $\sigma(t) \sim \pm Cheb_d(t)$ or $\sigma(t) \sim Lat_d$. (This is an ad hoc version of terminology from [15].) Flat rational maps naturally appear in a number of contexts; cf Remark 1.5. In the present paper our interest in flat functions comes from the fact that if $\sigma(t) \in \mathbf{C}(t)$ is flat and has coefficients in a number field F then $\bar{\sigma}_\wp(t)$ has a

non-zero invariant form of non-zero weight for all but finitely many places $\wp$ of F. To check this we may write $\sigma = \varphi \circ \sigma_1 \circ \varphi^{-1}$ where $\sigma_1 = t^{\pm d}$ or $\sigma_1 = \pm Cheb_d(t)$ or $\sigma_1 = Lat_d$ and $\varphi \in \mathbf{C}(t)$, $deg(\varphi) = 1$, cf. Examples $1, 2, 3$ above. A standard specialization argument shows that we may replace σ_1 and φ by maps defined over a finite extension F' of F, where, in case $\sigma_1 = Lat_d$, the elliptic curve to which σ_1 is attached is also defined over F'. Then we may conclude by the discussion of the Examples $1, 2, 3$.

The aim of this note is to prove that, conversely, we have the following:

Theorem 1.2. *Assume $\sigma(t) \in \mathbf{C}(t)$ has coefficients in a number field F and has degree $d \geq 2$. Assume that, for infinitely many places $\wp$ of F, $\bar{\sigma}_\wp(t) \in k_\wp(t)$ admits a non-zero invariant form of non-zero weight. Then σ is flat.*

We stress the fact that the form and the weight in the above statement depend a priori on $\wp$.

The proof of the Theorem will be presented in Section 2. The idea is to show that the existence of invariant forms for $\bar{\sigma}_\wp$ implies that $\bar{\sigma}_\wp$ have a "very special type of ramification". This will imply that σ itself has the same type of ramification. Then one concludes by using the topological characterization of postcritically finite rational maps with non-hyperbolic orbifold [6]; the latter is, itself, an easy application of Thurston's orbifold theory.

In the rest of Section 1 we make some Remarks and raise some questions; in particular we indicate the connection between our Theorem and results in [3], [4], [10].

Remark 1.3. Our Theorem suggests, more generally, the problem of characterizing all pairs (σ_1, σ_2) of non-constant morphisms $\sigma_1, \sigma_2 : \tilde{Y} \to Y$ of smooth projective curves over a number field F satisfying the property that:

(*) *For all except finitely many places $\wp$ of F, there exists an integer $\nu_\wp \neq 0$ and a non-zero $\nu_\wp-$tuple form $\omega_\wp \in \Omega^{\otimes \nu_\wp}_{k_\wp(Y)/k_\wp}$ with the property that $\bar{\sigma}^*_{1,\wp}\omega_\wp = \bar{\sigma}^*_{2,\wp}\omega_\wp$.*

Here $k_\wp(Y)$ is the field of rational functions on the reduction of Y mod $\wp$ and $\bar{\sigma}_{i,\wp}$ are the induced morphisms mod $\wp$ (with respect to some model of σ_i over a ring of $S-$integers of F, S a finite set of places of F). The only interesting case of this problem is, of course, that in which the smallest equivalence relation in $Y \times Y$ containing the image of

$$\sigma_1 \times \sigma_2 : \tilde{Y} \to Y \times Y$$

is Zariski dense in $Y \times Y$. The Examples 1.1 fit into the above scheme with $Y = \tilde{Y} = \mathbf{P}^1$ and $\sigma_1 = id$. If one allows, however, both σ_i's to be different from the identity then there are interesting additional examples of pairs (σ_1, σ_2) satisfying property (*). A series of such examples originates in the work of [10]: the curves Y and $\tilde{Y}$ are in this case modular or Shimura curves and the forms $\omega_\wp$ correspond to "Hasse invariants at $\wp$" viewed as appropriate modular forms mod $\wp$. Other, more elementary, examples of pairs (σ_1, σ_2) satisfying property (*) can be produced by taking, for instance, $Y = \tilde{Y} = \mathbf{P}^1$ and $\sigma_2 = \sigma_1 \circ \tau$ where $\sigma_1 : \mathbf{P}^1 \to \mathbf{P}^1$ is a Galois cover and τ is an automorphism of $\mathbf{P}^1$. One can wonder if these examples, together with the Examples 1.1 are (essentially) the only examples for which (*) is satisfied. Cf. also [2] for a measure theoretic analogue.

