RAMIFICATION IN ITERATED TOWERS FOR RATIONAL FUNCTIONS

JOHN CULLINAN, FARSHID HAJIR

Abstract. Let $\phi(x)$ be a rational function of degree > 1 defined over a number field K and let $\Phi_n(x,t) = \phi^{(n)}(x) - t \in K(x,t)$ where $\phi^{(n)}(x)$ is the nth iterate of $\phi(x)$. We give a formula for the discriminant of the numerator of $\Phi_n(x,t)$ and show that, if $\phi(x)$ is postcritically finite, for each specialization t_0 of t to K, there exists a finite set S_{t_0} of primes of K such that for all n, the primes dividing the discriminant are contained in S_{t_0}.

1. Introduction

Let K be a number field and fix a rational self-map ϕ of $\mathbf{P}^1$ defined over K. In concrete terms, choosing a coordinate function x on $\mathbf{P}^1$, *i.e.* choosing a generator for the function field of $\mathbf{P}^1$ over K, ϕ is a rational function $\phi(x) = g(x)/h(x)$ where $g(x), h(x) \in K[x]$ have no common roots in $\overline{K}$. We choose and fix an integral model of $\phi(x)$ for the rest of the paper (so $g(x), h(x) \in \mathcal{O}_K[x]$). Let $\phi^{(n)}(x) = \phi \circ \phi^{(n-1)}(x)$ be the nth iterate of $\phi(x)$ and write $\phi^{(n)}(x) = g_n(x)/h_n(x)$ where $g_n(x)$ and $h_n(x)$ are coprime polynomials in $\mathcal{O}_K[x]$. Define $\Phi_n(x,t) := \phi^{(n)}(x) - t$.

The purpose of this paper is to give a formula for the discriminant $\operatorname{disc}_x(g_n(x) - th_n(x))$ thereby generalizing the discriminant formula for polynomials found in [1]. The main number-theoretic consequence is that it gives a bound on the primes which ramify in characteristic-0 function field extensions. The formula also allows for analysis of ramification for all specializations of t to K.

In the special case where ϕ is postcritically finite, *i.e.* if the union of all forward orbits of the critical points of ϕ is a finite set, then the tower of all iterates of ϕ is geometrically finitely ramified, in the sense that only finitely many places of the base are ramified in the tower of ramified coverings by the iterates of ϕ. The arithmetic question which then arises is: if we specialize this tower at some particular value $t = t_0 \in K$, will it also be finitely ramified? We answer this question in the affirmative. Further number-theoretic applications are discussed in the final section of the paper.

Acknowledgements. We would like to thank Rafe Jones for his careful reading of an early draft of the paper and the referee for many helpful suggestions and comments.

2. Background and Setup

We recall a few facts about the discriminant and resultant of polynomials. For a polynomial $P(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$, where K is a number field, we let $\ell(P) = a_n$ be the leading term of P. For $P, Q \in K[x]$, if we factor $Q(x) = \ell(Q)\prod_{j=1}^{\deg Q}(x - \theta_j)$, with $\theta_j \in \overline{K}$, the *resultant* $\operatorname{Res}(P,Q)$ of P and Q is defined as follows:

$$\operatorname{Res}(P,Q) = (-1)^{\deg P \deg Q} \ell(Q)^{\deg P} \prod_{j=1}^{\deg Q} P(\theta_j).$$

It should be noted (though it is not obvious from this definition) that if $P, Q \in \mathcal{O}_K[x]$ then $\operatorname{Res}(P,Q) \in \mathcal{O}_K$. This follows from the definition of the resultant in terms of a determinant involving only the coefficients of the polynomials. See [4, Ch. 2.4] for more details. The following formulas are well-known and will be used

2000 *Mathematics Subject Classification.* 11R99.

Key words and phrases. ramified covering, postcritically finite, arithmetic dynamics.

extensively:

$$\operatorname{Res}(P,Q) = (-1)^{\deg P \deg Q} \operatorname{Res}(Q,P) \tag{1}$$

$$\operatorname{Res}(P,QR) = \operatorname{Res}(P,Q) \cdot \operatorname{Res}(P,R) \tag{2}$$

$$\operatorname{disc}(P) = (-1)^{d(d-1)/2} \ell(P)^{-1} \operatorname{Res}(P,P'), \tag{3}$$

where P' denotes the derivative of P. In addition, we will make use of the following elementary result.

Lemma 1. *Let a, b, c, d be polynomials. Then*

$$\operatorname{Res}(a-bc, d-b) = \left[(-1)^{\deg(d-b)} \ell(d-b)\right]^{(\deg(a-bc)-\deg(a-dc))} \operatorname{Res}(a-dc, d-b).$$

Proof. The lemma says that, up to a simple factor, we may replace d by b in the first argument since, according to the second argument, d "is" b. We compute

$$\begin{aligned}
\operatorname{Res}(a-bc, d-b) &= (-1)^{\deg(a-bc)\deg(d-b)} \ell(d-b)^{\deg(a-bc)} \prod_{d(\theta_j)=b(\theta_j)} (a-bc)(\theta_j) \\
&= (-1)^{\deg(a-bc)\deg(d-b)} \ell(d-b)^{\deg(a-bc)} \prod_{d(\theta_j)=b(\theta_j)} (a-dc)(\theta_j) \\
&= \frac{(-1)^{\deg(a-bc)\deg(d-b)} \ell(d-b)^{\deg(a-bc)} \operatorname{Res}(a-dc, d-b)}{(-1)^{\deg(a-dc)\deg(d-b)} \ell(d-b)^{\deg(a-dc)}} \\
&= (-1)^{[\deg(a-bc)-\deg(a-dc)]\deg(d-b)} \ell(d-b)^{\deg(a-bc)-\deg(a-dc)} \operatorname{Res}(a-dc, d-b) \\
&= \left[(-1)^{\deg(d-b)} \ell(d-b)\right]^{(\deg(a-bc)-\deg(a-dc))} \operatorname{Res}(a-dc, d-b).
\end{aligned}$$

