A PROOF OF THE WEIERSTRASS GAP THEOREM NOT USING THE RIEMANN-ROCH FORMULA

PETER PAULE AND CRISTIAN-SILVIU RADU

Dedicated to our good friend George Andrews at the occasion of his 80th birthday.

Abstract. Usually the Weierstrass gap theorem is derived as a straightforward corollary of the Riemann-Roch theorem. Our main objective in this article is to prove the Weierstrass gap theorem by following an alternative approach based on "first principles" and which does not use the Riemann-Roch formula. Having mostly applications in connection with modular functions in mind, we describe our approach for the case when the given compact Riemann surface is fixed to the modular curve $X_0(N)$.

1. Main Objective

Various topical areas in the theory of partitions, like congruences for partition numbers, are connected to modular functions for congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ as, for instance, $\Gamma_0(N)$; see Section 15 for definitions. Such functions live on compact Riemann surfaces, for instance, on $X_0(N)$ for $\Gamma_0(N)$. Number theoretic aspects then relate to properties of certain subalgebras formed by these functions. In cases where the genus of such surfaces is zero like, for instance, for $X_0(5)$ and $X_0(7)$, these algebras essentially have a relatively simple structure. For positive genus g, for example in the case of $X_0(11)$, this changes. One explanation is this: when considering sets of meromorphic functions with poles only at one point p, the Weierstrass gap theorem says that one can obtain functions with all possible pole orders at p with exactly g exceptions:

Theorem 1.1 (Weierstraß gap theorem; e.g., Sect. III.5.3 in [5])**.** *Let X be a compact Riemann surface having genus $g \geq 1$. Then for each $p \in X$ there are precisely g integers $n_j = n_j(p)$ with*

$$1 = n_1 < \cdots < n_g \leq 2g - 1 \tag{1}$$

such that there does not exist a meromorphic function on X which is holomorphic on $X \setminus \{p\}$ and which has a pole of pole order n_j at p.

Date: Updated version of version from January 31, 2019: TYPOS REMOVED.
Both authors were supported by grant SFB F50-06 of the Austrian Science Fund (FWF).
2010 Mathematics Subject Classification: primary 14H55, 11F03; secondary 11P83.
Keywords and phrases: Weierstrass gap theorem, modular functions.

Usually, as in [5], this theorem is derived as a straightforward corollary of the Riemann-Roch theorem. Our main objective in this article is to prove the Weierstrass gap theorem by following an alternative approach based on "first principles" and which does not use the Riemann-Roch formula. Having mostly applications in connection with modular functions in mind, we describe our approach for the case when the given compact Riemann surface X is fixed to $X_0(N)$. Some ingredients of our setting are related to ideas from the celebrated paper [16] by Dedekind and Weber; see [3] for an English translation together with an excellent introduction by John Stillwell.

2. Introduction

To exemplify the usage of Weierstrass's gap theorem we choose an example related to the classical Ramanujan congruences and which in further details is discussed in [13]. Let

$$M(N) := \text{ field of meromorphic modular functions for } \Gamma_0(N).$$

To keep this article as self-contained as possible, we list basic definitions and properties of modular functions in a separate Appendix Section 15.

One standard way to construct modular functions is by eta-quotients; i.e., products of the form

$$\prod_{d|m} \eta(d\tau)^{r_d}, \tau \in \mathbb{H}. \tag{2}$$

Here $\mathbb{H}$ denotes the upper half of the complex plane, $m \in \mathbb{Z}_{>0}$, the r_d are chosen integers, and, η denotes the Dedekind eta function defined as

$$\eta(\tau) = q(\tau/24) \prod_{n=1}^{\infty} (1 - q(\tau)^n) \text{ where } q(\tau) = \exp(2\pi i \tau). \tag{3}$$

Usually one writes q instead of $q(\tau)$.

The case $m = \ell$, $\ell \geq 5$ a prime, gives rise to a simple but important class of eta quotients

$$z_\ell(\tau) := \Big(\frac{\eta(\ell\tau)}{\eta(\tau)}\Big)^{\frac{24}{\gcd(\ell-1,24)}}, \tag{4}$$

which are modular functions in $M(\ell)$ with (e.g., [8, Ch. 7, Thm. 1])

$$\operatorname{ord}_{[\infty]_\ell} z_\ell^* = \frac{\ell - 1}{\gcd(\ell - 1, 12)}. \tag{5}$$

Here the notation z_ℓ^* is explained by the fact that, in general, every modular function $f \in M(N)$ gives rise to an induced meromorphic function $f^* : X_0(N) \to \hat{\mathbb{C}} := \mathbb{C} \cup \{\infty\}$ which for $x = [\tau]_N$ is defined as

$$f^*(x) = f^*([\tau]_N) := f(\tau),\ \tau \in \hat{\mathbb{H}} := \mathbb{H} \cup \mathbb{Q} \cup \{\infty\};$$

see Section 15. There one also finds the definition of $[\tau]_N$ as the orbit of τ under $\Gamma_0(N)$, as well as definitions of basic notions like of $\operatorname{ord}_{[a/c]_N} f^*$, the order of f^* at a cusp $[a/c]_N$, $a/c \in \mathbb{Q} \cup \{\infty\}$. Note that $[\infty]_N = [1/0]_N$.

Example 2.1. [8, Ch. 7, Thm. 1] Consider

$$z_5(\tau) = \Big(\frac{\eta(5\tau)}{\eta(\tau)}\Big)^6 = q\prod_{j=1}^{\infty}\Big(\frac{1-q^{5j}}{1-q^j}\Big)^6 = q + 6q^2 + 27q^3 + 98q^4 + \cdots . \tag{6}$$

We have $\operatorname{ord}_{[\infty]_N} f^* := \operatorname{ord}_q f$, confirming that

$$\operatorname{ord}_{[\infty]_5} z_5^* = \frac{5-1}{\gcd(5-1,12)} = 1 = \operatorname{ord}_q z_5. \tag{7}$$

Because of

$$z_\ell\Big(-\frac{1}{\tau}\Big) z_\ell\Big(\frac{\tau}{\ell}\Big) = \ell^{-\frac{12}{\gcd(\ell-1,12)}},\ \ell \text{ a prime} \geq 5, \tag{8}$$

$$z_5\Big(-\frac{1}{\tau}\Big) = \frac{5^{-3}}{z_5(\tau/5)} = \frac{1}{5^3}\Big(\frac{1}{q^{1/5}} - 6 + 9q^{1/5} + 10q^{2/5} - \dots\Big), \tag{9}$$

which owing to $\operatorname{ord}_{[0]_N} f^* := \operatorname{ord}_{q^{1/N}} f(-1/\tau)$ confirms that

$$\operatorname{ord}_{[0]_5} z_5^* = -\frac{5-1}{\gcd(5-1,12)} = -1 = \operatorname{ord}_{q^{1/5}} z_5\Big(-\frac{1}{\tau}\Big). \tag{10}$$

In general, for ℓ a prime, $X_0(\ell)$ has exactly two cusps $[\infty]_\ell$ and $[0]_\ell$ with widths 1 and ℓ, respectively; see [8, Ch. 2, Sect. 2], resp. Section 15 for the definition of width. The q-series (6) and (9) are the local q-expansions of z_5^* at these cusps.

Being meromorphic, modular functions form fields. For example, a classical fact, e.g., [4, Prop. 7.5.1], is that $M(N) = \mathbb{C}(j(\tau), j(N\tau))$, where j is the modular invariant (Klein j function). The subset

$$M^!(N) := \{f \in M(N) : f^* \text{ has poles only at } [\tau]_N \text{ with } \tau \in \mathbb{Q} \cup \{\infty\}\}$$

obviously is not a field but a $\mathbb{C}$-algebra.[1]

Example 2.2. By definition (6) together with (7) and (10), $z_5 \in M^!(5)$ because z_5^* has its only pole of pole order 1 at $[0]_5$.

[1] A $\mathbb{C}$-algebra is a commutative ring with 1 which is also a vector space over $\mathbb{C}$.

An important $\mathbb{C}$-subalgebra, in particular, with regard to algorithms, is

$$M^\infty(N) := \{f \in M^!(N) : f^* \text{ has poles only at } [\infty]_N\}.$$

By [14, Lemma 20], $M^\infty(N)$ for each $N \geq 1$ contains an eta quotient μ_N of the form as in (2) and such that $\mathrm{ord}_{[a/c]_N} \mu_N^* > 0$ for all $a/c \in \mathbb{Q}$ with $[a/c]_N \neq [\infty]_N$.. Hence one can multiply with a suitable power of μ_N to turn any given $f \in M^!(N)$ into an element $\mu_N^\alpha f$ in $M^\infty(N)$.

Example 2.3. Choose $f(\tau) := j(\tau) \in M^!(N)$, the Klein j function, and α such that $\mu_N^\alpha j \in M^\infty(N)$. Let $\beta := \mathrm{ord}_{[\infty]_N} \mu_N$, then $\mathrm{ord}_{[\infty]_N} \mu_N^\alpha j = \alpha\beta - 1$. In particular,

$$\gcd(\mathrm{ord}_{[\infty]_N} \mu_N, \mathrm{ord}_{[\infty]_N} \mu_N^\alpha j) = 1,$$

which will be needed later. A description of how to construct such μ_N is given in [14].

Since we will prove the gap Theorem 1.1 in the version of Theorem 12.2 where $X = X_0(N)$ and with $p = [\infty]_N$, a key issue in our approach concerns the question of finding appropriate representations of $M^\infty(N)$.

Example 2.4. Owing to (7) and (10), $1/z_5 = \frac{1}{q} - 6 + 9q + \cdots \in M^\infty(5)$. Because of $\mathrm{ord}_{[\infty]_5}(1/z_5)^* = -1$ each $f \in M^\infty(5)$ can be written as a polynomial in $1/z_5$; in short,

$$M^\infty(5) = \mathbb{C}\Big[\frac{1}{z_5}\Big],$$

where $\mathbb{C}[x]$ denotes the ring of polynomials in x with complex coefficients. One also has

$$M^\infty(7) = \mathbb{C}\Big[\frac{1}{z_7}\Big],$$

but already for $\ell = 11$ the situation is quite different. For example, in [13] we proved (implicitly) that $M^\infty(11)$ can be represented as a $\mathbb{C}[1/z_{11}]$-module which is freely generated by modular functions F_2, F_3, F_4, and $F_6 \in M^\infty(11)$. More concretely,

$$\begin{aligned} M^\infty(11) = \big\{&p_0(z_{11}) + p_2(z_{11})F_2 + p_3(z_{11})F_3 \\ &+ p_4(z_{11})F_4 + p_6(z_{11})F_6 : p_i(z_{11}) \in \mathbb{C}[1/z_{11}]\big\} \\ =: &\langle 1, F_2, F_3, F_4, F_6\rangle_{\mathbb{C}[\frac{1}{z_{11}}]} \end{aligned} \tag{11}$$

where the F_i are determined as follows [13, Sect. 9]: From the two functions $f_2, f_3 \in M^!(22)$,

$$f_2(\tau) := q^{-2} \prod_{n=1}^{\infty} \frac{(1-q^n)(1-q^{2n})^3}{(1-q^{11n})^3(1-q^{22n})} \text{ and } f_3(\tau) := q^{-3} \prod_{n=1}^{\infty} \frac{(1-q^n)^3(1-q^{2n})}{(1-q^{11n})(1-q^{22n})^3},$$

one constructs the desired $F_i \in M^\infty(11)$ by

$$F_2(\tau) := f_2(\tau) - (U_2 f_3)(\tau) = q^{-2} + 2q^{-1} - 12 + 5q + 8q^2 + \dots,$$
$$F_3(\tau) := f_3(\tau) - 4(U_2 f_2)(\tau) = q^{-3} - 3q^{-2} - 5q^{-1} + 24 - 13q - \dots,$$
$$F_4(\tau) := f_2(\tau)^2 + \frac{1}{2}(U_2 f_3^2)(\tau) = q^{-4} - \frac{3}{2}q^{-3} - \frac{7}{2}q^{-2} - \frac{21}{2}q^{-1} + 48 - \dots,$$
$$F_6(\tau) := f_3(\tau)^2 + 8(U_2 f_2^2)(\tau) = q^{-6} - 6q^{-5} + 7q^{-4} + 22q^{-3} - 41q^{-2} + \dots,$$

where U_2 is the special case $\ell = 2$ ("summing the even part") of the standard U-operator:

$$U_\ell \sum_{k=N}^{\infty} a(k) q^k := \sum_{k=\lceil N/\ell \rceil}^{\infty} a(\ell k) q^k. \tag{12}$$

In addition to $\operatorname{ord}_{[\infty]_{11}}(1/z_{11})^* = -5$, one has

$$(\operatorname{ord}_{[\infty]_{11}} F_2^*, \operatorname{ord}_{[\infty]_{11}} F_3^*, \operatorname{ord}_{[\infty]_{11}} F_4^*, \operatorname{ord}_{[\infty]_{11}} F_6^*) = (-2, -3, -4, -6). \tag{13}$$

Thus the minimal pole order of the functions which in the sense of (11) generate $M^\infty(11)$ is 2, not 1. Indeed, the gap at 1 is predicted by the Weierstrass gap theorem, Theorem 1.1, owing to the fact that the compact Riemann surface $X := X_0(11)$ has genus 1. A formula for the genus of $X_0(N)$, if $N = \ell$ is a prime, for instance, can be found in [4, Ex. 3.1.4(e)]; the genus for general N is determined in [4, Sec. 3.9].

Usually, as for instance in [5, III.5.3], Weierstrass's gap theorem is proved as a consequence of the Riemann-Roch theorem. In this article we prove Theorem 12.2, a version of the gap Theorem 1.1 for the case $X = X_0(N)$ and with the only pole put at ∞. The main objective of our proof and of this article is to present a proof which follows "first principles" as closely as possible and which avoids to invoke the Riemann-Roch theorem. In addition, our approach provides new algebraic insight by consisting in a combination of module presentations of modular function algebras, integral bases, Puiseux series, and discriminants. For example, using our approach to prove the bound $\leq 2g-1$ stated in the Weierstrass gap theorem is reduced to an elementary combinatorial argument; see Section 12. Another by-product of our proof of the Weierstrass gap Theorem 12.2 is a natural explanation of the genus $g = 0$ case as a consequence of the reduction to an integral basis.

In view of various constructive aspects involved, we are planning to exploit the algorithmic content of our approach for computer algebra applications, for instance, for the effective computation of suitable module bases for modular functions. As already mentioned, some ideas we used trace back to the celebrated work [16] by Dedekind and Weber; see [3] for an English translation together with an excellent introduction by John Stillwell.

Finally we remark that the history of Weierstrass's gap theorem and related topics like Weierstrass points present somehow a challenge. The historical account [1] by Andrea Del Centina describes the scientific evolution of the gap theorem up to the 1970s. Concerning its beginnings Centina says, "The history of Weierstrass points is not marked by a precise starting date because it is not clear when Weierstrass stated and proved his *Lückensatz* (or "gap" theorem) but one can argue that probably it was in the early 1860s."