Remark 1.4. Let us say that a ν−tuple form $\omega \in k(t)(dt)^{\nu}$ of weight ν is *semi-invariant* for σ if $\sigma^*\omega = \lambda\omega$ for some $\lambda \in k^{\times}$. One can show that $\sigma(t) \in \mathbf{C}(t)$ is flat if and only if there exists a non-zero form $\omega \in \mathbf{C}(t) \cdot (dt)^{\nu}$ of weight $\nu \neq 0$ which is *semi-invariant* for σ. (For the "only if" part one can use the arguments in the discussion of the Examples 1.1; the "if" part follows, for instance, from Lemmas 2.6, 2.7 and Proposition 2.1 below.) So our Theorem implies, in particular, the following statement:

(**) *If $\sigma \in \mathbf{C}(t)$ has coefficients in a number field and $\bar{\sigma}_{\wp}(t)$ possesses a non-zero invariant form of non-zero weight for infinitely many places $\wp$ then $\sigma(t)$ itself possesses a non-zero semi-invariant form of non-zero weight.*

On the other hand (**) fails in the context of correspondences! Indeed if $\sigma_1, \sigma_2 : \tilde{Y} \to Y$ define a Hecke correspondence between modular curves over the complex numbers it generally happens that condition (*) in the preceding Remark holds but, nevertheless, there is no non-zero *semi-invariant* form of non-zero weight for this correspondence in characteristic zero i.e. no non-zero ν−tuple form $\omega \in \Omega^{\otimes\nu}_{\mathbf{C}(Y)/\mathbf{C}}$, $\nu \neq 0$, with the property that $\sigma_2^*\omega = \lambda \cdot \sigma_1^*\omega$ for some $\lambda \in \mathbf{C}^{\times}$.

Remark 1.5. Flat rational maps naturally appear in a number of (a priori unrelated) contexts such as: dynamical systems with smooth Julia sets [14], pp 67-70, orbifold theory [6], [14], density conjecture for hyperbolic rational maps [12], isospectral deformations of rational maps [13], permutable rational maps [16], measure theory related to rational maps [18], and Galois theory of function fields related to "Shur's conjecture" [7], [8]. Cf. also [15] for an overview of some of these topics.

The result of the present paper is closely related (and can be applied to) the theory developed in [4], [3], [5]. That theory implies the existence of what one can call "invariant δ−*forms*" for flat functions [4] and for Hecke correspondences on modular and Shimura curves [3]. These invariant δ−forms are objects in characteristic zero but transcending usual algebraic geometry (because they involve not only the coordinates of the points but also their iterated "Fermat quotients" up to a certain "order"). It turns out that the presence of invariant δ−forms implies the presence of invariant forms mod p (in the sense of the present paper); this allows one to prove "converse theorems" along the lines of the "main questions" raised in [4]. Explaining this application would require reviewing the δ−geometric context of the above papers. This would go beyond the scope of the present paper and will be discussed elsewhere [5].

2. Proof of the Theorem

For the proof we need some preliminaries. Let k be an algebraically closed field of characteristic $p \geq 0$. For later purposes we will assume $p \neq 2, 3$. We identify the projective line $\mathbf{P}^1$ over k with its set $k \cup \{\infty\}$ of k−points. Let $\sigma \in k(t)$ be a non-constant rational function which we view as a rational function $\sigma : \mathbf{P}^1 \to \mathbf{P}^1$. We denote by $e_{\sigma} : \mathbf{P}^1 \to \mathbf{Z}_{>0}$ the ramification index function: for $B \in \mathbf{P}^1$, $e_{\sigma}(B)$

is the valuation at B, $v_B(\sigma^*t_A)$, of σ^*t_A where t_A is a parameter of the local ring of $\mathbf{P}^1$ at $A = \sigma(B)$. Recall that σ is *tamely ramified* if $e_\sigma(B)$ is not divisible by p for all B. Recall [6] that one defines the *critical locus* Ω_σ and *postcritical locus* P_σ of σ as

$$\Omega_\sigma := \{B \in \mathbf{P}^1 \mid e_\sigma(B) > 1\} \text{ and } P_\sigma := \bigcup_{n \geq 1} \sigma^n(\Omega_\sigma)$$

respectively. For any integer $n \geq 1$ we have $P_\sigma = P_{\sigma^n}$. If σ is separable then Ω_σ is finite; if in addition k is the algebraic closure of a finite field then P_σ is also finite. (However, if $char(k) = 0$, P_σ is generally infinite.)