□

Recall that we write $\phi(x) = g(x)/h(x)$ where $g(x), h(x) \in \mathcal{O}_K[x]$ and $\operatorname{Res}(g(x), h(x)) \neq 0$. We now set some notation:

$$\begin{aligned}
g(x) &= \sum_{r=0}^{\delta} a_r x^r, \\
h(x) &= \sum_{s=0}^{\epsilon} b_s x^s, \\
\ell &= \ell_x(g(x) - th(x)), \\
D &= \ell(h(x)g'(x) - g(x)h'(x)),
\end{aligned}$$

and note that $D, \ell \in \mathcal{O}_K$. Let m be the degree (in x) of $g(x) - th(x)$ (we will soon reduce to the case where $m = \delta$) and let q be the degree of $hg' - gh'$.

It may be the case that $g(x)$ has repeated roots, which will complicate our discriminant formulæ below. To prepare for that possibility, we use the $\mathcal{O}_K$-factorization $g(x) = \prod_{j=1}^{T} g_j(x)^{e_j}$ into powers of irreducibles of degree d_j and with leading terms ℓ_j. We introduce a related polynomial that will be used extensively below. Define $P(x)$ by the following:

$$h(x)g'(x) - h'(x)g(x) = \prod_{i=1}^{T} g_i(x)^{e_i - 1} \times \underbrace{\left[h(x) \sum_{j=1}^{T} e_j g_1(x) \cdots g_j'(x) \cdots g_T(x) - h'(x) \prod_{i=1}^{T} g_i(x)\right]}_{P(x)}$$

and set $d = \deg P(x)$ and $L = \ell(P)$.

We will soon restrict attention to a special class of rational functions and so we recall some of the notation of [1] and interpret it in the context of rational functions. Let

$$\mathcal{R}_\phi := \{r \in \overline{K} \ : \ (hg' - gh')(r) = 0\} \text{ and } \mathcal{B}_\phi := \{\phi(r) \ : \ r \in \mathcal{R}_\phi\}$$

be the sets of *ramification points* and *branch points* of ϕ, respectively. In particular, $\mathcal{R}_\phi$ consists of the roots of $h(x)g'(x) - g(x)h'(x)$ counted *without* multiplicity. For any $r \in \mathcal{R}_\phi$, we define m_r to be its multiplicity as a root of $h(x)g'(x) - g(x)h'(x)$ and M_β as the corresponding multiplicity in $\mathcal{B}_\phi$. A rational function ϕ is said to be *postcritically finite* if the forward orbit of the critical points under all iterations is a finite set. In other words, if

$$\mathcal{B}_{\phi^{(n)}} = \mathcal{B}_\phi \cup \phi(\mathcal{B}_\phi) \cup \cdots \cup \phi^{(n-1)}(\mathcal{B}_\phi)$$

is the set of branch points of $\phi^{(n)}$ then ϕ is postcritically finite if $\bigcup_{n=1}^{\infty} \mathcal{B}_{\phi^{(n)}}$ is finite.

Proposition 1. *With all notation as above, we have*

$$\operatorname{disc}_x(g(x) - th(x)) = \pm \frac{\ell^{d+m-q-2} D^m L^{-\delta}}{\ell(h)^{m-\delta}} \left(\prod_{i=1}^{T} t^{e_i-1}\right) \left(\prod_{j=1}^{T} \ell_j^{-d(e_j-1)} \operatorname{Res}(g_j, h)^{e_j-1}\right) \times$$
$$\left(\prod_{j=1}^{T} [\ell_j^{2-\delta_j} \operatorname{disc}(g_j)]^{e_j}\right) \left(\prod_{i=1}^{T} \prod_{\substack{j=1 \\ j\neq i}}^{T} [\ell_i^{-\delta_j} \operatorname{Res}(g_i, g_j)]^{e_i}\right) \left(\prod_{\{\mu\,:\,P(\mu)=0\}} (1 - t/\phi(\mu))\right).$$

Remarks.

(1) When $\operatorname{disc} g \neq 0$ and $\delta > \epsilon$, the formula of Proposition 1 reduces to

$$\operatorname{disc}_x(g(x) - th(x)) = \pm \operatorname{disc}(g) \prod_{\beta \in \mathcal{B}_\phi} (1 - t/\beta)^{M_\beta}.$$

(2) The product $\prod_\mu (1 - t/\phi(\mu)) \in K[t]$ since the roots of $P(x)$ are in the same Galois-orbit.

(3) Another way to view Proposition 1 is that if $f(x)$ and $g(x)$ are coprime polynomials then we give exactly the set of c such that $f(x) - cg(x)$ has no repeated roots; the exceptional set is precisely the set of values of $f(r)/g(r)$ as r runs over the roots of the Wronskian $hg' - gh'$.