The rest of our article is structured as follows. In Section 3 we introduce order-complete bases of modules over a polynomial ring $\mathbb{C}[t]$ to describe modular function algebras. In Section 4 we describe how such bases can be step-wise modified to obtain an integral basis; i.e., an order-complete basis for the full algebra $M^\infty(N)$. Under particular circumstances one can keep track of the total number of such steps, which then gives a proof of the Weierstrass gap Theorem 12.2. In order to do this bookkeeping one can use "order-reduction" polynomials discussed in Section 5. In Section 6 we explain how obtain order-reduction polynomials computationally; Section 7 deals with important special cases. In Section 8 and Section 9 we derive important ingredients for our proof of Theorem 12.2; for example, a factorization property of the discriminant polynomial in Prop. 9.3. In Section 10 and 11 we relate discriminant polynomials to order-reduction polynomials associated to integral bases. In Section 12 we use these results to prove the Weierstrass gap theorem in the version of Theorem 12.2. To prove the bound $2g-1$ for the size of the maximal gap, our approach allows a purely combinatorial argument (a gap property of monoids) which we describe in Section 13. At various places we require functions to have the separation property as defined in Section 9. In Section 14 we prove the existence of such functions by giving an explicit construction.

In order to keep this article as much self-contained as possible, the first Appendix Section 15 gives a short account on basic modular function facts needed; the second Appendix Section 16 recollects some fundamental facts about meromorphic functions on Riemann surfaces.

3. Modular function algebras as $\mathbb{C}[t]$-modules

We already used (implicitly) the convention that if a meromorphic function f has a pole, then the *pole order* is defined as the negative order at this point; i.e.,

$$\operatorname{pord}_p f := -\operatorname{ord}_p f.$$

If $f \in M^\infty(N)$ we simplify notation by using the convention for the pole order at infinity,

$$\operatorname{pord} f := -\operatorname{ord}_{[\infty]_N} f^*.$$

Definition 3.1. *A tuple $(b_0, b_1, \dots b_{n-1})$, $n \geq 1$, of modular functions in $M^\infty(N)$ is called order-complete if*

$$b_0 = 1 \ \text{ and } \ \operatorname{pord} b_i \equiv i \pmod{n} \ \text{ for } \ i = 1, \dots, n-1.$$

Slightly more general, any tuple $(1, \beta_1, \dots, \beta_{n-1})$ which is a reordering of an order-complete tuple $(1, b_1, \dots, b_{n-1})$; i.e.,

$$\{\beta_1, \dots, \beta_{n-1}\} = \{b_1, \dots, b_{n-1}\}, \tag{14}$$

is also called order-complete.

Example 3.2. The tuple $(1, F_6, F_2, F_3, F_4)$ with $F_j \in M^\infty(11)$ as in (11) is order-complete.

Example 3.3. Let

$$f(\tau) := q\,\frac{1}{z_{11}} \prod_{k=1}^{\infty}(1-q^{11k}) \sum_{n=0}^{\infty} p(11n+6)q^n.$$

The tuple $(1, f, f^2, f^3, f^4)$ is order-complete. Notice that $\operatorname{pord} f = 4$. In [12] it is shown that the subalgebra $\mathbb{C}[1/z_{11}, f]$ of $M^\infty(11)$, which is generated by all bivariate polynomials in $1/z_{11}$ and f, finds a representation as a $\mathbb{C}[1/z_{11}]$-module as follows:

$$\mathbb{C}[\frac{1}{z_{11}}, f] = \langle 1, f, f^2, f^3, f^4 \rangle_{\mathbb{C}[\frac{1}{z_{11}}]}.$$

In view of these examples we note that in contrast to (11), $\mathbb{C}[1/z_{11}, f] \neq M^\infty(11)$. For instance, it is obvious that this subalgebra does not contain any $g \in M^\infty(11)$ with $\operatorname{pord} g = 3$. Nevertheless, both function tuples,

$$\langle 1, F_6, F_2, F_3, F_4 \rangle_{\mathbb{C}[t]}, \ \text{ and } \ \langle 1, f, f^2, f^3, f^4 \rangle_{\mathbb{C}[t]},$$

form a *basis* of the corresponding $\mathbb{C}[t]$-module they generate where $t := 1/z_{11}$. Namely, since the generators have different pole orders modulo $\operatorname{pord} t = 5$, each element contained in these modules can be represented as a *unique* linear combination of the module generators with coefficients being polynomials in t. This motivates the

Definition 3.4. *For $t \in M^\infty(N)$ let $n := \operatorname{pord} t \geq 1$. Let M be the $\mathbb{C}[t]$-module generated by an order-complete tuple in $M^\infty(N)$; i.e.,*

$$\begin{aligned} M &= \big\{ p_0(t) + p_1(t) b_1 + \cdots + p_{n-1}(t) b_{n-1} : p_i(x) \in \mathbb{C}[x] \big\} \\ &=: \langle 1, b_1, b_2, \dots, b_{n-1} \rangle_{\mathbb{C}[t]}. \end{aligned}$$

Then we call $(1, b_1, \dots, b_{n-1})$ an order-complete basis for M over $\mathbb{C}[t]$. Slightly more general, any tuple $(1, \beta_1, \dots, \beta_{n-1})$ which is a reordering, in the sense of (14), of an order-complete basis $(1, b_1, \dots, b_{n-1})$ for M is also called an order-complete basis for M.

Proposition 3.5. *Let $t, f \in M^\infty(N)$ with $n := \operatorname{pord} t \geq 1$ and $\gcd(n, \operatorname{pord} f) = 1$. Then*

$$\mathbb{C}[t, f] = \langle 1, f, f^2, \ldots, f^{n-1} \rangle_{\mathbb{C}[t]},$$

where $(1, f, f^2, \ldots, f^{n-1})$ is an order-complete module basis.

Proof. If $\operatorname{pord} f^i \equiv \operatorname{pord} f^j \pmod n$ then $n \mid (i-j) \operatorname{pord} f$. This implies

$$\{1, 2, \ldots, n-1\} = \{\operatorname{pord} f \,(\mathrm{mod}\, n), \operatorname{pord} f^2 \,(\mathrm{mod}\, n), \ldots, \operatorname{pord} f^{n-1} \,(\mathrm{mod}\, n)\}.$$

In addition, as a consequence of Theorem 7.1 and Lemma 7.3 in [13], $f^n \in \langle 1, f, f^2, \ldots, f^{n-1} \rangle_{\mathbb{C}[t]}$. Hence $\mathbb{C}[t, f] \subseteq \langle 1, f, f^2, \ldots, f^{n-1} \rangle_{\mathbb{C}[t]}$. The reverse direction of this inclusion is trivial, which completes the proof. □

4. Integral bases

In Example 3.3 we saw that $(1, f, \ldots, f^4)$ is an order-complete basis of $\mathbb{C}[1/z_{11}, f]$ which is a proper subalgebra of $M^\infty(11)$.[2] In this section we shall see how such an order-complete basis can be step-wise modified to obtain an order-complete basis for the full algebra $M^\infty(11)$.

Definition 4.1. *Let $t \in M^\infty(N)$ with $n := \operatorname{pord} t \geq 1$. An order-complete tuple $(1, b_1, \ldots, b_{n-1})$, $b_j \in M^\infty(N)$, is called integral basis for $M^\infty(N)$ over $\mathbb{C}[t]$ if*

$$\langle 1, b_1, \ldots, b_{n-1} \rangle_{\mathbb{C}[t]} = M^\infty(N).$$

The motivation for this terminology comes from the

Lemma 4.2. *Let $f \in M(N)$ and $t \in M^\infty(N)$ with $\operatorname{pord} t \geq 1$ and*

$$\gcd(\operatorname{pord} f, \operatorname{pord} t) = 1.$$

Then f satisfies an algebraic relation

$$f^n + p_1(t) f^{n-1} + \cdots + p_n(t) = 0$$

with polynomials $p_j(x) \in \mathbb{C}[x]$ (i.e., f is integral over $\mathbb{C}[t]$) if and only if

$$f \in M^\infty(N).$$

Moreover, if $f \in M^\infty(N)$ then there exists an algebraic relation with $n = \operatorname{pord} t$.

Proof. The directions with the assumption $f \in M^\infty(N)$ follow immediately from Prop. 3.5. For the other direction, assume that $m := \operatorname{pord}_p f^* > 0$ for $p \neq [\infty]_N$. Then $\operatorname{pord}_p(f^n)^* = mn$, a contradiction to

$$\operatorname{pord}_p(p_1(t) f^{n-1} + \cdots + p_n(t))^* \leq (n-1)m.$$

□

[2] Notice that $\operatorname{pord} 1/z_{11} = 5$.

A crucial observation for the process to obtain an integral basis for $M^\infty(N)$ from an order-complete basis is stated in

Proposition 4.3. *Let $t \in M^\infty(N)$ with $n := \operatorname{pord} t \geq 1$. Let $(1, b_1, \ldots, b_{n-1})$ with $b_j \in M^\infty(N)$ be an order-complete basis of the $\mathbb{C}[t]$-module*

$$M := \langle 1, b_1, \ldots, b_{n-1} \rangle_{\mathbb{C}[t]} \subseteq M^\infty(N).$$

Then for any $f \in M^\infty(N)$ there exist polynomials $q(x)$ and $p_j(x)$ in $\mathbb{C}[x]$ such that

$$f = \frac{p_0(t)}{q(t)} + \frac{p_1(t)}{q(t)} b_1 + \cdots + \frac{p_{n-1}(t)}{q(t)} b_{n-1}. \tag{15}$$

Proof. For $j \in \mathbb{Z}_{\geq 0}$ consider the sets

$$G_j := \{t^j f - h : h \in M\}.$$

For each $j \geq 0$ choose a non-zero $g_j \in G_j$ such that $\operatorname{pord} g_j$ is minimal amongst all the elements in G_j. By construction, and using the convention $n\mathbb{Z}_{\geq 0} := \{nk : k \in \mathbb{Z}_{\geq 0}\}$, we have for all $j \geq 0$:

$$\operatorname{pord} g_j \notin S := (0 + n\mathbb{Z}_{\geq 0}) \cup (\operatorname{pord} b_1 + n\mathbb{Z}_{\geq 0}) \cup \cdots \cup (\operatorname{pord} b_{n-1} + n\mathbb{Z}_{\geq 0}).$$

Obviously, S is an additive submonoid of $(\mathbb{Z}_{\geq 0}, +)$. Moreover, $\mathbb{Z}_{\geq 0} \setminus S$ has only finitely many elements; let k be the maximal element in this set. Then there exist $c_j \in \mathbb{C}$, not all zero, such that

$$c_0 g_0 + c_1 g_1 + \cdots + c_{k+1} g_{k+1} = 0. \tag{16}$$

This is owing to the fact that equating the coefficients of non-positive powers in the q-expansions of both sides (which are functions in $M^\infty(N)$) gives $k+1$ equations in $k+2$ variables c_j. Hence the dimension of the $\mathbb{C}$-vector space G, which is generated by all the g_j, $j \geq 0$, is bounded by $k+1$. Using $g_j := t^j f - h_j$ with $h_j \in M$, (16) rewrites into the form

$$\begin{aligned} &c_0(f - h_0) + c_1(tf - h_1) + \cdots + c_{k+1}(t^{k+1} f - h_{k+1}) \\ &\quad = (c_0 + c_1 t + \cdots + c_{k+1} t^{k+1}) f - (c_0 h_0 + c_1 h_1 + \cdots + c_{k+1} h_{k+1}) = 0. \end{aligned}$$

The linear combination of the h_j is in M, hence this gives the desired relation for f with $q(t) = c_0 + c_1 t + \cdots + c_{k+1} t^{k+1}$. □

Corollary 4.4. *Let $t \in M^\infty(N)$ with $n := \operatorname{pord} t \geq 1$. Let $(1, b_1, \ldots, b_{n-1})$ with $b_j \in M^\infty(N)$ be an order-complete basis of the $\mathbb{C}[t]$-module*

$$M := \langle 1, b_1, \ldots, b_{n-1} \rangle_{\mathbb{C}[t]} \subseteq M^\infty(N).$$

If $M \neq M^\infty(N)$ then there exist $c_j \in \mathbb{C}$, not all zero, and α in $\mathbb{C}$ such that

$$h_\alpha := \frac{c_0 + c_1 b_1 + \cdots + c_{n-1} b_{n-1}}{t - \alpha} \in M^\infty(N) \setminus M. \tag{17}$$

In particular, there exists a uniquely determined $k \in \{1, \dots, n-1\}$ *such that*

$$\operatorname{pord} h_\alpha = \operatorname{pord} b_k - n \geq k \ \text{ and } \ c_k \neq 0. \tag{18}$$

Proof. By Prop. 4.3 there exists an $f \in M^\infty(N) \setminus M$ of the form (15) such that $q(x) \nmid p_i(x)$ for some $i \in \{0, \dots, n-1\}$. Hence there exists an $\alpha \in \mathbb{C}$ such that $x - \alpha \mid q(x)$ but $x - \alpha \nmid p_i(x)$. Consequently, $q(t)/(t-\alpha) \in M^\infty(N)$ and thus

$$g := f\frac{q(t)}{t-\alpha} = \frac{p_0(t) + p_1(t)b_1 + \cdots + p_{n-1}(t)b_{n-1}}{t-\alpha} \in M^\infty(N) \setminus M.$$

By division with remainder there are polynomials $q_j(x) \in \mathbb{C}[x]$ and $c_j \in \mathbb{C}$ such that $p_j(x) = (x-\alpha)q_j(x) + c_j$, $j = 0, \dots, n-1$. Rewriting the representation of g and noting that $c_i \neq 0$ proves the first part of the statement on h_α. To prove (18), consider

$$(t-\alpha)h_\alpha = c_0 + c_1 b_1 + \cdots + c_{n-1}b_{n-1},$$

which implies,

$$\operatorname{pord}(th_\alpha) = n + \operatorname{pord} h_\alpha = \max_{\substack{1 \leq j \leq n-1 \\ \text{and } c_j \neq 0}} \{\operatorname{pord} b_j\}.$$

Let k be that index for which $\operatorname{pord} b_k$ becomes maximal with $c_k \neq 0$. Recalling $\operatorname{pord} b_j \equiv j \pmod n$, $j = 1, \dots, n$, proves $\operatorname{pord} b_k \geq k + n$. Because otherwise $\operatorname{pord} b_k = k$ which owing to the choice of k would imply $\operatorname{pord} b_j = j$ for all $j = 1, \dots, n$, and the given order-complete basis would be integral. This proves (18). □

Corollary 4.4 motivates the following

Definition 4.5. *Let* $M = \langle 1, b_1, \dots, b_{n-1}\rangle_{\mathbb{C}[t]}$ *and* $h_\alpha \in M^\infty(N)$ *be as in Corollary 4.4; i.e.,* $M \neq M^\infty(N)$ *and* $\operatorname{pord} h_\alpha = \operatorname{pord} b_k - n \geq k$. *The replacement*

$$(1, \dots, b_{k-1}, b_k, b_{k+1}, \dots) \to (1, \dots, b_{k-1}, h_\alpha, b_{k+1}, \dots)$$

of b_k *by* h_α *is called a pole-order-reduction step associated to* $\alpha \in \mathbb{C}$.