The function e_σ and the critical locus Ω_σ make sense, of course, in the more general situation when σ is a morphism of non-singular curves over k.

Assume now $\sigma(t) \in k(t)$ has degree ≥ 2; then we define, following [6], [14], a function $\mu_\sigma : \mathbf{P}^1 \to \mathbf{Z}_{>0} \cup \{\infty\}$ by the formula

$$\mu_\sigma(A) := lcm \{e_{\sigma^m}(B) \mid m \geq 1, \ \sigma^m(B) = A\}.$$

Here *lcm* stands for *lowest common multiple* in the multiplicative monoid $\mathbf{Z}_{>0} \cup \{\infty\}$. Clearly $\mu_\sigma(A) = 1$ for $A \notin P_\sigma$ and $\mu_\sigma(A) > 1$ for $A \in P_\sigma$. The function μ_σ can be characterized as being the smallest among all functions $\mu : \mathbf{P}^1 \to \mathbf{Z}_{>0} \cup \{\infty\}$ such that $\mu(A) = 1$ for $A \notin P_\sigma$ and such that $\mu(A)$ is a multiple of $\mu(B) \cdot e_\sigma(B)$ for each $B \in \sigma^{-1}(A)$. One defines the *orbifold* attached to σ as the pair $O_\sigma := (\mathbf{P}^1, \mu_\sigma)$ and one defines the *Euler characteristic* as being the rational number

$$\chi(O_\sigma) := 2 - \sum_{A \in P_\sigma} \left(1 - \frac{1}{\mu_\sigma(A)}\right) \in \mathbf{Q}.$$

Over the complex numbers we have:

Proposition 2.1. [6] *Assume $\sigma(t) \in \mathbf{C}(t)$ has degree ≥ 2, P_σ is finite, and $\chi(O_\sigma) = 0$. Then σ is flat.*

Proof. This follows by combining Proposition 9.2, p. 290, Proposition 9.3, p. 290, and Corollary 2.4, p. 269, in [6]. $\qquad\square$

In what follows we will prove a series of Lemmas. Recall that a $\nu-$tuple form $\omega \in \Omega_{k(X)/k}^{\otimes \nu}$ on a non-singular projective curve X over k is called *semi-invariant* (of weight ν) for an endomorphism $\sigma : X \to X$ if $\sigma^*\omega = \lambda \omega$ for some $\lambda \in k^\times$.

Lemma 2.2. *Assume $\sigma(t) \in k(t)$ is tamely ramified. Let $B \in \mathbf{P}^1$, $A := \sigma(B)$, and let $\omega = f(dt)^\nu$ be a $\nu-$tuple form. Then*

$$(2.1) \qquad\qquad ord_B(\sigma^*\omega) + \nu = e_\sigma(B) \cdot (ord_A(\omega) + \nu).$$

Proof. One may assume

$$\sigma^*t_A = t_B^e + ... \in k[[t_B]], \quad \omega = (t_A^n + ...)(dt_A)^\nu \in k((t_A))(dt_A)^\nu,$$

where $e = e_\sigma(B)$, $n = ord_A(\omega)$. Then one gets

$$\sigma^*\omega = (t_B^{en} + ...)(et_B^{e-1} + ...)^\nu(dt_B)^\nu = (e^\nu t_B^{en+e\nu-\nu} + ...)(dt_B)^\nu,$$

and we are done. $\qquad\square$

Lemma 2.3. *If $\sigma(t) \in k(t)$ is tamely ramified of degree $d \geq 2$ and admits a semi-invariant non-zero form of weight one then $\sigma \sim t^{\pm d}$.*

Here $\sim$ means conjugation by an automorphism of $k(t)$.

Proof. Assume $\sigma^* \omega = \lambda \omega$, $\lambda \in k^\times$. Let S be the support of the divisor (ω). Let $B \notin S$, $A := \sigma(B)$. By Equation 2.1 we have $1 = e_\sigma(B)(ord_A(\omega) + 1)$ hence $e_\sigma(B) = 1$ so $ord_A(\omega) = 0$ so $A \notin S$. This shows that $\sigma^{-1}(S) \subset S$. It follows that the restriction $\sigma_{|S} : S \to S$ is a bijection and $\sigma^*[S] = d[S]$. So there is an integer $N \geq 1$ such that $\sigma_{|S}^N$ is the identity on S. By Equation 2.1 we get