Proof of Proposition 1. By definition, $\operatorname{disc}_x(g(x) - th(x)) = \pm\ell^{-1} \operatorname{Res}(g(x) - th(x), g'(x) - th'(x))$. Using the identity (2) above, we can write

$$\begin{aligned}\ell^{-1} \operatorname{Res}(g(x) - th(x), g'(x) - th'(x)) &= \frac{\pm \operatorname{Res}(g(x) - th(x), h(x)g'(x) - th(x)h'(x))}{\ell \operatorname{Res}(g(x) - th(x), h(x))} \\ &= \frac{\pm \operatorname{Res}(h(x)g'(x) - th(x)h'(x), g(x) - th(x))}{\ell\ell(h)^{m-\delta} \operatorname{Res}(g(x), h(x))},\end{aligned}$$

where the last equality follows from switching the inputs of the resultant in the numerator and applying Lemma 1 to the denominator with $a = g$, $b = -h$, $c = -t$, and $d = 0$. Now apply Lemma 1 to the numerator with $a = hg'$, $b = th$, $c = h'$, and $d = g$ to get

$$\begin{aligned}\operatorname{disc}_x(g(x) - th(x)) &= \pm \frac{\ell^{\epsilon+m-q-2}}{\ell(h)^{m-\delta} \operatorname{Res}(g(x), h(x))} \operatorname{Res}(h(x)g'(x) - g(x)h'(x), g(x) - th(x)) \\ &= \pm \frac{\ell^{\epsilon+m-q-2} D^m}{\ell(h)^{m-\delta} \operatorname{Res}(g(x), h(x))} \prod_{r \in \mathcal{R}_\phi} (g(r) - th(r))^{m_r}.\end{aligned}$$

Let $\{\theta_i^{(j)}\}_{i=1}^{d_j}$ be the roots of $g_j(x)$. Note that the roots of $P(x)$ are disjoint from those of the g_j. This allows us to factor

$$\prod_{r \in \mathcal{R}_\phi} (g(r) - th(r))^{m_r} = \prod_{j=1}^{T} \prod_{i=1}^{d_j} (-th(\theta_i^{(j)}))^{e_j-1} \prod_{\{\mu\,:\,P(\mu)=0\}} g(\mu) \prod_{\{\mu\,:\,P(\mu)=0\}} (1 - t/\phi(\mu)),$$

and analyze each product separately. To begin, we have

$$\prod_{j=1}^{T} \prod_{i=1}^{d_j} (-th(\theta_i^{(j)}))^{e_j-1} = \pm \left(\prod_{i=1}^{T} t^{e_i-1}\right) \prod_{j=1}^{T} \ell_j^{-d(e_j-1)} \operatorname{Res}(g_j, h)^{e_j-1}.$$

Next, we evaluate $g(x)$ on the roots of $P(x)$:

$$\begin{aligned}\prod_{\{\theta\ :\ P(\theta)=0\}} g(\theta) &= \pm L^{-\delta}\ell^d \prod_{\{\theta\ :\ g(\theta)=0\}} P(\theta) = \pm L^{-\delta}\ell^d \prod_{j=1}^{T}\prod_{i=1}^{\deg g_j} P(\theta_i^{(j)})^{e_j} \\ &= \pm L^{-\delta}\ell^d \left(\prod_{j=1}^{T}\prod_{i=1}^{\deg g_j} h(\theta_i^{(j)})^{e_j}\right)\left(\prod_{j=1}^{T}\prod_{i=1}^{\deg g_j}\left(e_j g_1(\theta_i^{(j)})\cdots g_j'(\theta_i^{(j)})\cdots g_T(\theta_i^{(j)})\right)^{e_j}\right) \\ &= \pm L^{-\delta}\ell^d\ell^{-\epsilon}\operatorname{Res}(g,h)\left(\prod_{j=1}^{T}[\ell_j^{2-\delta_j}\operatorname{disc}(g_j)]^{e_j}\right)\left(\prod_{i=1}^{T}\prod_{\substack{j=1\\ j\neq i}}^{T}[\ell_i^{-\delta_j}\operatorname{Res}(g_i,g_j)]^{e_i}\right).\end{aligned}$$

Putting together all the constants finishes the proof of the theorem. □

3. Projective Transformations

We wish to obtain a similar formula as in the previous section for the nth iterate $\phi^{(n)}$ of ϕ. To do that, we need to generalize the following quantities from the formula of Proposition 1: $\epsilon, \delta, \ell, m, q, D, \ell(h)$, and $\operatorname{Res}(g, h)$. It turns out that the derivations of the formulas for these generalizations are greatly simplified when $\delta > \epsilon$. Using Möbius transformations we will show that it is always possible to reduce to this case. We start by switching viewpoints to projective coordinates.

Any $s \in \mathbf{P}^1$ can be represented by $[s_1 : s_2]$ uniquely up to scalar multiples. We define

$$D_{1,\phi}([s_1 : s_2]) := \operatorname{disc}_x(s_2 g(x) - s_1 h(x)),$$

where $s_1, s_2 \in \mathcal{O}_K$. The sets of primes that we will describe will depend on this choice and the choice of coordinates for ϕ, but the finiteness of those sets will not be affected. We define $D_{n,\phi}$ similarly for the n^{th} iterate of ϕ. By the factorization properties of discriminants, a different representative of the same finite point (say $[1 : s_1/s_2]$) only contributes a power of s_2 to the discriminant, which has only finitely-many prime divisors in $\mathcal{O}_K$. For a specialization to the point at infinity $[1 : 0]$ our discriminant reduces to that of $h(x)$.