We summarize in the form of

Proposition 4.6. *Let* $t \in M^\infty(N)$ *with* $n := \operatorname{pord} t \geq 1$. *Let* $(1, b_1, \dots, b_{n-1})$ *with* $b_j \in M^\infty(N)$ *be an order-complete basis of the* $\mathbb{C}[t]$*-module*

$$M := \langle 1, b_1, \dots, b_{n-1}\rangle_{\mathbb{C}[t]} \subseteq M^\infty(N).$$

If $M \neq M^\infty(N)$ *then:*

(i) *By a finite sequence of pole-order-reduction steps the order-complete basis* $(1, b_1, \dots, b_{n-1})$ *can be transformed into an integral basis* $(1, \beta_1, \dots, \beta_{n-1})$ *such that*

$$\langle 1, \beta_1, \dots, \beta_{n-1}\rangle_{\mathbb{C}[t]} = M^\infty(N).$$

(ii) *If* $(1, \beta_1', \ldots, \beta_{n-1}')$ *is any another integral basis; i.e.,*

$$\langle 1, \beta_1', \ldots, \beta_{n-1}' \rangle_{\mathbb{C}[t]} = M^\infty(N),$$

then

$$\{\operatorname{pord}\beta_1, \ldots, \operatorname{pord}\beta_{n-1}\} = \{\operatorname{pord}\beta_1', \ldots, \operatorname{pord}\beta_{n-1}'\}. \tag{19}$$

Proof. The proof of part (i) is an immediate consequence of Cor. 4.4. Namely, owing to (18) each step reduces the pole order of one of the basis elements by n. This guarantees termination in finitely many steps. To prove (ii), without loss of generality we can assume that $\operatorname{pord}\beta_j \equiv \operatorname{pord}\beta_j' \equiv j \pmod n$ for all j. Suppose $\operatorname{pord}\beta_j \neq \operatorname{pord}\beta_j'$ for some $j \in \{1, \ldots, n-1\}$; i.e., $\operatorname{pord}\beta_j' = \operatorname{pord}\beta_j + kn$ with $k \geq 1$. But this implies that $\beta_j \notin \langle 1, \beta_1', \ldots, \beta_{n-1}' \rangle_{\mathbb{C}[t]}$, because then no element in this module can have the same pole order as β_j, a contradiction. □

5. Order-reduction polynomials

The previous section showed that by applying a procedure using finitely many steps any order-complete basis of a subalgebra of $M^\infty(N)$ can be extended to an integral basis of $M^\infty(N)$. Moreover, by (19) the pole orders of the integral basis functions are uniquely determined. It turns out that under particular circumstances one can keep track of the number of order-reduction steps, which then gives a proof of the Weierstrass gap Theorem 12.2. In order to do this bookkeeping one can use "order-reduction" polynomials. To our knowledge the first time such polynomials have been used was by Dedekind and Weber [16]; see [3] for Stillwell's translation into English.

Throughout this section, $t \in M^\infty(N)$ with $n := \operatorname{pord} t \geq 1$ and $(1, b_1, \ldots, b_{n-1})$ with $b_j \in M^\infty(N)$ is an order-complete basis of the $\mathbb{C}[t]$-module

$$M := \langle 1, b_1, \ldots, b_{n-1} \rangle_{\mathbb{C}[t]} \subseteq M^\infty(N).$$

Owing to $t(\tau) = \infty$ if and only if $[\tau]_N = [\infty]_N$, t is a holomorphic function on $\mathbb{H}$. Moreover, the induced function t^*, which is meromorphic on the compact Riemann surface $X_0(N)$, has a pole only at $[\infty]_N$.

Remark 5.1 (a basic notational convention). In general, every modular function $f \in M(N)$ gives rise to an induced meromorphic function $f^* : X_0(N) \to \hat{\mathbb{C}}$ which for $x = [\tau]_N$ is defined as

$$f^*(x) = f^*([\tau]_N) := f(\tau),\ \tau \in \hat{\mathbb{H}}; \tag{20}$$

see Appendix Section 15. A central theme in what follows is to consider maps

$$f^* \circ (t^* \mid U)^{-1} : V \to \hat{\mathbb{C}}$$

where $U \subseteq X_0(N)$ and $V \subseteq \mathbb{C}$ are open sets such that

$$t^* : U \to V \text{ is bi-holomorphic.}$$

Hence for $v \in V$, evaluations

$$f^* \circ (t^* \mid U)^{-1}(v) = f^*((t^* \mid U)^{-1}(v))$$

have to be interpreted in the sense of (20); i.e., interpreting $x = (t^* \mid U)^{-1}(v)$ as $x = [\tau]_N$ for some $\tau \in \hat{\mathbb{H}}$.

Depending on the context, we will freely move between considering t as a function on $\mathbb{H}$, resp. $\hat{\mathbb{H}}$, and its induced version $t^* : X_0(N) \to \hat{\mathbb{C}}$.

Using the terminology explained in the Appendix Section 16, we assume that $v_0 \in \mathbb{C}$ is not a branch point of t^*; in short, $v_0 \notin \text{BranchPts}(t^*)$. In this case there are n pairwise distinct points $x_j = [\tau_j]_N \in X_0(N)$ with $\tau_j \in \mathbb{H}$ such that

$$t^{*-1}(v_0) = \{x_1, \ldots, x_n\}. \tag{21}$$

In addition, there exists a neighborhood V of v_0 and neighborhoods U_j of the x_j such that

$$t^{*-1}(V) = U_1 \cup \cdots \cup U_n \text{ as a disjoint union of open sets,}$$

and such that for $j = 1, \ldots, n$ the restricted functions

$$t^*|U_j : U_j \to V \text{ are bi-holomorphic.}$$

Let

$$T_j := (t^*|U_j)^{-1} : V \to U_j,\ j = 1, \ldots, n.$$

Define

$$D_t(1, b_1, \ldots, b_{n-1}) : V \to \mathbb{C} \tag{22}$$

by

$$D_t(1, b_1, \ldots, b_{n-1})(v) := \begin{vmatrix} 1 & 1 & \cdots & 1 \\ (b_1^* \circ T_1)(v) & (b_1^* \circ T_2)(v) & \cdots & (b_1^* \circ T_n)(v) \\ \vdots & \vdots & \ddots & \vdots \\ (b_{n-1}^* \circ T_1)(v) & (b_{n-1}^* \circ T_2)(v) & \cdots & (b_{n-1}^* \circ T_n)(v) \end{vmatrix}^2.$$

Taking the square of the determinant guarantees that the expression on the right side is symmetric with respect to any permutation of $T_1, \ldots, T_n$. Consequently, $D_t(1, b_1, \ldots, b_{n-1})$ is a holomorphic function on V. Carrying out the same construction on neighborhoods V for all $v_0 \in \mathbb{C} \setminus \text{BranchPts}(t^*)$, and gluing the resulting functions $D_t(1, b_1, \ldots, b_{n-1}) : V \to \mathbb{C}$ together, gives a global holomorphic function

$$D_t(1, b_1, \ldots, b_{n-1}) : \mathbb{C} \setminus \text{BranchPts}(t^*) \to \mathbb{C}.$$

By using the same arguments as in the proof of Theorem 8.2 in [6], this function can be extended to a meromorphic function

$$D_t(1, b_1, \ldots, b_{n-1}) : \hat{\mathbb{C}} := \mathbb{C} \cup \{\infty\} \to \hat{\mathbb{C}}$$

with ∞ as its only pole. Classical complex analysis tells that $\mathcal{M}(\hat{\mathbb{C}}) = \mathbb{C}(z)$; i.e., the field of meromorphic functions on $\hat{\mathbb{C}}$ are rational functions with coefficients in $\mathbb{C}$. Hence we have

Lemma 5.2. *The meromorphic function $D_t(1, b_1, \ldots, b_{n-1})(v)$ constructed above is a polynomial function in v.*

Definition 5.3. *The polynomial $D_t(1, b_1, \ldots, b_{n-1})(x) \in \mathbb{C}[x]$ is called order-reduction polynomial for the order-complete basis $(1, b_1, \ldots, b_{n-1})$, $b_j \in M^\infty(N)$, of the $\mathbb{C}[t]$-module*

$$\langle 1, b_1, \ldots, b_{n-1}\rangle_{\mathbb{C}[t]} \subseteq M^\infty(N),$$

where $t \in M^\infty(N)$ with $n := \operatorname{pord} t \geq 1$.

Example 5.4. Taking

$$t := \frac{1}{z_{11}} = \frac{1}{q^5} - \frac{12}{q^4} + \frac{54}{q^3} - \frac{88}{q^2} - \frac{99}{q} + 540 - 418q - \cdots \in M^\infty(11)$$

and

$$(1, b_1, \ldots, b_4) := (1, F_2, F_3, F_4, F_6)$$

where the $F_j \in M^\infty(11)$ are as in Example 2.4, one obtains

$$D_{1/z_{11}}(1, F_2, F_3, F_4, F_6)(x) = x^4(5^5 11^6 - 2 \cdot 3^2 \cdot 439081x + 5^5 x^2). \tag{23}$$

Example 5.5. Taking t and the b_j as in Example 5.4, one obtains

$$D_{1/z_{11}}(1, F_2, F_4^2, F_4, F_6)(x) = (11^3 + x)^2 D_{1/z_{11}}(1, F_2, F_3, F_4, F_6)(x). \tag{24}$$

Remark 5.6. How such polynomials are computed is explained in Section 6.

In Corollary 4.4 we proved that if $M \neq M^\infty(N)$ then there exist $c_j \in \mathbb{C}$, not all zero, and v_0 in $\mathbb{C}$ such that

$$\frac{c_0 + c_1 b_1 + \ldots c_{n-1} b_{n-1}}{t - v_0} \in M^\infty(N) \setminus M. \tag{25}$$

Recall that above we denoted the n pairwise distinct preimages of v_0 as follows:

$$t^*(x_1) = t^*([\tau_1]_N) = t(\tau_1) = v_0, \ldots, t^*(x_n) = t^*([\tau_n]_N) = t(\tau_n) = v_0.$$

Relation (25) implies

$$c_0 + c_1 b_1(\tau_1) + \cdots + c_{n-1} b_{n-1}(\tau_1) = 0, \ldots, c_0 + c_1 b_1(\tau_n) + \cdots + c_{n-1} b_{n-1}(\tau_n) = 0.$$

As a necessary condition for the existence of $c_j \in \mathbb{C}$ not all zero, the determinant

$$\begin{vmatrix} 1 & b_1(\tau_1) & \cdots & b_{n-1}(\tau_1) \\ 1 & b_1(\tau_2) & \cdots & b_{n-1}(\tau_2) \\ \vdots & \vdots & \ddots & \vdots \\ 1 & b_1(\tau_n) & \cdots & b_{n-1}(\tau_n) \end{vmatrix}$$

of the corresponding linear system has to be zero. In view of

$$(b_i^* \circ T_j)(v_0) = b_i^*((t^* \mid U_j)^{-1}(v_0)) = b_i^*(x_j) = b_i(\tau_j),$$

the square of this determinant (taking the underlying matrix transposed) is $D_t(1, b_1, \ldots, b_{n-1})(v_0)$. Above we used the fact that the definition for

$$D_t(1, b_1, \ldots, b_{n-1}) : \mathbb{C} \setminus \mathrm{BranchPts}(t^*) \to \mathbb{C}$$

extends to the polynomial function

$$D_t(1, b_1, \ldots, b_{n-1}) : \hat{\mathbb{C}} \to \hat{\mathbb{C}}.$$

This means, the case when $v_0 \in \mathbb{C}$ is a branch point of t^* is also covered by the same determinant condition

$$D_t(1, b_1, \ldots, b_{n-1})(v_0) = 0.$$

But if $v_0 \in \mathbb{C}$ is a branch point, this condition is automatically satisfied, because then at least two rows,

$$(1, b_1(\tau_i), \ldots, b_{n-1}(\tau_i)) \text{ and } (1, b_1(\tau_j), \ldots, b_{n-1}(\tau_j)),$$

are equal for $i \neq j$. Summarizing, this gives

Lemma 5.7. *Let $t \in M^\infty(N)$ with $n := \operatorname{pord} t \geq 1$. Let $(1, b_1, \ldots, b_{n-1})$ with $b_j \in M^\infty(N)$ be an order-complete basis of the $\mathbb{C}[t]$-module*

$$M := \langle 1, b_1, \ldots, b_{n-1} \rangle_{\mathbb{C}[t]} \subseteq M^\infty(N) \text{ and } M \neq M^\infty(N).$$

Let $v_0 \in \mathbb{C}$ be such that[3]

$$\frac{c_0 + c_1 b_1 + \ldots c_{n-1} b_{n-1}}{t - v_0} \in M^\infty(N) \setminus M.$$

for $c_j \in \mathbb{C}$, not all zero. Then

$$D_t(1, b_1, \ldots, b_{n-1})(v_0) = 0. \tag{26}$$

If v_0 is a branch point of t^*, condition (26) is automatically satisfied.

[3]The existence of such a v_0 is owing to Corollary 4.4.

6. How to compute order-reduction polynomials

Next we explain how to compute the order-reduction polynomials in (23) and (24).

To this end, it will be convenient to introduce the following notation:

Definition 6.1. *If*

$$f(\tau) = \sum_{n=-K}^{\infty} f_n q^n$$

is the q-expansion at infinity for some $f \in M^\infty(N)$, we define

$$\tilde{f}(q) := \sum_{n=-K}^{\infty} f_n q^n;$$

i.e.,

$$f(\tau) = \tilde{f}(q(\tau)) = \tilde{f}(q) \ \textit{ with } \ q = q(\tau) = e^{2\pi i \tau} \ \textit{ for } \ \tau \in \mathbb{H}.$$

Returning to the setting (21), we again assume that $v_0 \in \mathbb{C}$ is not a branch point of t^*. This means, there exist pairwise distinct $x_j = [\tau_j]_N \in X_0(N)$ with $\tau_j \in \mathbb{H} \cup \mathbb{Q}$ such that $[\tau_j]_N \neq [\infty]_N$ and[4]

$$t^{*-1}(v_0) = \{x_1, \dots, x_n\},$$

together with neighborhoods U_j of the x_j such that for a suitable neighborhood V of v_0,

$$t^{*-1}(V) = U_1 \cup \dots \cup U_n, \ \text{ as a disjoint union of open sets,}$$

and such that the restricted functions

$$T_j = (t^*|U_j)^{-1} : V \to U_j \ \text{ are bi-holomorphic.}$$

For each $j = 1, \dots, n$ and $v \in V$ our goal, achieved in Lemma 6.2(ii), is to determine expressions for $q_j(v) := q^{2\pi i \tau(j)}$ where $\tau(j)$ is close to τ_j such that

$$t^*([\tau(j)]_N) = t(\tau(j)) = \tilde{t}(q_j(v)) = v.$$

For $q = e^{2\pi i \tau}$ with $\tau \in \mathbb{H}$ we have:

$$\tilde{t}(q) = \frac{1}{q^n}(1 + \varphi(q)) := \frac{1}{q^n}(1 + \varphi_1 q + \varphi_2 q^2 + \dots).$$

Here we assume that the first coefficient in this q-expansion of t is 1. Now, if

$$1 + \psi(q) := 1 + \psi_1 q + \psi_2 q^2 + \dots := \frac{1}{1 + \varphi(q)},$$

[4]Notice that, in particular, $\tau \neq \infty$.

and

$$(1+\psi(q))^{1/n} := \sum_{l=0}^{\infty} \binom{1/n}{l} \psi(q)^l, \tag{27}$$

then

$$\tilde{t}(q) = \frac{1}{U(q)^n} \text{ where } U(q) := q(1+\psi(q))^{1/n}. \tag{28}$$

To fix a branch of the nth root we choose the preimage τ_n and recall that

$$v_0 = t^*([\tau_n]_N) = t(\tau_n) = \tilde{t}(e^{2\pi i \tau_n}).$$

Now, for each $v \in \mathbb{C}$ close to v_0 there is for each $j \in \{1, \ldots, n\}$ a uniquely determined $\tau(j) \in \mathbb{H}$ close to τ_j such that

$$v = t^*([\tau(j)]_N) = t(\tau(j)) = \tilde{t}(e^{2\pi i \tau(j)}). \tag{29}$$

By choosing a neighborhood of τ_n we fix a branch of the nth root of $v \in \mathbb{C}$ close to v_0:

$$\sqrt[n]{v} := \frac{1}{U(q)} \text{ with } q = e^{2\pi i \tau(n)} \text{ where } \tau(n) \text{ is close to } \tau_n \text{ and determined as in (29).} \tag{30}$$

In addition, let W be such that $U(W(q)) = W(U(q)) = q$, and define

$$\zeta_n := e^{\frac{2\pi i}{n}}.$$

After this preparation, in view of (30) we can put things together as follows.