$$ord_A(\omega) + 1 = e_{\sigma^N}(A)(ord_A(\omega) + 1) = d^N(ord_A(\omega) + 1)$$

for all $A \in S$. Hence $ord_A(\omega) = -1$ for all $A \in S$. Since the genus of $\mathbf{P}^1$ is zero, $deg\ (\omega) = -2$. Hence $\sharp S = 2$ so we may assume $S = \{0, \infty\}$. We find that $\sigma^{-1}(\{0, \infty\}) = \{0, \infty\}$ which implies that $\sigma = ct^{\pm d}$ for some $c \in k^\times$ hence $\sigma \sim t^{\pm d}$ and we are done. $\square$

Lemma 2.4. *If $\sigma(t) \in k(t)$ admits a semi-invariant non-zero form of non-zero weight then σ also admits a semi-invariant non-zero form of positive weight not divisible by p.*

Proof. We may assume $p > 0$. Let $\omega = f(dt)^\nu$ be a semi-invariant non-zero form of non-zero weight ν where ν has minimum absolute value. We may assume $\nu > 0$. We claim that ν is not divisible by p. Assume it is and seek a contradiction. If $df = 0$ then $f = g^p$ for some $g \in k(t)$ and then $g(dt)^{\nu/p}$ is semi-invariant, a contradiction. So we may assume $df \neq 0$. Since ω is semi-invariant and ν is divisible by p it follows that $\sigma^* f = u^p f$, where $u = \lambda^{1/p}(d\sigma/dt)^{-\nu/p}$. It follows that

$$\sigma^* \left(\frac{df}{f} \right) = \frac{d(\sigma^* f)}{\sigma^* f} = \frac{d(u^p f)}{u^p f} = \frac{u^p df}{u^p f} = \frac{df}{f}$$

so df/f is invariant of weight $1 < \nu$, a contradiction. $\square$

Let us consider the following construction. Assume $\sigma \in k(t)$ admits a non-zero semi-invariant form $\omega = f(dt)^\nu$ of positive weight ν not divisible by p. We let

$$(2.2) \qquad\qquad\qquad\qquad \pi : X_\omega \to \mathbf{P}^1$$

be the cyclic Galois cover of non-singular projective curves corresponding to the field extension

$$k(t) \subset k(t, f^{1/\nu}).$$

Lemma 2.5. *Assume $\sigma \in k(t)$ admits a non-zero semi-invariant form ω of positive weight ν not divisible by p. There exists a rational $1-$form η on X_ω such that $\pi^* \omega = \eta^\nu$. Moreover $\sigma : \mathbf{P}^1 \to \mathbf{P}^1$ lifts to an endomorphism $\tau : X_\omega \to X_\omega$ admitting η as a semi-invariant form of weight one.*

Proof. Set $\eta := f^{1/\nu} dt$; then clearly $\pi^* \omega = \eta^\nu$. Now extend σ^* to a field embedding, τ^*, of $k(t, f^{1/\nu})$ into an algebraic closure of $k(t)$. If $\sigma^* \omega = \lambda \omega$ then we have

$$(\tau^* f^{1/\nu})^\nu = \sigma^* f = (\lambda^{1/\nu}(d\sigma/dt)^{-1} f^{1/\nu})^\nu$$

for some $\nu-$th power $\lambda^{1/\nu}$ of λ, hence

$$\tau^* f^{1/\nu} = \zeta \lambda^{1/\nu} \left(\frac{d\sigma}{dt} \right)^{-1} f^{1/\nu},$$

for some $\nu-$th root of unity ζ. So τ^* induces an endomorphism of the field $k(t, f^{1/\nu})$ and therefore it comes from an enodomorphism τ of X_ω. Clearly η is a semi-invariant for τ. $\square$

If, in Lemma 2.5, σ has degree ≥ 2 then τ has degree $deg(\tau) = deg(\sigma) \geq 2$ so, by Hurwitz' formula [9], p. 301, X_ω has genus

$$(2.3) \qquad\qquad g(X_\omega) = 0 \;\; or \;\; 1.$$

Consider the Galois group

$$(2.4) \qquad\qquad \Gamma = \langle \gamma \rangle$$

of the cover 2.2. If $g(X_\omega) = 1$ then γ must have a fixed point which we may take as the zero element for an algebraic group structure on X_ω. This being done, and assuming $p \neq 2, 3$, γ has order $2, 3, 4$, or 6. The order 4 can only occur for j−invariant $j = 1728$ while the orders 3 and 6 can only occur if $j = 0$. Cf. [9], p. 321.