Lemma 2. *Suppose $\phi \in K(x)$ and choose $\tau \in \operatorname{Aut}(\mathbf{P}^1/K)$ to be integral over K. Then (1) $D_{n,\phi}([s_1 : s_2])$ is divisible by finitely many primes as n goes to infinity if and only if the same holds for $D_{n,\phi^\tau}(\tau([s_1 : s_2]))$, and (2) there exists a finite extension K'/K and (K'-integral) $\tau \in \operatorname{Aut}(\mathbf{P}^1/K')$ such that ϕ^τ has the property that $\delta > \epsilon$.*

Proof. In both cases, the choice of integral model of τ will affect the prime divisors of the discriminant, but will not affect the finiteness of those sets. Any automorphism of $\mathbf{P}^1$ can be decomposed into a product of four transformations: two translations, a dilation/rotation, and an inversion. One can check that $D_{n,\phi}$ transforms in the following way under these operations:

$$\begin{aligned} D_{n,\phi^\tau}(\tau([s_1 : s_2])) &= D_{n,\phi}([s_1 : s_2]) \qquad \text{(translation, inversion)}, \\ D_{n,\phi^\tau}(\tau([s_1 : s_2])) &= \lambda^{(\max(\delta,\epsilon))\cdot(\max(\delta,\epsilon)-1)} D_{n,\phi}([s_1 : s_2]) \qquad \text{(dilation/rotation)}, \end{aligned}$$

where for a dilation/rotation, λ is the determinant of the transformation. This proves the first claim. For the second, note that by enlarging the base field K to a finite extension K', we are guaranteed that $\phi(x)$ has a fixed-point defined over K' and $\deg g > \deg h$ is equivalent to ∞ being fixed by $\phi(x)$. Applying an automorphism of $\mathbf{P}^1$ that gives $\deg g > \deg h$ ensures that $\deg g_n > \deg h_n$ for all n. □

This brings up an important point which is crucial when applying our discriminant formula. The discriminant $\operatorname{disc}(g_n(x))$ appears as one of the factors in $\operatorname{disc}(g_n(x) - t h_n(x))$ below and it may be the case that there exists a positive integer N such that $\operatorname{disc}(g_n(x)) \neq 0$ for $1 \leq n \leq N$, but $\operatorname{disc}(g_n(x)) = 0$ for all $n > N$. This happens precisely when 0 is a postcritical value of ϕ (*e.g.* $\phi(x) = x^2 - 1$). This is something that, unlike fixing ∞, may not be able to be fixed by conjugating by a Möbius transformation. In particular, since the number of iterates needed to capture all of the branch points may be quite large, a Möbius transformation may need to be applied many times to "fix" ϕ, and doing so may affect the previous branch points. According to Proposition 1, the multiplicity of 0 as a branch point may be deduced from the power of t dividing the discriminant.

Thanks to Lemma 2, we will now suppose for the rest of the paper that $\phi(x) = g(x)/h(x)$ with $\deg g(x) > \deg h(x)$. In addition, we will focus on affine specializations, since specializing to $[1 : 0]$ reduces to $\operatorname{disc}(-h_n(x))$. For more information on $\operatorname{disc}(h_n(x))$, see below.

4. Iteration of Rational Functions

We begin by recursively defining two sequences of polynomials g_n, h_n such that $\phi^{(n)}(x) = g_n(x)/h_n(x)$. Namely,

$$g_n(x) = \sum_{r=0}^{\delta} a_r g_{n-1}^r(x) h_{n-1}^{\delta-r}(x), \qquad h_n(x) = h_{n-1}^{\delta-\epsilon}(x) \sum_{s=0}^{\epsilon} b_s g_{n-1}^s(x) h_{n-1}^{\epsilon-s}(x). \tag{4}$$

By Proposition 1, the discriminant $\operatorname{disc}_x(g_n(x) - th_n(x))$ is given by the following:

$$\operatorname{disc}_x(g_n(x) - th_n(x)) = \pm \frac{\ell_n^{\epsilon_n+m_n-\delta_n-2} D_n^{\delta_n}}{\ell(h_n)^{\delta_n-q_n} \operatorname{Res}(g_n, h_n)} \prod_{r \in \mathcal{R}_{\phi^{(n)}}} (g_n(r) - th_n(r))^{m_r}, \tag{5}$$

where a term with the subscript 'n' refers to the corresponding quantity for the nth iterate in the formula of Proposition 1.

Remark. It is not obvious that $\operatorname{Res}(g_n, h_n) \neq 0$ since $g_n(x)$ and $h_n(x)$ are defined recursively. See Proposition 2 for a proof that if $\operatorname{Res}(g, h) \neq 0$ then $\operatorname{Res}(g_n, h_n) \neq 0$.

We begin with a Lemma but omit the proof; it is routine algebraic manipulation.

Lemma 3. *Let $\delta > \epsilon$. With all notation as above, we have*

$$\begin{aligned}
\delta_n &= \delta^n \\
\epsilon_n &= \delta^n - (\delta - \epsilon)^n \\
\ell_n &= \ell(g_n) = \ell(g)^{\frac{1-\delta^n}{1-\delta}} \\
q_n &= 2\delta^n - (\delta - \epsilon)^n - 1 \\
\ell(h_n) &= \left(\frac{\ell(g)}{\ell(h)}\right)^{\sum_{k=1}^{n-1} \epsilon_k} \ell(h)^{\frac{1-\delta^n}{1-\delta}} \\
D_n &= \ell(h_n)\ell(g_n)(\delta - \epsilon)^n.
\end{aligned}$$

Proposition 2. *The resultant iterates in the following way:*

$$\operatorname{Res}(g_n, h_n) = \frac{\operatorname{Res}(g, h)^{\delta^{n-1}(1+\delta+\cdots+\delta^{n-1})} \ell(g)^{\delta^{n-1}(1+\delta+\cdots+\delta^{n-1})(\delta-\epsilon)}}{\ell(g_n)^{(\delta-\epsilon)^n(1+\delta+\cdots+\delta^{n-1})}}$$