Lemma 6.2. *In the given setting, for $j = 1, \ldots, n$ and $v \in \mathbb{C}$ close to v_0 let*

$$q_j(v) := W\Big(\zeta_n^j \frac{1}{\sqrt[n]{v}}\Big) \text{ where } \sqrt[n]{v} \text{ is defined as in (30),}$$

Then for $j = 1, \ldots, n$ and $v \in \mathbb{C}$ close to v_0:

(i) $q_j(v) = e^{2\pi i \tau(j)}$, *where* $[\tau(j)]_N = T_j(v)$ *with* $\tau(j)$ *as in* (29),

and

(ii) $\tilde{t}(q_j(v)) = v$, *where the values* $q_j(v)$ *are pairwise distinct for* $j = 1, \ldots, n$.

Proof. The values $q_j(v)$, $j = 1, \ldots, n$, are defined by power series in $q = q(\tau(n))$:

$$q_j(v) = W(\zeta_n^j U(q)) = \zeta_n^j q + O(q^2) \text{ with } q = e^{2\pi i \tau(n)} \text{ where } \tau(n) \text{ is close to } \tau_n.$$

For fixed v close to v_0 these values are pairwise different for $j = 1, \ldots, n$ because

$$q_j(v) = W(\zeta_n^j U(q)) = W(\zeta_n^k U(q)) = q_k(v) \Rightarrow \zeta_n^j U(q) = \zeta_n^k U(q).$$

By (28),

$$\tilde{t}(q_j(v)) = \frac{1}{U(q_j(v))^n} = U\Big(W\Big(\zeta_n^j \frac{1}{\sqrt[n]{v}}\Big)\Big)^{-n} = v.$$

This implies (i) and (ii). □

Lemma 6.2 enables us to compute the polynomial $D_t(1, b_1, \dots, b_{n-1})(v)$, because by part (i) with $i = 1, \dots, n-1$ and $j = 1, \dots, n$:

$$(b_i^* \circ T_j)(v) = b_i^*(T_j(v)) = \widetilde{b_i}(e^{2\pi i \tau(j)}) = \sum_{\ell = -\operatorname{pord} b_i} \beta_\ell^{(i)} q_j(v)^\ell = \widetilde{b_i}\Big(W\Big(\zeta_n^j \frac{1}{\sqrt[n]{v}}\Big)\Big).$$

This means, each $(b_i^* \circ T_j)(v)$ can be represented as a Laurent series in powers of $1/v^{1/n}$,

$$(b_i^* \circ T_j)(v) = \zeta_n^{-j \operatorname{pord} b_i} v^{\frac{\operatorname{pord} b_i}{n}} + \alpha_{i,j} v^{\frac{\operatorname{pord} b_i - 1}{n}} + \cdots + \beta_{i,j} \frac{1}{v^{1/n}} + \dots, \tag{31}$$

with coefficients $\alpha_{i,j}, \beta_{i,j}$, etc., in $\mathbb{C}$, and under the assumption that the first Laurent series coefficient $\beta^{(i)}_{-\operatorname{pord} b_i}$ of each $\widetilde{b_i}(q_j(v))$ is equal to 1. Owing to Lemma 5.2 $D_t(1, b_1, \dots, b_{n-1})(v)$ as defined in (22) must be a polynomial in v. Consequently we can compute it by taking suitable truncated versions of the expansions (31).

Remark 6.3. This is how we computed the order-reduction polynomials in (23) and (24).

7. Discriminant polynomials

Important special cases of order-reduction polynomials are produced by order-complete module bases of $\mathbb{C}[t, f]$ of the form as in Proposition 3.5.

Definition 7.1. *Let $t, f \in M^\infty(N)$ with $n := \operatorname{pord} t \geq 1$, and $\gcd(n, \operatorname{pord} f) = 1$. Then*

$$D_t(f)(v) := D_t(1, f, f^2, \dots, f^{n-1})(v)$$

is called the discriminant polynomial for the order-complete basis $(1, f, \dots, f^{n-1})$ of the $\mathbb{C}[t]$-module

$$\langle 1, f, f^2 \dots, f^{n-1} \rangle_{\mathbb{C}[t]} = \mathbb{C}[t, f] \subseteq M^\infty(N).$$

The discriminant polynomial

$$\begin{aligned} D_t(f)(v) &= \begin{vmatrix} 1 & 1 & \cdots & 1 \\ f^*(T_1(v)) & f^*(T_2(v)) & \cdots & f^*(T_n(v)) \\ \vdots & \vdots & \ddots & \vdots \\ f^*(T_1(v))^{n-1} & f^*(T_2(v))^{n-1} & \cdots & f(T_n(v))^{n-1} \end{vmatrix}^2 \\ &= \prod_{1 \leq i < j \leq n} \Big(f^*(T_i(v)) - f^*(T_j(v))\Big)^2. \end{aligned}$$

factors being the square of a Vandermonde determinant. Now invoking (31) with $b_i = f$, and thus $\operatorname{pord} b_i = \operatorname{pord} f$, gives

$$f^*(T_j(v)) = \zeta_n^{-j \operatorname{pord} f} v^{\frac{\operatorname{pord} f}{n}} + \alpha_j v^{\frac{\operatorname{pord} f - 1}{n}} + \cdots + \beta_j \frac{1}{v^{1/n}} + \ldots.$$

Hence

$$f^*(T_i(v)) - f^*(T_j(v)) = (\zeta_n^{-i \operatorname{pord} f} - \zeta_n^{-j \operatorname{pord} f}) v^{\frac{\operatorname{pord} f}{n}} + \ldots$$

and thus

$$D_t(f)(v) = \text{constant} \cdot v^{2\binom{n}{2}\frac{\operatorname{pord} f}{n}} + \ldots.$$

Summarizing, we have

Lemma 7.2. *Let $t, f \in M^\infty(N)$ with $n := \operatorname{pord} t \geq 1$, and $\gcd(n, \operatorname{pord} f) = 1$. Then the degree of the discriminant polynomial $D_t(f)(x) \in \mathbb{C}[x]$ is*

$$\deg_x D_t(f)(x) = (n-1) \operatorname{pord} f. \tag{32}$$

8. Reduction steps and order-reduction polynomials

In Section 4 we described how order-complete bases can be transformed into integral bases of $M^\infty(N)$ by a finite sequence of pole-order-reduction steps. In this section we establish a link between pole-order-reduction steps and order-reduction polynomials.

To this end, we consider again our standard situation: let $t \in M^\infty(N)$ with $n := \operatorname{pord} t \geq 1$, let $(1, b_1, \ldots, b_{n-1})$ with $b_j \in M^\infty(N)$ be an order-complete basis of the $\mathbb{C}[t]$-module

$$M := \langle 1, b_1, \ldots, b_{n-1} \rangle_{\mathbb{C}[t]} \subseteq M^\infty(N).$$

By Cor. 4.4, when $M \neq M^\infty(N)$ there exist $c_j \in \mathbb{C}$, not all zero, and α in $\mathbb{C}$ such that

$$h_\alpha := \frac{c_0 + c_1 b_1 + \ldots c_{n-1} b_{n-1}}{t - \alpha} \in M^\infty(N) \setminus M. \tag{33}$$

In particular, there exists a $k \in \{1, \ldots, n-1\}$ such that

$$\operatorname{pord} h_\alpha = \operatorname{pord} b_k - n \geq k \text{ and } c_k \neq 0. \tag{34}$$

Proposition 8.1. *With regard to order-reduction polynomials this setting is reflected by*

$$\begin{aligned} &D_t(1, b_1, \ldots, b_{k-1}, h_\alpha, b_{k+1}, \ldots, b_{n-1})(v) \\ &\quad = \frac{c_k^2}{(v-\alpha)^2} D_t(1, b_1, \ldots, b_{k-1}, b_k, b_{k+1}, \ldots, b_{n-1})(v). \end{aligned} \tag{35}$$

Proof. After filling the right side of (33) into the determinant definition (22) of $D_t(1, b_1, \ldots, b_{k-1}, h_\alpha, b_{k+1}, \ldots, b_{n-1})(v)$ and noticing that $t^*(T_j(v)) = v$, $j = 1, \ldots, n$, the proof is a straightforward consequence of determinant calculus. □

In other words, a pole-order-reduction step associated to $\alpha \in \mathbb{C}$,

$$(1, \dots, b_{k-1}, b_k, b_{k+1}, \dots) \to (1, \dots, b_{k-1}, h_\alpha, b_{k+1}, \dots),$$

from one order-complete basis to another, corresponds to factoring the order-reduction polynomial as

$$\begin{aligned} &D_t(1,b_1, \dots, b_{k-1}, b_k, b_{k+1}, \dots, b_{n-1})(x) \\ &\qquad = \text{constant} \cdot (x-\alpha)^2 D_t(1, b_1, \dots, b_{k-1}, h_\alpha, b_{k+1}, \dots, b_{n-1})(x). \end{aligned} \tag{36}$$

Example 8.2. In the situation of Ex. 5.5:

$$F_3 + 12F_2 + 11^2 = -\frac{161051 + 15972F_2 + F_4^2 + 242F_4 - 121/4F_6}{1/z_{11} + 11^3}.$$

9. Local Puiseux Expansions

By considering local expansions at finitely many points $[\tau_j]_N \in X_0(N)$ for $\tau_j \in \hat{\mathbb{H}} = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$, in this section we derive important ingredients for our proof of Theorem 12.2. To this end, we consider charts $\varphi_{\tau_0} : U_0 \to \mathbb{C}$ with $\varphi_{\tau_0}([\tau]_N) := \phi_{\tau_0}(\tau)$ defined in a standard way either by

$$\phi_{\tau_0}(\tau) := \tau - \tau_0, \text{ if } \tau_0 \in \mathbb{H} \text{ is no elliptic point,} \tag{37}$$

or by

$$\phi_{\tau_0}(\tau) := \Big(\frac{\tau - \tau_0}{\tau - \overline{\tau_0}}\Big)^{h(\tau_0)}, \text{ if } \tau_0 \in \mathbb{H} \text{ is an elliptic point (cf. (41)),} \tag{38}$$

or, according to (91), by

$$\phi_{\tau_0}(\tau) := e^{2\pi i \gamma^{-1}\tau / w_N(c)}, \text{ if } \tau_0 = \frac{a}{c} = \gamma\infty \in \mathbb{Q} \cup \{\infty\}. \tag{39}$$

Here $U_0 \subseteq X_0(N)$ is a neighborhood of $[\tau_0]_N$; furthermore, the periods $h(\tau_0)$ equal either 2 or 3. We note explicitly that all these charts are centered at 0; i.e.,

$$\phi_{\tau_0}(\tau_0) = 0. \tag{40}$$

Remark 9.1. The explanation why such charts have to be chosen can be found, for instance, in [4, Sect. 2.2 and 2.3]. Charts, being homeomorphisms between open subsets of Riemann surfaces and of $\mathbb{C}$, are used to set up local series expansions. Charts of the kind as in (38) have to be taken when $[\tau_0]_N$ is an *elliptic* point; i.e., if

$$\{\gamma \in \Gamma_0(N) : \gamma\tau_0 = \tau_0\} \neq \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)\}. \tag{41}$$

Throughout this section, again $t \in M^\infty(N)$ with $n := \operatorname{pord} t \geq 1$. Now we reconsider the setting in Section 5 by dropping the assumption that $v_0 \in \mathbb{C}$ is

not a branch point of t^*. This means, we allow $\ell \leq n$ pairwise distinct points $x_j = [\tau_j]_N \in X_0(N)$ with $\tau_j \in \mathbb{H} \cup \mathbb{Q}$ such that $[\tau_j]_N \neq [\infty]_N$ and[5]

$$t^{*-1}(v_0) = \{x_1, \ldots, x_\ell\}.$$

There exists a neighborhood V_0 of v_0 and neighborhoods U_j of the x_j such that

$$t^{*-1}(V_0) = U_1 \cup \cdots \cup U_\ell \text{ as a disjoint union of open sets.}$$

Now, if $\ell < n$, not all of the restricted functions

$$t^*|U_j : U_j \to V_0 \text{ are bi-holomorphic.}$$

Summarizing this setting,

$$t^*(x) = v_0 \text{ has } \ell \leq n \text{ solutions } x_1 = [\tau_1]_N, \ldots, x_\ell = [\tau_\ell]_N$$
$$\text{with multiplicities } k_1, \ldots, k_\ell, \text{respectively. (I.e., } k_1 + \cdots + k_\ell = n.)$$

Hence, if V is an open subset of V_0 not containing v_0, then for each $j = 1, \ldots, \ell$ there exist pairwise disjoint open subsets $U_{j,k} \subseteq U_j$, $k = 1, \ldots, k_j$ such that

$$t^{*-1}(V) = \Big(U_{1,1} \cup \cdots \cup U_{1,k_1}\Big) \cup \cdots \cup \Big(U_{\ell,1} \cup \cdots \cup U_{\ell,k_\ell}\Big) \tag{42}$$

as a disjoint union, and for $k = 1, \ldots, k_j$, the restricted functions

$$t^*|U_{j,k} : U_{j,k} \to V \text{ are bi-holomorphic.}$$

For all $[\tau]_N \in U_j$, $j = 1, \ldots, \ell$, one has expansions

$$t^*([\tau]_N) = v_0 + a_{j,0}\phi_{\tau_j}(\tau)^{k_j} + a_{j,1}\phi_{\tau_j}(\tau)^{k_j+1} + \ldots \text{ with } a_{j,0} \neq 0. \tag{43}$$

Again by using (27) one has

$$t(\tau) - v_0 = B_j(\phi_{\tau_j}(\tau))^{k_j} \tag{44}$$

where

$$B_j(z) := z\Big(a_{j,0} + a_{j,1}z + \ldots\Big)^{1/k_j}.$$

For $j = 1, \ldots, \ell$ let

$$A_j(z) = A_{j,1}z + A_{j,2}z^2 + \ldots \text{ such that } A_j(B_j(z)) = B_j(A_j(z)) = z.$$

Now, by inverting the relation (44) and using Puiseux series, the situation of (42) is reflected as follows: For each $v \in V$ there is for fixed (j,k), $j = 1, \ldots, k_j$ and $k \in \{1, \ldots, k_j\}$, a uniquely determined $\tau = \tau(j,k) \in U_{j,k}$ such that

$$[\tau]_N = [\tau(j,k)]_N = (t^* \mid U_{j,k})^{-1}(v).$$

For such pairs $\tau = \tau(j,k)$ and v one has

$$\begin{aligned}\phi_{\tau_j}(\tau) = \phi_{\tau_j}(\tau(j,k)) &= A_j\Big(\zeta_{k_j}^k (v - v_0)^{1/k_j}\Big) \\ &= A_{j,1}\zeta_{k_j}^k (v - v_0)^{1/k_j} + A_{j,2}\zeta_{k_j}^{2k} (v - v_0)^{2/k_j} + \ldots\end{aligned} \tag{45}$$

[5]Note that, in particular, $\tau_j \neq \infty$.