Lemma 2.6. *Assume $\sigma : \mathbf{P}^1 \to \mathbf{P}^1$ has degree $d \geq 2$ and admits a non-zero semi-invariant form ω of positive weight not divisible by p. Assume either $p > d$ or $p = 0$. Assume moreover that $g(X_\omega) = 0$. Then $\sharp P_\sigma \leq 3$ and $\chi(O_\sigma) = 0$.*

Proof. Consider the lifting $\tau : X_\omega = \mathbf{P}^1 \to \mathbf{P}^1$ and the form η in Lemma 2.5. Note that τ has the same degree d as σ so it is tamely ramified. By Lemma 2.3 we may assume $\tau(t) = t^{\pm d}$. With π and γ defined in Equations 2.2 and 2.4 note that the equation $\pi \circ \tau = \sigma \circ \pi$ implies that $\tau \circ \gamma = \gamma^s \circ \tau$ for some s. We get equalities of divisors

$$\tau^* \gamma^* 0 + \tau^* \gamma^* \infty = d\gamma^{s*} 0 + d\gamma^{s*} \infty,$$

hence $\{\gamma^{-1}(0), \gamma^{-1}(\infty)\} = \{0, \infty\}$ hence $\gamma(t) = \lambda t$ or $\gamma(t) = \lambda t^{-1}$ for some $\lambda \in k^\times$. If $\gamma(t) = \lambda t$, $n = \sharp \Gamma$, we may assume $\pi(t) = t^n$ so $(t^{\pm d})^n = \sigma(t^n)$ so $\sigma(t) = t^{\pm d}$ hence, trivially, $\sharp P_\sigma = 2$ and $\chi(O_\sigma) = 0$. If $\gamma(t) = \lambda t^{-1}$ then $\gamma^2 = id$ hence we may assume $\pi(t) = t + \lambda t^{-1}$. We must have $\tau \circ \gamma = \gamma \circ \tau$ from which we get $\lambda^{\pm d} = \lambda$. Hence we have a functional equation

$$t^{\pm d} + \lambda^{\pm d} t^{\mp d} = \sigma(t + \lambda t^{-1}).$$

Taking derivatives in this equation one trivially sees that $\sharp P_\sigma = 3$ and $\chi(O_\sigma) = 0$. (By the way, if $c^2 = \lambda$ then $c^{-1}\sigma(ct)$ is, clearly $\pm Cheb_d(t)$.) $\square$

Lemma 2.7. *Assume $\sigma : \mathbf{P}^1 \to \mathbf{P}^1$ has degree $d \geq 2$ and admits a non-zero semi-invariant form ω of positive weight not divisible by p. Assume either $p > d$ or $p = 0$. Assume moreover that $g(X_\omega) = 1$. Then $\sharp P_\sigma \leq 4$ and $\chi(O_\sigma) = 0$.*

Proof. Consider the lifting $\tau : X := X_\omega \to X$ in Lemma 2.5 and let $G = \langle \gamma \rangle$ ($n = \sharp G$) be the Galois group of the covering $\pi : X \to \mathbf{P}^1$ as in the discussion following Equation 2.4. Then τ is étale. Let $S := \pi(\Omega_\tau) = \{A_1, ..., A_s\}$ and $\tilde{A}_i \in \pi^{-1}(A_i)$. An easy analysis of the fixed points of γ shows that the tuple

$$(e_\pi(\tilde{A}_1), ..., e_\pi(\tilde{A}_s))$$

coincides, up to order, with one of the tuples

$$(2.5) \qquad\qquad (2,2,2,2), \; (3,3,3), \; (4,4,2), \; (6,3,2),$$

according as n is $2, 3, 4$ or 6. Note that for any $A \in \mathbf{P}^1$ we have

$$\mu_\sigma(A) = lcm\{\frac{e_\pi(\tilde{A})}{e_\pi(\tilde{B})} \mid \tilde{B} \in X, \; \tilde{A} = \tau^m(\tilde{B}), \; m \geq 1, \; \pi(\tilde{A}) = A\};$$

here we are using the fact that, for $B := \pi(\tilde{B})$, we have

$$(2.6) \qquad e_{\sigma^m}(B) \cdot e_\pi(\tilde{B}) = e_\pi(\tilde{A}) \cdot e_{\tau^m}(\tilde{B}) = e_\pi(\tilde{A}).$$

By the above equation $e_\pi(\tilde{A}) = 1$ imples $e_\pi(\tilde{B}) = 1$ hence $\mu_\sigma(A) = 1$ for all $A \notin S$. Now we claim that

$$(2.7) \qquad \mu_\sigma(A_i) = e_\pi(\tilde{A}_i)$$

for all i. In view of the allowed values for $e_\pi(\tilde{A}_i)$ listed in Equation 2.5 one sees that Equation 2.7 implies $\sharp P_\sigma \leq 4$ and $\chi(O_\sigma) = 0$ which will end our proof.