Before we prove Proposition 2, we recall the definition of the resultant of bivariate polynomials $A(x, y)$ and $B(x, y)$; for more information see [4, Ch. 2.4]. Let

$$\begin{aligned}
A(x, y) &= a_0x^n + \cdots + a_ny^n \\
B(x, y) &= b_0x^m + \cdots + b_my^m
\end{aligned}$$

be homogeneous polynomials. Then the resultant $\underline{\mathrm{Res}}(A, B)$ of A and B is defined to be the determinant of the $(m+n) \times (m+n)$ matrix

$$\underline{\mathrm{Res}}(A, B) = \det \begin{pmatrix} a_0 & a_1 & \cdots & a_n & & & & & \\ & a_0 & a_1 & \cdots & a_n & & & & \\ & & a_0 & a_1 & \cdots & a_n & & & \\ & & & \ddots & & & \ddots & & \\ & & & & a_0 & a_1 & \cdots & a_n & \\ b_0 & b_1 & \cdots & \cdots & b_m & & & & \\ & b_0 & b_1 & \cdots & \cdots & b_m & & & \\ & & b_0 & b_1 & \cdots & \cdots & b_m & & \\ & & & \ddots & & & & \ddots & \\ & & & & b_0 & b_1 & \cdots & \cdots & b_m \end{pmatrix}$$

If $a_0 b_0 \neq 0$, and A and B factor as

$$A = a_0 \prod_{i=1}^{n} (x - \alpha_i y) \text{ and } B = b_0 \prod_{j=1}^{m} (x - \beta_j y),$$

then

$$\underline{\mathrm{Res}}(A, B) = a_0^m b_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j).$$

In particular, if A and B have the same degree and represent the homogenizations of two univariate polynomials a and b (*e.g.* $A(x, y) = y^{\deg a} a(x/y)$), then the resultant of the specializations of A and B at $y = 1$ is exactly the resultant of the univariate polynomials a and b. Moreover, the bivariate resultant transforms under composition in the following way [4, ex. 2.12]: if F and G are homogeneous polynomials of degree D and f and g are homogeneous of degree d, and $A(x, y) = F(f, g)$ and $B(x, y) = G(f, g)$ are their compositions, then

$$\underline{\mathrm{Res}}(A, B) = \underline{\mathrm{Res}}(F, G)^d \cdot \underline{\mathrm{Res}}(f, g)^{D^2}.$$

Proof of Proposition 2. Recall that g and h have different degrees. In particular, if we write their homogenizations $G(x, y)$ and $H(x, y)$ as

$$G(x, y) = y^{\delta} g(x/y) \text{ and } H(x, y) = y^{\delta} h(x/y) := y^{\delta - \epsilon} \widetilde{H}(x, y),$$

then the leading term (in x) of $H(x, y)$ contains non-trivial multiples of y. In order to relate the bivariate resultant to the univariate resultant, we use the factorization $H(x, y) = y^{\delta - \epsilon} \widetilde{H}(x, y)$ together with the definition in terms of the determinant to get

$$\underline{\mathrm{Res}}(G, H) = \ell(G)^{\delta - \epsilon} \, \mathrm{Res}(G, \widetilde{H}).$$

By iterating the result of [4, ex. 2.12] referred to above, we get

$$\underline{\mathrm{Res}}(G_n, H_n) = \underline{\mathrm{Res}}(G, H)^{d^{n-1}(1 + d + \cdots + d^{n-1})}.$$

It follows that $\ell(G_n)^{\delta_n - \epsilon_n} \underline{\mathrm{Res}}(G_n, \widetilde{H_n}) = [\underline{\mathrm{Res}}(G, \widetilde{H}) \ell(G)^{\delta - \epsilon}]^{d^{n-1}(1 + \cdots + d^{n-1})}$. Altogether this gives

$$\underline{\mathrm{Res}}(G_n, \widetilde{H_n}) = \frac{[\underline{\mathrm{Res}}(G, \widetilde{H}) \ell(G)^{\delta - \epsilon}]^{d^{n-1}(1 + \cdots + d^{n-1})}}{\ell(G)^{(\delta - \epsilon)^n (1 + \cdots + d^{n-1})}}.$$

Since $\underline{\mathrm{Res}}(G_n, \widetilde{H}_n) = \mathrm{Res}(g_n, h_n)$, and $\underline{\mathrm{Res}}(G, \widetilde{H}) = \mathrm{Res}(g, h)$, we obtain the desired formula. □

Proposition 2 and Equation (5) give a formula for the *geometric* ramification in the function field extensions given by the $\Phi_n(x, t)$. We now wish to consider the *arithmetic* ramification in the number fields obtained by specializing t to $t_0 \in K$. A consequence of Lemma 3 and Proposition 2 is that if we write

$$\mathrm{disc}_x(g_n(x) - t h_n(x)) = C_n \prod_{r \in \mathcal{R}_{\phi(n)}} (g_n(r) - t h_n(r))^{m_r},$$

then the primes which divide C_n have finitely-many prime divisors as $n \to \infty$. We now provide a key result that will show, under appropriate hypotheses, that the discriminants do indeed have only finitely many prime divisors. It is natural to assume ϕ is postcritically finite, since this is the condition that guarantees $\operatorname{disc}(g_n(x) - th_n(x))$ has only finitely many prime divisors in $K[t]$ as n goes to infinity.

To set up for the next series of Propositions, we factor $g_n(x) = g_{n,1}(x)^{e_1} g_{n,2}(x)^{e_2} \cdots g_{n,R}(x)^{e_R}$ into powers of K-irreducibles. We further define

$$g_n^S(x) = g_{n,1}(x) g_{n,2}(x) \cdots g_{n,R}(x).$$

Using the identity $\operatorname{disc}(AB) = \pm \operatorname{disc}(A) \operatorname{disc}(B) \operatorname{Res}(A, B)^2$ for monic coprime polynomials, one can work out a formula for $\operatorname{disc} g_n^S$. It suffices then to give a formula for $\operatorname{disc} g_n$ when $g_n(x)$ has no repeated roots.