As in Section 5 one works with a fixed branch of the k_jth root; moreover, we note that as a consequence of the definition of $A_j(z)$, $A_{j,1} \neq 0$ for all $j = 1, \ldots, \ell$.

In order to connect to discriminant polynomials, let $f \in M^\infty(N)$ be such that $\gcd(n, \operatorname{pord} f) = 1$. Moreover, without loss of generality, for $j = 1, \ldots, \ell$ we can assume that the neighborhoods U_j are chosen such that the following expansions exist for all $[\tau]_N \in U_j$:

$$f^*([\tau]_N) = f(\tau) = f(\tau_j) + \sum_{m=1}^{\infty} b_{j,m} \phi_{\tau_j}(\tau)^m. \tag{46}$$

Invoking (45) one obtains

Lemma 9.2. *For $v_0 \in \mathbb{C}$ and $j = 1, \ldots, \ell$ suppose that open neighborhoods $U_{j,k}$, $k = 1, \ldots, k_j$ and V are chosen as above. Then there exist series expansions with complex coefficients $c_{j,p}$ such that for all $v \in V$:*

$$f\Big((t^* \mid U_{j,k})^{-1}(v)\Big) = f(\tau_j) + \sum_{p=1}^{\infty} c_{j,p} \zeta_{k_j}^{pk} (v - v_0)^{p/k_j}. \tag{47}$$

Proof. Setting $[\tau]_N := (t^* \mid U_{j,k})^{-1}(v) \in U_{j,k}$ the statement follows from applying (45) to (46):

$$f(\tau) = f(\tau_j) + \sum_{m=1}^{\infty} b_{j,m} \Big(A_{j,1} \zeta_{k_j}^{k} (v - v_0)^{1/k_j} + A_{j,2} \zeta_{k_j}^{2k} (v - v_0)^{2/k_j} + \ldots \Big)^m.$$

□

To adapt to the refined setting (42) we extend our T_j-notation to the additional restricted functions:

$$T_{j,k} = (t^* | U_{j,k})^{-1} : V \to U_{j,k}.$$

Finally we use the information we obtained in terms of the local holomorphic Puiseux series expansion to represent the discriminant polynomial at $v_0 \in \mathbb{C}$.

Namely, for all $v \in V$:

$$\begin{aligned} D_t(f)(v) &= (-1)^{\binom{n}{2}} \prod_{(j,k)\neq(j',k')} \Big(f(T_{j,k}(v)) - f(T_{j',k'}(v))\Big) \\ &= (-1)^{\binom{n}{2}} \prod_{\substack{1\le j\le \ell \\ 1\le k,k'\le k_j, k\neq k'}} \Big(f(T_{j,k}(v)) - f(T_{j,k'}(v))\Big) \\ &\qquad \prod_{\substack{1\le j,j'\le \ell, j\neq j' \\ 1\le k,k'\le k_j}} \Big(f(T_{j,k}(v)) - f(T_{j',k'}(v))\Big) \\ &= (-1)^{\binom{n}{2}} \prod_{\substack{1\le j\le \ell \\ 1\le k,k'\le k_j, k\neq k'}} \Big(\sum_{p=1}^{\infty} c_{j,p}(\zeta_{k_j}^{pk} - \zeta_{k_j}^{pk'})(v-v_0)^{p/k_j}\Big) \\ &\qquad \prod_{\substack{1\le j,j'\le \ell, j\neq j' \\ 1\le k,k'\le k_j}} \Big(f(\tau_j) - f(\tau_{j'}) + O((v-v_0)^{1/k_j}) - O((v-v_0)^{1/k_{j'}})\Big). \end{aligned}$$

The last equality is by (47); it gives rise to the following

Proposition 9.3. *Let $t \in M^\infty(N)$ with $n := \operatorname{pord} t \ge 1$, let $f \in M^\infty(N)$ be such that $\gcd(n, \operatorname{pord} f) = 1$. For $v_0 \in \mathbb{C}$ suppose that*

$t^*(x) = v_0$ has $\ell \le n$ pairwise distinct solutions $x_1 = [\tau_1]_N, \dots, x_\ell = [\tau_\ell]_N$ with multiplicities $k_1, \dots, k_\ell$, respectively. (I.e., $k_1 + \cdots + k_\ell = n$.)

If

$$\text{the values } f(\tau_1), \dots, f(\tau_\ell) \text{ are pairwise distinct,} \tag{48}$$

and

$$f'(\tau_1) \neq 0, \dots, f'(\tau_\ell) \neq 0, \tag{49}$$

then there exists a polynomial $p(x) \in \mathbb{C}[x]$ such that for all $v \in \mathbb{C}$:

$$D_t(f)(v) = (v-v_0)^{n-\ell} p(v) \text{ where } p(v_0) \neq 0. \tag{50}$$

Proof. The statement follows from the last equality of the derivation preceding this proposition. Namely, under the condition (48) the second product on the right side of this equality is non-zero for $v = v_0$. Condition (49) means that $b_{j,1} \neq 0$ in (46), thus $c_{j,1} \neq 0$ for $j = 1, \dots, \ell$ in (47). Consequently, from the first product in the expression under consideration one can pull out $v - v_0$ as follows:

$$\begin{aligned} &c_{1,1} \prod_{1\le k,k'\le k_1, k\neq k'} (\zeta_{k_1}^k - \zeta_{k_1}^{k'})(v-v_0)^{1/k_1} \dots c_{\ell,1} \prod_{1\le k,k'\le k_\ell, k\neq k'} (\zeta_{k_\ell}^k - \zeta_{k_\ell}^{k'})(v-v_0)^{1/k_\ell} \\ &\quad = \text{constant} \cdot (v-v_0)^{2\binom{k_1}{2}\frac{1}{k_1} + \cdots + 2\binom{k_\ell}{2}\frac{1}{k_\ell}}. \end{aligned}$$

Recalling that $k_1 + \cdots + k_l = n$ completes the proof for all $v \in V$ where V is an open subset of a neighborhood V_0 of v_0 such that V does not contain v_0. But invoking the identity theorem from complex analysis the statement extends to all $v \in \mathbb{C}$. □

Properties (48) and (49) are sufficiently important to deserve a

Definition 9.4 (separation property)**.** *Let $t \in M^\infty(N)$ with $n := \operatorname{pord} t \geq 1$, let $f \in M^\infty(N)$ be such that $\gcd(n, \operatorname{pord} f) = 1$. For $v_0 \in \mathbb{C}$ suppose that*

$t^*(x) = v_0$ *has $\ell \leq n$ pairwise distinct solutions $x_1 = [\tau_1]_N, \ldots, x_\ell = [\tau_\ell]_N$.*

We say that f has the separation property for (t, v_0) if f satisfies (48) *and* (49)*.*

Remark 9.5. In Section 14 we describe how to construct such f having the separation property.

An immediate consequence of Prop. 9.3(50) is

Corollary 9.6. *Let f have the separation property for (t, β) with $\beta \in \mathbb{C}$. Then*

$$D_t(f)(\beta) = 0 \;\Leftrightarrow\; \beta \in \operatorname{BranchPts}(t^*). \tag{51}$$

Another consequence of our analysis above is

Proposition 9.7. *Let $t \in M^\infty(N)$ with $n := \operatorname{pord} t \geq 1$, let $f \in M^\infty(N)$ be such that $\gcd(n, \operatorname{pord} f) = 1$. For $v_0 \in \mathbb{C}$ suppose that*

$t^*(x) = v_0$ *has $\ell \leq n$ pairwise distinct solutions $x_1 = [\tau_1]_N, \ldots, x_\ell = [\tau_\ell]_N$*

with multiplicities $k_1, \ldots, k_\ell$, respectively. (I.e., $k_1 + \cdots + k_\ell = n$).

For complex numbers $a_0, \ldots, a_{n-1}$, not all zero, define a meromorphic function on $\mathbb{H}$ by

$$F(\tau) := \frac{a_0 + a_1 f(\tau) + \cdots + a_{n-1} f(\tau)^{n-1}}{t(\tau) - v_0}.$$

If f has the separation property for (t, v_0), then[6]

$$F(\tau_j) = \infty \text{ for some } j \in \{1, \ldots, \ell\}. \tag{52}$$

Proof. Suppose F^* is analytic in $X_0(N) \setminus \{[\infty]_N\}$. Then, assuming the setting as above, by (43) one has for all $\tau \in U_1$ a series expansion

$$\begin{aligned} a_0 + a_1 f(\tau) + \cdots + a_{n-1} f(\tau)^{n-1} &= (t(\tau) - v_0) F(\tau) \\ &= (a_{1,0} \phi_{\tau_1}(\tau)^{k_1} + a_{1,1} \phi_{\tau_1}(\tau)^{k_1+1} + \ldots)(F_0 + F_1 \phi_{\tau_1}(\tau) + \ldots) \end{aligned} \tag{53}$$

with $a_{1,0} \neq 0$. Hence owing to (40),

$$a_0 + a_1 f(\tau_1) + \cdots + a_{n-1} f(\tau_1)^{n-1} = 0,$$

[6] Note that the $\tau_j \in \mathbb{H} \cup \mathbb{Q}$ are such that $[\tau_j]_N \neq [\infty]_N$. Hence (52) implies that $F \notin M^\infty(N)$.

which implies a factorization

$$\begin{aligned} &a_0 + a_1 f(\tau) + \cdots + a_{n-1} f(\tau)^{n-1} \\ &\quad = (f(\tau) - f(\tau_1))(A_0 + A_1 f(\tau) + \cdots + A_{n-2} f(\tau)^{n-2}) \\ &\quad = (b_{1,0}\phi_{\tau_1}(\tau) + b_{1,1}\phi_{\tau_1}(\tau)^2 + \dots)(A_0 + A_1 f(\tau) + \cdots + A_{n-2} f(\tau)^{n-2}), \end{aligned}$$

where the last equality is by (46) with $b_{1,0} \neq 0$ owing to (49). As a consequence of (53), if $k_1 > 1$:

$$A_0 + A_1 f(\tau_1) + \cdots + A_{n-2} f(\tau_1)^{n-2} = 0,$$

and by iteration,

$$\begin{aligned} &a_0 + a_1 f(\tau) + \cdots + a_{n-1} f(\tau)^{n-1} \\ &\quad = (f(\tau) - f(\tau_1))^{k_1}(B_0 + B_1 f(\tau) + \cdots + B_{n-1-k_1} f(\tau)^{n-1-k_1}). \end{aligned}$$

Notice that if

$$B(x) := B_0 + B_1 x + \cdots + B_{n-1-k_1} x^{n-1-k_1}$$

is the zero-polynomial (e.g., if $k_1 = n$), the assumption that $(1, f, \dots, f^{n-1})$ is an order-complete basis would imply that all $a_j = 0$, and the proof would stop with this contradiction.

Using the same argument, one derives

$$\begin{aligned} &a_0 + a_1 f(\tau) + \cdots + a_{n-1} f(\tau)^{n-1} \\ &\quad = (f(\tau) - f(\tau_2))^{k_2}(C_0 + C_1 f(\tau) + \cdots + C_{n-1-k_2} f(\tau)^{n-1-k_2}), \end{aligned}$$

etc, up to

$$\begin{aligned} &a_0 + a_1 f(\tau) + \cdots + a_{n-1} f(\tau)^{n-1} \\ &\quad = (f(\tau) - f(\tau_\ell))^{k_\ell}(D_0 + D_1 f(\tau) + \cdots + D_{n-1-k_\ell} f(\tau)^{n-1-k_\ell}). \end{aligned}$$

If one of the polynomial factors in the role of $B(x)$ above would be the zero polynomial, we are done. Otherwise, invoking condition (48) implies that

$$\begin{aligned} &(f(\tau) - f(\tau_1))^{k_1} \dots (f(\tau) - f(\tau_\ell))^{k_\ell} \text{ divides} \\ &\qquad a_0 + a_1 f(\tau) + \cdots + a_{n-1} f(\tau)^{n-1}. \end{aligned}$$

Recalling that not all the a_j are zero and $k_1 + \cdots + k_\ell = n$, we obtain a contradiction to the assumption that F^* is analytic in $X_0(N) \setminus \{[\infty]_N\}$. □

Corollary 9.8. *Let $t \in M^\infty(N)$ with $n := \operatorname{pord} t \geq 1$, let $f \in M^\infty(N)$ be such that $\gcd(n, \operatorname{pord} f) = 1$. For $v_0 \in \mathbb{C}$ suppose that*

$$t^*(x) = v_0 \text{ has } \ell \leq n \text{ pairwise distinct solutions. } x_1 = [\tau_1]_N, \dots, x_\ell = [\tau_\ell]_N.$$

For complex numbers $a_0, \dots, a_{n-1}$ define a meromorphic function on $\mathbb{H}$ by

$$F(\tau) := \frac{a_0 + a_1 f(\tau) + \cdots + a_{n-1} f(\tau)^{n-1}}{t(\tau) - v_0}.$$

If f has the separation property for (t, v_0), then:

$$F \in M^\infty(N) \Rightarrow F = 0.$$

Proof. If one of the a_j would be non-zero, Prop. 9.7 would imply a pole of F^* at some $[\tau_j]_N \neq [\infty]_N$, $\tau_j \in \mathbb{H} \cup \mathbb{Q}$. □

10. Order-reduction and discriminant polynomials

In this section we relate discriminant polynomials to order-reduction polynomials associated to integral bases. Throughout this section, let $t \in M^\infty(N)$ with $n := \operatorname{pord} t \geq 1$, let $(1, b_1, \ldots, b_{n-1})$, $b_j \in M^\infty(N)$, be an order-complete tuple forming an an integral basis for $M^\infty(N)$ over $\mathbb{C}[t]$; i.e,

$$\langle 1, b_1, \ldots, b_{n-1} \rangle_{\mathbb{C}[t]} = M^\infty(N). \tag{54}$$

Moreover, let $f \in M^\infty(N)$ again be chosen such that $\gcd(n, \operatorname{pord} f) = 1$. By Prop. 3.5 such an f gives rise to an order-complete basis $(1, f, \ldots, f^{n-1})$ of the $\mathbb{C}[t]$-module

$$\langle 1, f, f^2 \ldots, f^{n-1} \rangle_{\mathbb{C}[t]} = \mathbb{C}[t, f] \subseteq M^\infty(N).$$

By exemplifying the case for $n = 3$, we shall see how the discriminant polynomial

$$D_t(f)(v) := D_t(1, f, f^2, \ldots, f^{n-1})(v)$$

is related to the order-reduction polynomial

$$D_t(1, b_1, \ldots, b_{n-1})(v).$$

By the identity theorem from complex analysis, it is sufficient to consider the situation for v from a neighborhood V of $v_0 \in V$. With the setting as in (22), one has

$$\begin{pmatrix} 1 & 0 & 0 \\ r_0^{(1)}(v) & r_1^{(1)}(v) & r_2^{(1)}(v) \\ r_0^{(2)}(v) & r_1^{(2)}(v) & r_2^{(2)}(v) \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ (b_1 \circ T_1)(v) & (b_1 \circ T_2)(v) & (b_1 \circ T_3)(v) \\ (b_2 \circ T_1)(v) & (b_2 \circ T_2)(v) & (b_2 \circ T_3)(v) \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 1 & 1 \\ f(T_1(v)) & f(T_2(v)) & f(T_3(v)) \\ f(T_1(v))^2 & f(T_2(v))^2 & f(T_3(v))^2 \end{pmatrix},$$

because owing to (54) there exist polynomials $r_j^{(i)}(x) \in \mathbb{C}[x]$ such that

$$f(\tau)^i = r_0^{(i)}(t(\tau)) + r_1^{(i)}(t(\tau))\ b_1(\tau) + r_2^{(i)}(t(\tau))\ b_2(\tau),\ \tau \in \mathbb{H}.$$