In order to check Equation 2.7 we need to show that for any i there exists $m \geq 1$ and $\tilde{B} \in X$ such that $\tau^m(\tilde{B}) = \tilde{A}_i$, $e_\pi(\tilde{B}) = 1$. This is, however, clear because

$$\sharp \, \tau^{-m}(\tilde{A}_i) = \sharp \, Ker \, \tau^m \longrightarrow \infty \quad as \quad m \longrightarrow \infty,$$

hence the set $\tau^{-m}(\tilde{A}_i) \backslash \Omega_\sigma$ is non-empty for m sufficiently big. $\qquad \square$

We are ready to prove our Theorem.

Proof. Assume $\bar{\sigma}_\wp$ admits an invariant form of non-zero weight for infinitely many $\wp$'s. By Lemma 2.4, for infinitely many $\wp$'s, $\bar{\sigma}_\wp$ admits a semi-invariant form of positive weight not divisible by the residual characteristic of $\wp$. By Lemmas 2.6 and 2.7

$$\sharp(P_{\bar{\sigma}_\wp}) \leq 4, \quad \chi(O_{\bar{\sigma}_\wp}) = 0$$

for infinitely many $\wp$'s. This immediately implies $\chi(O_\sigma) = 0$ hence, by Proposition 2.1, σ is flat. $\qquad \square$

References

1. A. F. Beardon, *Iteration of Rational Functions*, GTM 132, Springer, 1991.
2. L. Clozel, E. Ullmo, *Correspondences modulaires et mesures invariantes*, Crelle J. 558 (2003), 47-83.
3. A. Buium, *Differential modular forms on Shimura curves*, Composition Math. 139(2003), 197-237.
4. A.Buium, K. Zimmerman, *Differential orbit spaces of discrete dynamical systems*, Crelle J, to appear.
5. A. Buium, *Arithmetic Differential Equations*, Math. Surveys and Monographs, AMS, to appear.
6. A. Douady, J. H. Hubbard, *A proof of Thurston's topological characterization of rational functions*, Acta Math., 171 (1993), 263-297.
7. M. Fried, *On a conjecture of Schur*, Michigan Math. J. 17 (1970), 41-55.
8. R. M. Guralnick, P. Muller, J. Saxl, *The rational function analogue of a question of Schur and exceptionality of permutation representations*, Memoirs A.M.S. 773 (2003).
9. R. Hartshorne, *Algebraic Geometry*, GTM 52, Springer, 1977.
10. Y. Ihara, *On the differentials associated to congruence relations and the Schwarzian equations defining uniformizations*, J. Fac. Sci. Univ. Tokyo, Sec. IA, Vol. 21, No. 3, (1974), 309-332.
11. S. Lattès, *Sur l'iteration des substitutions rationelles et les fonctions de Poincaré*, C.R.Acad. Sci. Paris 16 (1918), 26-28.
12. R. Mané, P. Sad. D. Sullivan, *On the dynamics of rational maps*, Ann. Sci. Ecole Norm. Sup. 16 (1983), 193-217.
13. C. McMullen, *Families of rational maps and iterative root-finding algorithms*, Ann. of Math. 125 (1987), 467-493.
14. J. Milnor, *Dynamics in One Complex Variable*, Vieweg, 1999.
15. J. Milnor, *On Lattès maps*, preprint: www.math.sunysb.edu/jack/PREPRINTS/index.html.
16. J. F. Ritt, *Permutable rational functions*, Trans AMS 25 (1923), 399-448.
17. J. H. Silverman, *Integer points, Diophantine approximation, and iteration of rational maps*, Duke Math. J. 17 (1993), 793-829.

18. A. Zdunick, *Parabolic orbifolds and the dimension of the maximal measure for rational maps,* Invent. Math. 99 (1990), 627-649.

UNIVERSITY OF NEW MEXICO, ALBUQUERQUE, NM 87131
E-mail address: `buium@math.unm.edu`