Proposition 3. *With all notation as above, we have*

$$\operatorname{disc} g_n = \pm \ell^{1-\epsilon_{n-1}(\delta^2-\delta)+(1-\delta_{n-1})\delta} \operatorname{disc} g \operatorname{Res}(g_{n-1}, h_{n-1})^{\delta(\delta-1)} \prod_{j=1}^{\delta} \operatorname{disc}(g_{n-1} - \beta_j h_{n-1}).$$

Proof. We leave it to the reader to check the power of ℓ. Factor $g(x)$ over $\overline{K}$ as

$$g(x) = \ell(g) \prod_{j=1}^{\delta} (x - \beta_j).$$

Then, up to a power of ℓ, the discriminant $\operatorname{disc} g_n(x)$ is given by $\prod_{\{\theta\ :\ g_n(\theta)=0\}} g_n{}'(\theta)$. Using the factorization $g_n(x) = \ell \prod_{j=1}^{\delta} (g_{n-1}(x) - \beta_j h_{n-1}(x))$, one sees that the set of roots of g_n is partitioned into δ subsets $\{\theta_i^{(j)}\}_{i=1}^{\delta_{n-1}}$; the fact that these sets are disjoint follows from g_n and h_n having no common roots and that the β_j are distinct. The derivative of $g_n(x)$ is given by

$$g_n'(x) = \ell \sum_{j=1}^{\delta} \left[(g_{n-1}'(x) - \beta_j h_{n-1}'(x)) \prod_{\substack{k=1 \\ k \neq j}}^{\delta} (g_{n-1}(x) - \beta_k h_{n-1}(x)) \right],$$

and so we evaluate $g_n{}'(x)$ on the roots of $g_n(x)$:

$$\begin{aligned} \prod_{\{\theta\ :\ g_n(\theta)=0\}} g_n'(\theta) &= \prod_{j=1}^{\delta} \prod_{i=1}^{\delta_{n-1}} g_n'(\theta_i^{(j)}) \\ &= \ell \left(\prod_{j=1}^{\delta} \prod_{\substack{k=1 \\ k \neq j}}^{\delta} \prod_{i=1}^{\delta_{n-1}} g_{n-1}(\theta_i^{(k)}) - \beta_j h_{n-1}(\theta_i^{(k)}) \right) \left[\prod_{j=1}^{\delta} \prod_{i=1}^{\delta_{n-1}} g_{n-1}'(\theta_i^{(j)}) - \beta_j h_{n-1}(\theta_i^{(j)}) \right]. \end{aligned}$$

The quantity in parentheses is, up to powers of ℓ, simply all the resultants $\operatorname{Res}(g_{n-1} - \beta_j h_{n-1}, g_{n-1} - \beta_k h_{n-1})$ for $j \neq k$. It is easy to check that, up to powers of ℓ, we have

$$\left(\prod_{j=1}^{\delta} \prod_{\substack{k=1 \\ k \neq j}}^{\delta} \prod_{i=1}^{\delta_{n-1}} g_{n-1}(\theta_i^{(k)}) - \beta_j h_{n-1}(\theta_i^{(k)}) \right) = \pm \operatorname{disc} g^S \operatorname{Res}(g_{n-1}, h_{n-1})^{\delta(\delta-1)}.$$

The quantity in brackets is, up to powers of ℓ, the product over all the β_j of $\operatorname{disc}(g_{n-1} - \beta_j h_{n-1})$. This proves the Proposition. □

We now state and prove the main result of the paper.

Theorem 1. *Let $\phi(x) \in K(x)$ be postcritically finite. Choose an integral model $\phi(x) = g(x)/h(x)$ so that $g(x), h(x) \in \mathcal{O}_K[x]$ and $\operatorname{Res}(g(x), h(x)) \neq 0$. If $g_n(x), h_n(x)$ are given by (4), then for each $t_0 \in K$, there exists a finite set S_{t_0} of primes of K such that for all $n \geq 1$, if $\mathfrak{p}$ is a prime of K not in S_{t_0}, then $v_{\mathfrak{p}}(\operatorname{disc}(g_n(x) - t_0 h_n(x))) = 0$.*

Proof. We divide the proof into two cases based on whether the discriminant $\operatorname{disc} g_n = 0$.

Case 1: $\operatorname{disc} g_n(x) \neq 0$ **for all** n

According to the Remark preceeding the proof of Proposition 1, we have

$$\operatorname{disc}_x(g_n(x) - th_n(x)) = \pm \operatorname{disc}(g_n) \prod_{\beta \in \mathcal{B}_{\phi^{(n)}}} (1 - t/\beta)^{M_\beta}.$$

Since ϕ is postcritically finite, there exists an $N \in \mathbf{Z}_{>0}$ such that for all $n \geq N$

$$\prod_{\beta \in \mathcal{B}_{\phi^{(n)}}} (1 - t/\beta)^{M_\beta} = \prod_{\beta \in \mathcal{B}_{\phi^{(N)}}} (1 - t/\beta)^{M_\beta}$$

as K-polynomials. It therefore suffices to focus on $\operatorname{disc} g_n$. By Proposition 3 we have

$$\operatorname{disc} g_n = \pm \ell^{1-\epsilon_{n-1}(\delta^2-\delta)+(1-\delta_{n-1})\delta} \operatorname{disc} g \operatorname{Res}(g_{n-1}, h_{n-1})^{\delta(\delta-1)} \prod_{j=1}^{\delta} \operatorname{disc}(g_{n-1} - \beta_j h_{n-1}),$$

where the β_j are the roots of $g(x)$. By Proposition 2, $\operatorname{Res}(g_{n-1}, h_{n-1})$ is a power of $\operatorname{Res}(g, h)$. We then have