This implies

$$f(T_j(v))^i = r_0^{(i)}(v) + r_1^{(i)}(v)(b_1 \circ T_j)(v) + r_2^{(i)}(v)(b_2 \circ T_j)(v)$$

using

$$t(T_j(v)) = t((t \mid U_j)^{-1}(v)) = v.$$

Taking determinants of both sides of the matrix equation squared, this gives for the general case,

$$\text{as polynomials in } v: \ D_t(1, b_1, \ldots, b_{n-1})(v) \text{ divides } D_t(f)(v). \tag{55}$$

Next we consider the other direction. By Prop. 4.3 there exist polynomials $q_j(x)$ and $p_i(x)$ in $\mathbb{C}[x]$ such that

$$b_j = \frac{p_0^{(j)}(t)}{q_j(t)} + \frac{p_1^{(j)}(t)}{q_j(t)} f + \cdots + \frac{p_{n-1}^{(j)}(t)}{q_j(t)} f^{n-1}, \ j = 1, \ldots, n-1, \tag{56}$$

where $q_j(t)$ is either a constant or such that

$$\gcd(q_j(x), p_0^{(j)}(x), \ldots, p_{n-1}^{(j)}(x)) = 1. \tag{57}$$

As before this can be expressed as a matrix equation. We display the case $n = 3$:

$$\begin{pmatrix} 1 & 0 & 0 \\ s_0^{(1)}(v) & s_1^{(1)}(v) & s_2^{(1)}(v) \\ s_0^{(2)}(v) & s_1^{(2)}(v) & s_2^{(2)}(v) \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ f(T_1(v)) & f(T_2(v)) & f(T_3(v)) \\ f(T_1(v))^2 & f(T_2(v))^2 & f(T_3(v))^2 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 1 & 1 \\ (b_1 \circ T_1)(v) & (b_1 \circ T_2)(v) & (b_1 \circ T_3)(v) \\ (b_2 \circ T_1)(v) & (b_2 \circ T_2)(v) & (b_2 \circ T_3)(v) \end{pmatrix},$$

where

$$s_i^{(j)}(v) := \frac{p_i^{(j)}(v)}{q_j(v)}.$$

Again taking determinants of both sides of the matrix equation squared, for the general case this gives another polynomial relation in v:

$$D_t(1, b_1, \ldots, b_{n-1})(v) = \frac{s(v)^2}{q_1(v)^2 \ldots q_{n-1}(v)^2} D_t(f)(v)$$

where $s(x), q_1(x), \ldots, q_{n-1}(x)$ are polynomials in $\mathbb{C}[x]$. It will be convenient to cancel out possible common factors and to write, as polynomials in $\mathbb{C}[x]$,

$$D_t(1, b_1, \ldots, b_{n-1})(x) = \frac{S(x)^2}{Q_1(x)^2 \ldots Q_{n-1}(x)^2} \ D_t(f)(x), \tag{58}$$

such that

$$S(x) \text{ and } Q_1(x) \ldots Q_{n-1}(x) \text{ are relatively prime polynomials,} \tag{59}$$

and

$$Q_j(x) \text{ divides } q_j(x), \ j = 1, \ldots, n-1, \tag{60}$$

where the $q_j(x)$ are determined as in (56).

11. Order-reduction polynomials: further results

In this section we continue the considerations made in the previous section. Again, $t \in M^\infty(N)$ with $n := \operatorname{pord} t \geq 1$, and $(1, b_1, \ldots, b_{n-1})$ with $b_j \in M^\infty(N)$ is assumed to be an integral basis for $M^\infty(N)$ over $\mathbb{C}[t]$.

Lemma 11.1. *Let $(1, \beta_1, \ldots, \beta_{n-1})$ with $\beta_j \in M^\infty(N)$ be an integral bases for $M^\infty(N)$ over $\mathbb{C}[t]$. Then there exists a $c \in \mathbb{C}$ such that*

$$D_t(1, b_1, \ldots, b_{n-1})(x) = c \cdot D_t(1, \beta_1, \ldots, \beta_{n-1})(x).$$

Proof. Applying the same kind of argument as used to derive (55), we obtain the polynomial relations

$$D_t(1, b_1, \ldots, b_{n-1})(x) \text{ divides } D_t(1, \beta_1, \ldots, \beta_{n-1})(x) \tag{61}$$

and

$$D_t(1, \beta_1, \ldots, \beta_{n-1})(x) \text{ divides } D_t(1, b_1, \ldots, b_{n-1})(x). \tag{62}$$

This proves the statement. □

Another application of the argument we used to derive (55) is the existence of some polynomial $R(x) \in \mathbb{C}[x]$ such that,

$$R(x)^2 \; D_t(1, b_1, \ldots, b_{n-1})(x) = D_t(f)(x).$$

This, using (58), implies

$$\frac{R(x)S(x)}{Q_1(x) \ldots Q_{n-1}(x)} = 1 \text{ or } -1.$$

Finally, as a consequence of (59) we obtain

$$R(x) = \frac{1}{c} \cdot Q_1(x) \ldots Q_{n-1}(x) \text{ and } S(x) = c \text{ for some non-zero } c \in \mathbb{C}. \tag{63}$$

We summarize,

Lemma 11.2. *There is a $c \in \mathbb{C}$ such that*

$$D_t(f)(x) = c \cdot Q_1(x)^2 \ldots Q_{n-1}(x)^2 \; D_t(1, b_1, \ldots, b_{n-1})(x), \tag{64}$$

where for $j = 1, \ldots, n-1$, the polynomials $Q_j(x)$ divide the polynomials $q_j(x)$ which are determined as in (56).

Lemma 11.3. *Let $Q_j(x)$ be the polynomials as in Lemma 11.2. Suppose f has the separation property for (t, β) for some $\beta \in \mathbb{C}$. Then*

$$Q_j(\beta) \neq 0 \text{ for all } j = 1, \ldots, n-1.$$

Proof. Suppose $x-\beta \mid Q_j(x)$ for some $j \in \{1,\dots,n-1\}$. By Lemma 11.2, $Q_j(x) \mid q_j(x)$ with $q_j(x)$ as in relation (56). Hence $x-\beta$ divides $q_j(x)$, and (56) can be rewritten as

$$\frac{q_j(t)}{t-\beta}\, b_j = \frac{p_0^{(j)}(t)}{t-\beta} + \frac{p_1^{(j)}(t)}{t-\beta} f + \cdots + \frac{p_{n-1}^{(j)}(t)}{t-\beta} f^{n-1}.$$

As in the proof of Cor. 4.4, by division with remainder there are polynomials $p_l(x) \in \mathbb{C}[x]$ and $a_l \in \mathbb{C}$ such that $p_l^{(j)}(x) = (x-\beta)p_l(x) + a_l$, $l = 0,\dots,n-1$. This means,

$$\begin{aligned}\frac{q_j(t)}{t-\beta}\, b_j = &\frac{a_0 + a_1 f + \cdots + a_{n-1} f^{n-1}}{t-\beta} \\ &+ p_0(t) + p_1(t) f + \cdots + p_{n-1}(t) f^{n-1} \in M^\infty(N).\end{aligned}$$

Owing to the fact that f has the separation property for (t,β), one has by Corollary 9.8,

$$\frac{a_0 + a_1 f + \cdots + a_{n-1} f^{n-1}}{t-\beta} = 0.$$

Iterating this argument cancels out all powers of $t-\beta$ and one arrives at a representation of b_j of the form

$$Q(t)\; b_j = P_0(t) + P_1(t) f + \cdots + P_{n-1}(t) f^{n-1}$$

with polynomials $P_l(x)$ and $Q(x)$ such that

$$x-\beta \nmid Q(x). \tag{65}$$

Comparing this to the representation (56), which rewrites as

$$q_j(t)\; b_j = p_0^{(j)}(t) + p_1^{(j)}(t) f + \cdots + p_{n-1}^{(j)}(t) f^{n-1},$$

produces a contradiction to the uniqueness of basis representation since in contrast to (65), $x-\beta$ divides the denominator polynomial $q_j(x)$. □

Proposition 11.4. *For any $\beta \in \mathbb{C}$:*

$$D_t(1, b_1, \dots, b_{n-1})(\beta) = 0 \;\Leftrightarrow\; \beta \in \mathrm{BranchPts}(t^*). \tag{66}$$

Proof. For the proof we choose f having the separation property for (t,β).[7] For the "⇒" direction of the statement, suppose $D_t(1, b_1, \dots, b_{n-1})(\beta) = 0$. Then (64) implies $D_t(f)(\beta) = 0$ which, owing to Cor. 9.6, is true if and only if $\beta \in \mathrm{BranchPts}(t)$. For the other direction we use the reverse direction of this "if and only if" relation: $\beta \in \mathrm{BranchPts}(t^*)$ implies $x-\beta \mid D_t(f)(x)$. Next we apply Lemma 11.3 to the equation (58) and obtain

$$x-\beta \mid D_t(1, b_1, \dots, b_{n-1})(x),$$

which completes the proof. □

[7] How to construct such f is described in Section 14.

From all this we obtain the complete factorization of order-reduction polynomials of integral bases. To state it, it is convenient to define

$$\mathrm{BranchPts}_{\mathbb{C}}(t^*) := \mathrm{BranchPts}(t^*) \cap \mathbb{C},$$

in order to keep the point ∞ out, as the image of the only pole at $[\infty]_N$.

Proposition 11.5. *Let $t \in M^\infty(N)$ with $n := \operatorname{pord} t \geq 1$ and $(1, b_1, \ldots, b_{n-1})$ with $b_j \in M^\infty(N)$ be an integral basis for $M^\infty(N)$ over $\mathbb{C}[t]$. Then there exists a $c \in \mathbb{C}$ and positive integers m_β such that*

$$D_t(1, b_1, \ldots, b_{n-1})(x) = c \cdot \prod_{\beta \in \mathrm{BranchPts}_{\mathbb{C}}(t^*)} (x - \beta)^{m_\beta}. \tag{67}$$

Moreover, for any $\beta \in \mathrm{BranchPts}_{\mathbb{C}}(t^*)$ suppose that $t^*(x) = \beta$ has

$\ell(\beta) < n$ pairwise distinct solutions $x_1^{(\beta)} = [\tau_1^{(\beta)}]_N, \ldots, x_{\ell(\beta)}^{(\beta)} = [\tau_{\ell(\beta)}^{(\beta)}]_N$
with multiplicities $k_1^{(\beta)}, \ldots, k_{\ell(\beta)}^{(\beta)}$, respectively. (I.e., $k_1^{(\beta)} + \cdots + k_{\ell(\beta)}^{(\beta)} = n$.)

Then

$$m_\beta = n - \ell(\beta). \tag{68}$$

Proof. The factorization (67) is immediate from Prop. 11.4. To prove (68) let $\beta \in \mathrm{BranchPts}_{\mathbb{C}}(t^*)$ be a branch point of the kind as stated. Choose f to have the separation property for (t, β). Then (50) implies the existence of a polynomial $p(x) \in \mathbb{C}[x]$ such that

$$D_t(f)(x) = (x - \beta)^{n - \ell(\beta)} p(x) \text{ where } p(\beta) \neq 0.$$

According to (64) there exist polynomials $Q_j(x)$ such that

$$D_t(f)(x) = c \cdot Q_1(x)^2 \ldots Q_{n-1}(x)^2 \; D_t(1, b_1, \ldots, b_{n-1})(x)$$

and, owing to Lemma 11.3,

$$Q_j(\beta) \neq 0 \text{ for all } j = 1, \ldots, n-1.$$

Hence $(x - \beta)^{n-\ell(\beta)}$ divides $D_t(1, b_1, \ldots, b_{n-1})(x)$ with maximal power, which proves (68). □

For the next consideration we again have to use the charts as in (37), (38), and (39). In the setting of Proposition 11.5 one has:

$$\begin{aligned}
D_t(1,b_1,\dots,b_{n-1})(x) &= c\cdot \prod_{\beta\in \mathrm{BranchPts}_{\mathbb{C}}(t^*)} (x-\beta)^{k_1^{(\beta)}+\cdots+k_{\ell(\beta)}^{(\beta)}-\ell(\beta)} \\
&= c\cdot \prod_{\beta\in \mathrm{BranchPts}_{\mathbb{C}}(t^*)} (x-\beta)^{k_1^{(\beta)}-1}\dots(x-\beta)^{k_{\ell(\beta)}^{(\beta)}-1} \\
&= c\cdot \prod_{\beta\in \mathrm{BranchPts}_{\mathbb{C}}(t^*)} (x-t(\tau_1^{(\beta)}))^{k_1^{(\beta)}-1}\dots(x-t(\tau_{\ell(\beta)}^{(\beta)}))^{k_{\ell(\beta)}^{(\beta)}-1} \\
&= c\cdot \prod_{\beta\in \mathrm{BranchPts}_{\mathbb{C}}(t^*)} \prod_{j=1}^{\ell(\beta)} (x-t(\tau_j^{(\beta)}))^{-1+\mathrm{mult}_{[\tau_j^{(\beta)}]_N}(\tau^*)} \\
&= c\cdot \prod_{\substack{\text{all orbits } [\tau_0]_N\in X_0(N),\\ [\tau_0]_N\neq[\infty]_N}} (x-t(\tau_0))^{-1+\mathrm{mult}_{[\tau_0]_N}(\tau^*)},
\end{aligned}$$

where the last line is by the fact that if $t(\tau_0)\notin \mathrm{BranchPts}(t^*)$ then

$$-1+\mathrm{mult}_{[\tau_0]_N}(\tau^*)=0.$$

Here we use the notion of multiplicity $\mathrm{mult}_x(f)$, also expained in Section 16, which stands for the multiplicity at the point $x\in X$ of a meromorphic function f on a (compact) Riemann surface X. For $x_0=[\tau_0]_N\in X_0(N)$, one has (e.g., [10, Lemma 4.7] and [4, Sec. 2.4]) with respect to our charts $\phi_{\tau_0}(\tau)$ centered at 0:[8]

$$\mathrm{mult}_{x_0}(t^*)=\begin{cases}\mathrm{ord}_{\phi_{\tau_0}(\tau)}(t(\tau)-t(\tau_0)) & ,\text{if } [\tau_0]_N \text{ is no pole of } t^*\\ -\mathrm{ord}_{\phi_{\tau_0}(\tau)}\, t(\tau) & ,\text{if } [\tau_0]_N \text{ is a pole of } t^*\end{cases}. \tag{69}$$

Hence we obtain from Proposition 11.5 the

Corollary 11.6. *Let $t\in M^\infty(N)$ with $n:=\mathrm{pord}\, t\geq 1$ and $(1,b_1,\dots,b_{n-1})$ with $b_j\in M^\infty(N)$ be an integral basis for $M^\infty(N)$ over $\mathbb{C}[t]$. Then*

$$\deg_x D_t(1,b_1,\dots,b_{n-1})(x)=\sum_{\substack{x_0\in X_0(N),\\ x_0\neq[\infty]_N}}(-1+\mathrm{mult}_{x_0}(t^*)).$$

Next, recall from Section 16 the definition of $\mathrm{Deg}(f)$, the degree of a meromorphic function f on a compact Riemann surface X:

$$\mathrm{Deg}(f):=\sum_{x\in f^{-1}(v)}\mathrm{mult}_x(f) \text{ where } v \text{ is any element in } \hat{\mathbb{C}}.$$

[8] I.e., $\phi_{\tau_0}(\tau_0)=0$.

Choosing $v := \infty$ we have $\mathrm{Deg}(t^*) = n$. Let

$$g(X) := \text{ genus of a compact Riemann surface } X.$$

Recall the Riemann-Hurwitz formula [10, Thm. 4.16][9] for a non-constant holomorphic map $F : X \to Y$ between compact Riemann surfaces:

$$2\ g(X) - 2 = \mathrm{Deg}(F)(2\ g(Y) - 2) + \sum_{x \in X} (\mathrm{mult}_x(F) - 1). \tag{70}$$

Now we apply this to our setting where $X := X_0(N)$ and $F := t^* : X_0(N) \to \hat{\mathbb{C}}$. Owing to $g(\hat{\mathbb{C}}) = 0$, together with (69) and Cor. 11.6, this gives:

$$\begin{aligned} 2\ g(X_0(N)) - 2 &= -2n + \sum_{x \in X_0(N)} (\mathrm{mult}_x(F) - 1) \\ &= -2n + \sum_{\substack{x_0 \in X_0(N), \\ x_0 \neq [\infty]_N}} (\mathrm{mult}_{x_0}(t^*) - 1) + \mathrm{pord}\, t - 1 \\ &= -n - 1 + \deg_x D_t(1, b_1, \ldots, b_{n-1})(x). \end{aligned}$$

We summarize in

Corollary 11.7. *Let $t \in M^\infty(N)$ with $n := \mathrm{pord}\, t \geq 1$ and $(1, b_1, \ldots, b_{n-1})$ with $b_j \in M^\infty(N)$ be an integral basis for $M^\infty(N)$ over $\mathbb{C}[t]$. Then*

$$\deg_x D_t(1, b_1, \ldots, b_{n-1})(x) = 2\ g(X_0(N)) + n - 1. \tag{71}$$

12. Proof of the Weierstrass Gap Theorem

In this section we prove the gap theorem for modular functions in $M^\infty(N)$.

Definition 12.1 (gaps in modular function algebras)**.** *Let M be a subalgebra of $M^\infty(N)$, the modular functions for $\Gamma_0(N)$ which are holomorphic in $\mathbb{H}$ and with a pole at ∞. A positive integer n is called a gap in M, if there is no $f \in M$ with $\mathrm{pord}\, f = n$. We also define the gap number g_M as the total number of gaps in M; i.e.,*

$$g_M := \#\{n \in \mathbb{Z}_{>0} : n \text{ is a gap of } M\}.$$

In this section we prove the gap theorem in the following version:

Theorem 12.2 (Weierstraß gap theorem for $X_0(N)$)**.** *Let $g := g(X_0(N))$ be the genus of $X_0(N)$. If $g \geq 1$ then $M^\infty(N)$ has exactly g gaps n_j with*

$$1 = n_1 < \cdots < n_g \leq 2g - 1. \tag{72}$$

If $g = 0$ then $M^\infty(N)$ has no gap; i.e., there exists an $h \in M^\infty(N)$ such that $\mathrm{pord}\, h = 1$.[10]

[9] Actually the special case we need, $Y = \hat{\mathbb{C}}$, was given by Riemann; e.g., [3].

[10] This means, in this case one has $M^\infty(N) = \mathbb{C}[h]$.

To prepare for the proof, we determine the gap number $g_{\mathbb{C}[t,f]}$, where $t, f \in M^\infty(N)$ with $n := \operatorname{pord} t \geq 2$, $l := \operatorname{pord} f \geq 2$, and $\gcd(l,n) = 1$. To construct such functions with relatively prime pole orders is straightforward; see, for instance, Example 2.3. By Prop. 3.5 we know that

$$\mathbb{C}[t,f] = \langle 1, f, f^2, \dots, f^{n-1} \rangle_{\mathbb{C}[t]},$$

where $(1, f, f^2, \dots, f^{n-1})$ is an order-complete module basis. Hence there are $l_j \in \mathbb{Z}_{\geq 0}$ such that

$$\begin{aligned}\{\operatorname{pord} f, \operatorname{pord} f^2, \dots, \operatorname{pord} f^{n-1}\} &= \{l, 2l, \dots, (n-1)l\} \\ &= \{l_1 n + 1, l_2 n + 2, \dots, l_{n-1} n + n - 1\}.\end{aligned}$$

Thus inspecting each of the residue classes modulo n for $j \in \{1, \dots, n-1\}$ makes clear that one cannot find any function of pole order

$$j, n + j, \dots, (l_j - 1)n + j \ \text{ if } \ l_j > 0.$$

in $\mathbb{C}[t,f]$. Hence for fixed j, l_j pole orders are missing; summing j from 1 to $n-1$ gives the total number of missing pole orders of functions in $\mathbb{C}[t,f]$:

$$\begin{aligned}l_1 + l_2 + \cdots + l_{n-1} &= \left\lfloor \frac{l_1 n + 1}{n} \right\rfloor + \left\lfloor \frac{l_2 n + 2}{n} \right\rfloor + \cdots + \left\lfloor \frac{l_{n-1} n + n - 1}{n} \right\rfloor \\ &= \sum_{j=1}^{n-1} \left\lfloor \frac{j\ l}{n} \right\rfloor = \frac{(l-1)(n-1)}{2},\end{aligned}$$

where the last equality is by [7, (3.32)]. We summarize in

Lemma 12.3. *Let $t, f \in M^\infty(N)$ with $n := \operatorname{pord} t \geq 1$, $l := \operatorname{pord} f \geq 1$, and $\gcd(l,n) = 1$. Then the total number of missing pole orders of functions in $\mathbb{C}[t,f]$ is*

$$\frac{(l-1)(n-1)}{2}.$$

Proof. If $n = 1$ or $\ell = 1$ then $\mathbb{C}[t,f] = M^\infty(N)$; i.e., there is no gap. The case both n and ℓ greater or equal to 2 was treated above. □

Proof of the gap Theorem 12.2. Recalling Def. 4.5, each pole-order-reduction step associated to some $\alpha \in \mathbb{C}$,

$$(1, \dots, \beta_{k-1}, \beta_k, \beta_{k+1}, \dots) \to (1, \dots, \beta_{k-1}, h_\alpha, \beta_{k+1}, \dots)$$

between order-complete bases

(i) by Cor. 4.4(18) reduces the total number of gaps by exactly one;

(ii) by Prop. 8.1(35) reduces the degree of the order-reduction polynomial by exactly two.

The gap theorem now will be proved by successively applying pole-order-reduction steps to the order-complete basis $(1, f, \ldots, f^{n-1})$ of $\mathbb{C}[t, f]$ where t and f are chosen from $M^\infty(N)$ such that $n := \operatorname{pord} t \geq 2$, $l := \operatorname{pord} f \geq 2$, and $\gcd(l, n) = 1$. Such a pair (t, f) can be easily constructed; see, for instance, Example 2.3.

Suppose that after r reduction steps we arrive at the integral basis $(1, b_1, \ldots, b_{n-1})$ of $M^\infty(N)$. Defining

$$d_f := \deg_x D_t(f)(x) \text{ and } d_b := \deg_x D_t(1, b_1, \ldots, b_{n-1})(x),$$

the reduction observation (ii) made above gives

$$d_b = d_f - 2r; \tag{73}$$

furthermore, reduction observation (i) implies for the gap numbers

$$g_{M^\infty(N)} = g_{\mathbb{C}[t,f]} - r. \tag{74}$$

Combining (73) and (74) gives the desired Weierstrass estimate for the total number of gaps in $M^\infty(N)$ in terms of the genus g:

$$\begin{aligned} g_{M^\infty(N)} &= g_{\mathbb{C}[t,f]} - \frac{1}{2}(d_f - d_b) && \text{(by (73), (74))} \\ &= \frac{1}{2}((n-1)(l-1) - d_f + d_b) && \text{(by Lemma 12.3)} \\ &= \frac{1}{2}(-(n-1) + d_b) && \text{(by (32))} \\ &= \frac{1}{2}(-(n-1) + n - 1 + 2g(X_0(N))) && \text{(by (71))} \\ &= g(X_0(N)) = g. \end{aligned}$$

Hence we proved that $M^\infty(N)$ has exactly g gaps. If $g = 0$ there are no gaps; i.e., in this case, after relabelling indices,

$$M^\infty(N) = \langle 1, b_1, \ldots, b_{n-1} \rangle_{\mathbb{C}[t]} \text{ with } \operatorname{pord} b_j = j, j = 1, \ldots, n-1.$$

Hence $M^\infty(N) = \mathbb{C}[h]$ for $h := b_1$.

To prove the remaining part of the gap theorem, namely the bound (72) for the the gaps $\{n_1 = 1, n_2, \ldots, n_g\}$ where $g \geq 1$, we will use a general combinatorial argument. Notice that $n_1 = 1$ because otherwise there would be no gap which, as we proved, is only possible if $g = 0$.

To prepare for the combinatorial argument, recall that after choosing t and f from $M^\infty(N)$ as above, by applying pole-order-reduction steps, we arrived, after relabelling indices, at an integral basis $(1, b_1, \ldots, b_{n-1})$ for $M^\infty(N)$ where $\operatorname{pord} b_j \equiv j \pmod{n}$, $j = 1, \ldots, n-1$. Defining

$$r_1 := \operatorname{pord} b_1, \ldots, r_{n-1} := \operatorname{pord} b_{n-1},$$

this basis gives rise to the additive submonoid

$$S := (0 + n\mathbb{Z}_{\geq 0}) \cup (r_1 + n\mathbb{Z}_{\geq 0}) \cup \cdots \cup (r_{n-1} + n\mathbb{Z}_{\geq 0})$$

of $(\mathbb{Z}_{\geq 0}, +)$ which describes the gap set of $M^\infty(N)$:

$$\mathbb{Z}_{\geq 0} \setminus S = \{n_1 = 1, n_2, \ldots, n_g\}.$$

Let $m+1$ be the smallest non-gap of $M^\infty(N)$; $m \geq 1$ owing to $n_1 = 1$.

To prove the desired bound (72) for the gap sizes n_j we change the representation of the monoid S with respect to $m+1$. Namely, it is easy to see that there exist positive integers $s_1, \ldots, s_m \in \mathbb{Z}_{>0}$ such that $s_j \equiv j \pmod{m+1}$ for all $j \in \{1, \ldots, m\}$ and

$$S = (0 + (m+1)\mathbb{Z}_{\geq 0}) \cup (s_1 + (m+1)\mathbb{Z}_{\geq 0}) \cup \cdots \cup (s_m + (m+1)\mathbb{Z}_{\geq 0}).$$

In Section 13 we denote the number of gaps in a monoid S by $\gamma(S)$. Hence in the given context, $g = \gamma(S)$. Recall that $m+1$ is chosen to be the smallest non-gap of $M^\infty(N)$. Therefore we choose a monoid representation with respect to $m+1$. Concretely, in this case there are $k_j \in \mathbb{Z}_{>0}$ such that

$$s_j = j + (m+1)k_j \text{ for } j = 1, \ldots, m,$$

Now the monoid gap Lemma 13.1 implies

$$2\,\gamma(S) - 1 \geq j + (m+1)(k_j - 1),\ j = 1, \ldots, m.$$

Since $j + (m+1)(k_j - 1)$ are the largest non-gaps in each residue class modulo $m+1$, this proves the bound given in (72), and the proof of the Weierstrass gap Theorem 12.2 is completed. □

13. A gap property of monoids

Let $m \in \mathbb{Z}_{>0}$ and $s_1, \ldots, s_m \in \mathbb{Z}_{>0}$ such that $s_j \equiv j \pmod{m+1}$ for all $j \in \{1, \ldots, m\}$. We consider the additive submonoid

$$S := (0 + (m+1)\mathbb{Z}_{\geq 0}) \cup (s_1 + (m+1)\mathbb{Z}_{\geq 0}) \cup \cdots \cup (s_m + (m+1)\mathbb{Z}_{\geq 0})$$

of $(\mathbb{Z}_{\geq 0}, +)$. A positive integer $\ell \notin S$ is called a gap of S.[11] Let $\gamma(S)$ be the total number of gaps of S. Relating to our proof setting in Section 12, we choose this representation of S under the assumption that $m+1$ is the smallest non-gap of S. By the definition of S there are *positive* integers k_j such that

$$s_j = j + (m+1)k_j \text{ for } j = 1, \ldots, m.$$

An easy count gives

$$\gamma(S) = k_1 + \cdots + k_m. \tag{75}$$

[11]The largest gap is called the Frobenius number of S.

Lemma 13.1 (monoid gap lemma)**.** *Under these assumptions one has for all* $j = 1, \dots, m$*:*

$$2\,\gamma(S) - 1 \geq j + (m+1)(k_j - 1). \tag{76}$$

In other words, the largest possible gap is bounded by $2\gamma(S) - 1$. Before proving this statement we prove two elementary observations.

Lemma 13.2. *If* i *and* ℓ *in* $\mathbb{Z}_{>0}$ *are such that* $i + \ell = j$ *for* $j \in \{1, \dots, m\}$*, then*

$$k_i + k_\ell \geq k_j.$$

Proof.

$$s_i + s_\ell = i + (m+1)k_i + \ell + (m+1)k_\ell = j + (m+1)(k_i + k_\ell) \geq j + (m+1)k_j.$$

The inequality is by $s_i + s_\ell \in S$ with $s_i + s_\ell \equiv j \pmod{m+1}$, and $s_j \in S$ is minimal with this property. □

Lemma 13.3. *If* i *and* ℓ *in* $\mathbb{Z}_{>0}$ *are such that* $i + \ell = j + m + 1$ *for* $j \in \{1, \dots, m\}$*, then* $k_i + k_\ell + 1 \geq k_j$*.*

Proof.

$$s_i + s_\ell = i + (m+1)k_i + \ell + (m+1)k_\ell = j + (m+1)(k_i + k_\ell + 1) \geq s_j.$$

The inequality is by $s_i + s_\ell \in S$ with $s_i + s_\ell \equiv j \pmod{m+1}$, and $s_j = j + (m+1)k_j \in S$ is minimal with this property. □

Proof of Lemma 13.1. By (75) the statement to prove is equivalent to

$$2(k_1 + \cdots + k_m) \geq j + (m+1)k_j - m. \tag{77}$$

By Lemma 13.2,

$$k_j \leq k_1 + k_{j-1}, k_j \leq k_2 + k_{j-2}, \dots, k_j \leq k_{j-1} + k_1.$$

Summing the left and right sides, respectively, of these $j - 1$ inequalities gives

$$(j-1)k_j \leq 2(k_1 + \cdots + k_{j-1}).$$

By Lemma 13.3,

$$k_j \leq k_{j+1} + k_{m+1-1} + 1, k_j \leq k_{j+2} + k_{m+1-2} + 1, \dots, k_j \leq k_m + k_{j+1} + 1.$$

Summing the left and right sides, respectively, of these $m - j$ inequalities gives

$$(m-j)k_j \leq 2(k_{j+1} + \cdots + k_m) + m - j.$$

Combining the two inequalities we obtained results in

$$(m-1)k_j \leq 2(k_1 + \dots k_m) - 2k_j + m - j,$$

which is (77). □

14. Functions with Separation Property

The setting which we use throughout this section is: $t \in M^\infty(N)$ with $n := \operatorname{pord} t \geq 2$ and $(1, b_1, \ldots, b_{n-1})$ with $b_j \in M^\infty(N)$ is an integral basis for $M^\infty(N)$ over $\mathbb{C}[t]$. Because of $\operatorname{pord} t = n$, for any fixed $\alpha \in \mathbb{C}$ we have that[12]

(78) $t^*(x) = \alpha$ has $\ell \leq n$ pairwise distinct solutions $x_1 = [\tau_1]_N, \ldots, x_\ell = [\tau_\ell]_N$, with multiplicities $k_1, \ldots, k_\ell$, respectively. (I.e., $k_1 + \cdots + k_\ell = n$.)