$$\prod_{j=1}^{\delta} \operatorname{disc}(g_{n-1} - \beta_j h_{n-1}) = \pm \operatorname{disc}(g_{n-1})^{\delta} \prod_{j=1}^{\delta} \prod_{\beta \in \mathcal{B}_{\phi^{(n-1)}}} (1 - \beta_j/\beta)^{M_\beta}$$

is simply a product of the discriminants of the type in this Theorem evaluated on the β_j. Since ϕ is postcritically finite, there exists an N (the same N as above suffices) such that for all $n \geq N$, the products

$$\prod_{j=1}^{\delta} \prod_{\beta \in \mathcal{B}_{\phi^{(n-1)}}} (1 - \beta_j/\beta)^{M_\beta} = \prod_{j=1}^{\delta} \prod_{\beta \in \mathcal{B}_{\phi^{(N)}}} (1 - \beta_j/\beta)^{M_\beta}$$

are equal. This finishes the proof in the case where $\operatorname{disc} g_n \neq 0$ for all n.

Case 2: $\operatorname{disc} g_n(x) = 0$ **for some** n

The proof in this case is more complicated, but has the same strategy. The main point is that the coefficients of the product $\prod_{P_n(\mu)=0}(1 - t/\phi^{(n)}(\mu))$ have the same prime divisors for all n sufficiently large and the product itself remains fixed for all n sufficiently large.

We therefore take n large enough such that for all $\nu > n$, we have $\mathcal{B}_{\phi^{(n)}} = \mathcal{B}_{\phi^{(\nu)}}$. We refer to the formula of Proposition 1 and note that the coefficient in front of the initial parentheses iterates as in Lemma 3 and so has only finitely-many prime divisors as $n \to \infty$. Under iteration, the product $\prod_{i=1}^{T} t^{e_i - 1}$ simply contributes more powers of t to the discriminant, and thus does not provide any new prime divisors for a given specialization.

Next, the product $\prod_{j=1}^{T} \ell_j^{-d(e_j-1)} \operatorname{Res}(g_j, h)^{e_j-1}$ can be rewritten as

$$\prod_{j=1}^{T} \ell_j^{-d(e_j-1)} \operatorname{Res}(g_j, h)^{e_j-1} = \frac{\prod_{j=1}^{T} \ell_j^{-d(e_j)} \operatorname{Res}(g_j, h)^{e_j}}{\prod_{j=1}^{T} \ell_j^{-d} \operatorname{Res}(g_j, h)} = \frac{\ell^d \operatorname{Res}(g, h)}{\ell(g^S)^d \operatorname{Res}(g^S, h)}.$$

As $n \to \infty$, the prime divisors of the iterates of $\frac{\ell^d \operatorname{Res}(g,h)}{\ell(g^S)^d \operatorname{Res}(g^S,h)}$ form a finite set (use the fact that $\operatorname{Res}(g^S, h)$ and $\ell(g^S)$ are $\mathcal{O}_K$-divisors of $\operatorname{Res}(g, h)$ and ℓ, respectively).

Finally, the two products

$$\left(\prod_{j=1}^{T} [\ell_j^{2-\delta_j} \operatorname{disc}(g_j)]^{e_j} \right) \left(\prod_{i=1}^{T} \prod_{\substack{j=1 \\ j \neq i}}^{T} [\ell_i^{-\delta_j} \operatorname{Res}(g_i, g_j)]^{e_i} \right)$$

are, up to powers of divisors of ℓ, have exactly the same prime divisors as $\operatorname{disc}(g^S)$ (note that each resultant appears twice, and recursively apply the formula $\operatorname{disc}(AB) = \operatorname{disc}(A) \operatorname{disc}(B) \operatorname{Res}(A, B)^2$). Therefore, it remains to demonstrate that $\operatorname{disc} g_n^S$ has only finitely-many prime divisors as $n \to \infty$. But each irreducible factor of $g_n^S(x)$ is itself a product of factors of the type $g_{n-1} - \beta_j h_{n-1}$, the discriminants of which have already been shown to have finitely-many prime divisors as $n \to \infty$ under the hypothesis that ϕ is postcritically finite. This completes the proof of the Theorem. □

When $\delta - \epsilon > 1$, then $\operatorname{disc} h_n(x) = 0$ for any $h(x)$ once $n > 1$. In this case, a specialization of $D_{n,\phi}([s_1 : s_2])$ to infinity equals zero. When $\delta < \epsilon$, it is the case that $\delta_n = \epsilon_n$ for all $n > 1$ so it suffices to consider $0 \leq \delta - \epsilon \leq 1$. In that case, one can work out an analogous discriminant formula to the one in Proposition 3 to show that $\operatorname{disc} h_n$, if it is non-zero, has finitely-many prime divisors as $n \to \infty$.

5. Applications

The main application of the discriminant formula is the characterization of the primes ramifying in a finite extension of characteristic-0 function fields, and its number field specializations. In particular, it has potential usefulness in computing the different ideal of the extensions. This is complementary to results of Beckmann [2, 3]. There, the author provides a geometric framework in which the number field ramification can be described. For completeness, we briefly remind the reader of those results.

Let $X \longrightarrow \mathbf{P}^1$ be a branched covering of curves over $\mathbf{C}$ that can be defined over a number field K; let $X_K \longrightarrow \mathbf{P}^1_K$ be a model for this covering. Let S_{bad} be the union of the set of finite primes of $\mathcal{O}_K$ that

1. divide the order of the Galois group of the Galois closure of $K(X)$;
2. at which two branch points of $X \longrightarrow \mathbf{P}^1$ meet;
3. divide the discriminant of the polynomial generating the field extension,

where two points $a, b \in K$ *meet at* p if $\operatorname{ord}_p(a-b) > 0$. Further, if we specialize the function field extension at $t = a$, then let S_a be the set of primes at which a meets some branch point. A *good model* is a model for which the primes of $\mathcal{O}_K$ that ramify in $\mathcal{O}[X]$ are contained in S_{bad}.

Theorem. [3, thm. 5.1.1] *Suppose that G [the Galois group of the Galois closure of the cover] has trivial center, or that $X_K \longrightarrow \mathbf{P}^1_K$ is a good model. Let $a \in K$ and assume that $t = a$ is not a branch point of $X \longrightarrow \mathbf{P}^1$. Let $L_1, \ldots, L_m$ be the field extensions of K arising from the specialization of $X_K \longrightarrow \mathbf{P}^1_K$ to $t = a$. Then the finite primes of K that ramify in some L_i are contained in the set $S_{bad} \bigcup S_a$.*

For a concrete family of examples, recall [4, p. 351] that a rational map $\phi : \mathbf{P}^1 \longrightarrow \mathbf{P}^1$ of degree ≥ 2 is called a *Lattès map* if there exists an elliptic curve E, a morphism $\psi : E \longrightarrow E$, and a finite separable covering $\pi : E \longrightarrow \mathbf{P}^1$ such that the following diagram commutes:

$$\begin{tikzcd}
E \arrow[r, "\psi"] \arrow[d, "\pi"] & E \arrow[d, "\pi"] \\
\mathbf{P}^1 \arrow[r, "\phi"] & \mathbf{P}^1
\end{tikzcd}$$

It known [4, Prop. 6.45] that Lattès maps are postcritically finite. In particular, if we fix a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

take $\psi = [m]$ (the multiplication-by-m isogeny), and take π to be the projection onto the x-coordinate, then ϕ is a Lattès map and hence postcritically finite. In particular, $\phi^{(n)}(x) = x([m^n]P)$ is postcritically finite for all n.

Let $P \in E$ and set $\pi(P) = t \in \mathbf{P}^1$. Then the preimage of t under the compositions of π with the $[m^n]$ give rise to ramified coverings of $\mathbf{P}^1$ and hence to ramified extensions of number fields K_n/K:

$$\begin{tikzcd}
\vdots \arrow[d, "\phi"'] & \vdots \arrow[d, dash] \\
\mathbf{P}^1 \arrow[d, "\phi"'] \arrow[dd, bend right=60, "\phi^{(2)}"'] & K_2 \arrow[d, dash] \\
\mathbf{P}^1 \arrow[d, "\phi"'] & K_1 \arrow[d, dash] \\
\mathbf{P}^1 & K
\end{tikzcd}$$

Our formulæ not only show that the field extension $\bigcup_{n=1}^{\infty} K_n$ of K is ramified at a finite number of places, but it also gives an exact formula for the discriminant of all the K_n.

For an explicit example, we choose a Weierstrass equation for E of the form $y^2 = x^3 + ax + b$, with $a, b \in K$. We take $\psi = [2]$ so that

$$\phi(x) = \frac{x^4 - 2ax^2 - 8bx + a^2}{4x^3 + 4ax + 4b}.$$

Therefore, given a point P on E with coordinates (x, y), the rational function $\phi(x)$ gives the x-coordinate of $[2]P$ and so $\phi^{(n)}(x) = x([2^n]P)$. Applying Proposition 1 we get

$$\mathrm{disc}_x(g(x) - th(x)) = \pm 2^{12}(ta + b + t^3)^2(4a^3 + 27b^2).$$

For $n \geq 2$, an explicit formula for the discriminant can be found using the formula of Proposition 2, but the only primes ramifying in the field extension are those which divide $-2^{12}(ta + b + t^3)^2(4a^3 + 27b^2)$. Similarly, if $\Phi = \pi \circ [3]$, then

$$\Phi = \frac{G(x)}{H(x)} := \frac{x^9 - 12ax^7 - 96bx^6 + 30a^2x^5 - 24bax^4 + \left(36a^3 + 48b^2\right)x^3 + 48ba^2x^2 + \left(9a^4 + 96b^2a\right)x + \left(8ba^3 + 64b^3\right)}{9x^8 + 36ax^6 + 72bx^5 + 30a^2x^4 + 144bax^3 + \left(-12a^3 + 144b^2\right)x^2 - 24ba^2x + a^4},$$

and the discriminant $\mathrm{disc}_x(G(x) - tH(x))$ is given by

$$\pm 2^{48} 3^9 (t^3 + at + b)^4 (4a^3 + 27b^2)^{10}.$$

Similar formulas can be obtained for all positive integers m. More generally, given a point P of infinite order on an elliptic curve $E/\mathbf{Q}$ one can study the ramification in the Kummerian fields $\mathbf{Q}(E[m], P)$ via these formulæ in tandem with elliptic Kummer theory.

Finally, we note that in the case of postcritically finite extensions our discriminant formula guarantees finite ramification in the (infinite) tower of number fields. However, it is not clear whether a given non-postcritically-finite tower can be finitely-ramified, since not all primes dividing the discriminant must ramify.

References

[1] W. Aitken, F. Hajir, C. Maire, *Finitely ramified iterated extensions*, Int. Math. Res. Not. **2005**, no. 14, 855–880.

[2] S. Beckmann, *Ramified primes in the field of moduli of branched coverings of curves*, J. Algebra **125** (1989), no. 1, 236–255.

[3] S. Beckmann, *On extensions of number fields obtained by specializing branched coverings*, J. Reine Angew. Math. **419** (1991), 27–53.

[4] J. Silverman, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics, **241**. Springer, New York, 2007.

Department of Mathematics, Bard College, Annandale-On-Hudson, NY 12504
E-mail address: cullinan@bard.edu

Department of Mathematics, University of Massachusetts, Amherst MA 01003
E-mail address: hajir@math.umass.edu