We note that, as above, owing to $t \in M^\infty(N)$ the $x_j = [\tau_j]_N \in \Gamma_0(N)$ with $\tau_j \in \mathbb{H} \cup \mathbb{Q}$ are such that $[\tau_j]_N \neq [\infty]_N$.

In Definition 9.4 we defined the separation property of f for (t, v_0) with $v_0 = \alpha$ as in (78). At various places we required f to have this property, for instance, in Proposition 11.5. In this section we prove the existence of such f. Also here we have to use the charts as in (37), (38), and (39).

Lemma 14.1. *Given the setting of this section with $\ell \geq 2$, let $\tau, \tau' \in \{\tau_1, \ldots, \tau_\ell\}$ be such that $\tau \neq \tau'$. Then*

$$b_i(\tau) \neq b_i(\tau') \text{ for some } i \in \{1, \ldots, n-1\}.$$

Proof. We are free to relabel the indices of the preimages of α. Hence it is sufficient to prove the statement for $\tau_1 := \tau$ and $\tau_2 := \tau'$. Suppose

$$(\star) \qquad b_j(\tau_1) = b_j(\tau_2) \text{ for all } j \in \{1, \ldots, n-1\}.$$

As in (43), for $j = 1, \ldots, \ell$ and suitable neighborhoods U_j one has local expansions for $\tau \in U_j$:

$$t(\tau) - \alpha = a_{j,0}\phi_{\tau_j}(\tau)^{k_j} + a_{j,1}\phi_{\tau_j}(\tau)^{k_j+1} + \ldots \text{ with } a_{j,0} \neq 0.$$

Moreover, as in (46), for $j = 1, \ldots, \ell$ we can assume that the neighborhoods U_j are chosen such that the following expansions exist for all $\tau \in U_j$:

$$b_1(\tau) = b_1(\tau_j) + \sum_{l=1}^{\infty} d_l^{(1,j)} \phi_{\tau_j}(\tau)^l,$$

$$\ldots$$

$$b_{n-1}(\tau) = b_{n-1}(\tau_j) + \sum_{l=1}^{\infty} d_l^{(n-1,j)} \phi_{\tau_j}(\tau)^l.$$

Taking $a_j \in \mathbb{C}$ the quotient

$$(79) \qquad g := \frac{a_0 + a_1 b_1 + \ldots a_{n-1} b_{n-1}}{t - \alpha}$$

[12]Recall that $t^*([\tau]_n) = t(\tau)$.

defines a modular function $g \in M(N)$. Now $g \in M^\infty(N)$ if and only if all the zeros τ_j of $t(\tau_j) - \alpha = 0$ cancel out. Indeed, assuming $(\star)$ one can determine $a_j \in \mathbb{C}$, not all zero, such that this cancellation happens. Namely, using the local expansions the cancellation condition translates into a system of linear equations where j runs form 1 to ℓ:[13]

$$\begin{aligned} a_0 + a_1 b_1(\tau_j) + \cdots + a_{n-1} b_{n-1}(\tau_j) &= 0, \\ a_1 d_1^{(1,j)} + \cdots + a_{n-1} d_1^{(n-1,j)} &= 0, \\ \vdots &= \vdots \\ a_1 d_{k_j-1}^{(1,j)} + \cdots + a_{n-1} d_{k_j-1}^{(n-1,j)} &= 0. \end{aligned}$$

This gives in total $k_1 + \cdots + k_\ell = n$ equations. But owing to $(\star)$, two of these equations are the same. This means, we are left with $n-1$ equations in n unknowns $a_0, \ldots, a_{n-1}$. This implies that there exists a solution to the system with the a_j not all 0 . This produces a contradiction: Since $g \in M^\infty(N)$ there are polynomials $p_j(x) \in \mathbb{C}[x]$ such that

$$g = p_0(t) + p_1(t) b_1 + \cdots + p_{n-1}(t) b_{n-1}.$$

Combining this with (79), uniqueness of basis representation gives

$$a_0 = (t-\alpha) p_0(t), \ldots, a_{n-1} = (t-\alpha) p_{n-1}(t).$$

Consequently, all $p_j(x)$ and all a_j must be zero. Hence $(\star)$ leads to a contradiction and the lemma is proved. □

Lemma 14.2. *Given the setting of this section with $\ell \geq 2$. For $m \in \{2, \ldots, \ell\}$ let $S_m := \{[\tau_{i_1}]_N, \ldots, [\tau_{i_m}]_N\}$ be a subset of m pairwise distinct preimages of α. Then there exist $\alpha_i \in \mathbb{C}$ such that for $f = \alpha_1 b_1 + \cdots + \alpha_{n-1} b_{n-1}$:*

$$f(\tau_{i_1}), \ldots, f(\tau_{i_m}) \text{ are pairwise distinct.} \tag{80}$$

Proof. We proceed by mathematical induction on m. If $m = 2$, then by the previous lemma there exists an $i \in \{1, \ldots, n-1\}$ such that $b_i(\tau_{i_1}) \neq b_i(\tau_{i_2})$, and we choose $f := b_i$. Suppose $m \geq 2$. Because of index relabeling we can choose $S_m := \{\tau_1, \ldots, \tau_m\}$, and the induction hypothesis gives an $F \in M^\infty(N)$ as a $\mathbb{C}$-linear combination of the b_j such that the values $F(\tau_1), \ldots, F(\tau_m)$ are pairwise distinct. If $F(\tau_{m+1}) \neq F(\tau_i)$ for all $i = 1, \ldots, m$ the induction step is done. Otherwise, $F(\tau_{m+1}) = F(\tau_r)$ for some $r \in \{1, \ldots, m\}$. By the previous lemma there is some $k \in \{1, \ldots, n-1\}$ such that $b_k(\tau_{m+1}) \neq b_k(\tau_r)$, and we can choose a non-zero $c \in \mathbb{C}$ such that

$$c \neq \frac{F(\tau_j) - F(\tau_i)}{b_k(\tau_i) - b_k(\tau_j)} \text{ for all } 1 \leq i < j \leq m+1 \text{ with } b_k(\tau_i) \neq b_k(\tau_j).$$

[13] Notice that the charts $\phi_{\tau_j}(\tau)$ are centered at 0; i.e., $\phi_{\tau_j}(\tau_j) = 0$. Consequently, for fixed j the numerator in (79) has to be of the form $\phi_{\tau_j}(\tau)^{k_j}(c_0 + c_1 \phi_{\tau_j}(\tau) + \ldots)$.

By inspection one verifies for $F_r := F + c\, b_k$ that $F_r(\tau_{m+1}) \neq F_r(\tau_r)$ and also that the values

$$F_r(\tau_1), \ldots, F_r(\tau_m) \text{ are pairwise distinct.}$$

Suppose $F_r(\tau_{m+1}) = F_r(\tau_s)$ for some $s \in \{1, \ldots, m\} \setminus \{r\}$. If there is no such s, we are done with $f := F_r$. Otherwise, by the previous lemma there is some $l \in \{1, \ldots, n-1\}$ such that $b_l(\tau_{m+1}) \neq b_l(\tau_s)$, and we can choose a non-zero $d \in \mathbb{C}$ such that

$$d \neq \frac{F_r(\tau_j) - F_r(\tau_i)}{b_l(\tau_i) - b_l(\tau_j)} \text{ for all } 1 \leq i < j \leq m+1 \text{ with } b_l(\tau_i) \neq b_l(\tau_j).$$

Now we set $F_{r,s} := F_r + d\, b_l$, and see that we have

$$F_{r,s}(\tau_{m+1}) \neq F_{r,s}(\tau_r) \text{ and } F_{r,s}(\tau_{m+1}) \neq F_{r,s}(\tau_s)$$

together with pairwise distinct values $F_{r,s}(\tau_1), \ldots, F_{r,s}(\tau_m)$. Iterating this argument exhausts all possibilities and the induction step is proven. □

Under the assumptions as in (78), in order to have the separation property for (t, α), f additionally has to satisfy the conditions (49) which, rewritten as order conditions are

$$\operatorname{ord}_{\phi_{\tau_j}(\tau)}(f(\tau) - \alpha) = 1 \text{ for all } j = 1, \ldots, \ell. \tag{81}$$

Remark 14.3. The order in (81) has to be interpreted in view of (46) and in the sense of the ϕ-order defined in Def. 15.3. This deviates slightly from the standard notation used in the theory of Riemann surfaces, where (81) would be stated in the format

$$\operatorname{ord}_{\tau_j}(f - \alpha) = 1 \text{ for all } j = 1, \ldots, \ell. \tag{82}$$

This notation suppresses the explicit mentioning of the chart. We also use this notation, for instance in cases like (5), where the chart is clear from the context, or in Lemma 16.1 when citing from Riemann surface theory.

Lemma 14.4. *Given the setting of this section with $\ell \geq 1$. Suppose one has $k_i = \operatorname{ord}_{\phi_{\tau_i}(\tau)}(t(\tau) - \alpha) > 1$ for some $i \in \{1, \ldots, n-1\}$, then*

$$\operatorname{ord}_{\phi_{\tau_i}(\tau)}(b_j(\tau) - b_j(\tau_i)) = 1 \text{ for some } j \in \{1, \ldots, n-1\}.$$

Proof. Let us assume

$$\operatorname{ord}_{\phi_{\tau_i}(\tau)}(b_k(\tau) - b_k(\tau_i)) > 1 \text{ for all } k \in \{1, \ldots, n-1\}. \tag{$\star\star$}$$

As in (43), for $j = 1, \ldots, \ell$ and suitable neighborhoods U_j one has local expansions for $\tau \in U_j$:

$$t(\tau) - \alpha = a_{j,0}\phi_{\tau_j}(\tau)^{k_j} + a_{j,1}\phi_{\tau_j}(\tau)^{k_j+1} + \ldots \text{ with } a_{j,0} \neq 0.$$

Now we proceed with the proof exactly as above. Namely, as in (46), for $j = 1, \dots, \ell$ we can assume that the neighborhoods U_j are chosen such that the following expansions exist for all $\tau \in U_j$ and $k \in \{1, \dots, n-1\}$:

$$b_k(\tau) = b_k(\tau_j) + \sum_{l=1}^{\infty} d_l^{(k,j)} \phi_{\tau_j}(\tau)^l.$$

Now we apply the same strategy as in the proof of Lemma 14.1 and determine $a_j \in \mathbb{C}$, not all zero, such that

$$g := \frac{a_0 + a_1 b_1 + \dots a_{n-1} b_{n-1}}{t - \alpha} \in M^{\infty}(N).$$

This leads us to consider the same system of $k_1 + \dots + k_\ell = n$ linear equations. This time, owing to $(\star\star)$, we have $d_1^{(k,i)} = 0$ for all $k = 1, \dots, n-1$, and the equation containing the $d_1^{(k,i)}$ is always satisfied and can be removed. This means, we are left with $n-1$ equations in n unknowns $a_0, \dots, a_{n-1}$.[14] This implies that there exists a solution to the system with the a_j not all 0, which produces a contradiction as in the proof of Lemma 14.2. □

Lemma 14.5. *Given the setting of this section with $\ell \geq 1$. Then there exist $\alpha_i \in \mathbb{C}$ such that for $f := \alpha_0 t + \alpha_1 b_1 + \dots + \alpha_{n-1} b_{n-1}$:*

$$f(\tau_1), \dots, f(\tau_\ell) \text{ are pairwise distinct, and} \tag{83}$$

$$\operatorname{ord}_{\phi_{\tau_j}(\tau)}(f(\tau) - f(\tau_j)) = 1, \quad j = 1, \dots, \ell. \tag{84}$$

Proof. For the proof it is convenient to introduce an auxiliary function

$$g_i(\tau) := \begin{cases} t(\tau), & \text{if } \operatorname{ord}_{\phi_{\tau_i}(\tau)}(t(\tau) - \alpha) = 1 \\ b_j(\tau), & \text{if } \operatorname{ord}_{\phi_{\tau_i}(\tau)}(t(\tau) - \alpha) > 1 \end{cases}, \quad i = 1, \dots, \ell,$$

where j is chosen according to Lemma 14.4; namely, such that $\operatorname{ord}_{\phi_{\tau_i}(\tau)}(b_j(\tau) - b_j(\tau_i)) = 1$. We will show: given $F = a_0 t + a_1 b_1 + \dots + a_{n-1} b_{n-1}$ with $a_j \in \mathbb{C}$ such that

$$F(\tau_1), \dots, F(\tau_\ell) \text{ are pairwise distinct, and} \tag{85}$$

$$\operatorname{ord}_{\phi_{\tau_j}(\tau)}(F(\tau) - F(\tau_j)) = 1 \text{ for } j = 1, \dots, k, \tag{86}$$

then there is an $f = \alpha_0 t + \alpha_1 b_1 + \dots + \alpha_{n-1} b_{n-1}$ with $\alpha_j \in \mathbb{C}$ which satisfies (83) and

$$\operatorname{ord}_{\phi_{\tau_j}(\tau)}(f(\tau) - f(\tau_j)) = 1 \text{ for } j = 1, \dots, k+1. \tag{87}$$

In other words, we prove Lemma 14.5 by mathematical induction on k.

[14] Notice that for this argument to work we invoke $k_i > 1$.

The base case $k = 1$ corresponds to the induction step from $k = 0$ to $k = 1$. The existence of F such that (85) is by Lemma 14.2. If, in addition,

$$\mathrm{ord}_{\phi_{\tau_1}(\tau)}(F(\tau) - F(\tau_1)) = 1,$$

we take $f := F$, and the base case $k = 1$ is done. If $\mathrm{ord}_{\phi_{\tau_1}(\tau)}(F(\tau) - F(\tau_1)) > 1$, define

$$f := F + cg_1 \text{ with } c \in \mathbb{C} \setminus \{0\} \text{ such that } c \neq \frac{F(\tau_j) - F(\tau_i)}{g_1(\tau_i) - g_1(\tau_j)},$$

where the quotient is taken for all $i, j \in \{1, \ldots, \ell\}$ for which the denominator is non-zero. Now it is a straightforward verification that for this f the condition (83) holds and also that

$$\mathrm{ord}_{\phi_{\tau_1}(\tau)}(f(\tau) - f(\tau_1)) = 1.$$

This settles the base case $k = 1$.

For the induction step $k \to k + 1$ we assume we have an F of required form such that (85) and (86) holds. If, in addition,

$$\mathrm{ord}_{\phi_{\tau_{k+1}}(\tau)}(F(\tau) - F(\tau_{k+1})) = 1,$$

we are done. Otherwise, define

$$f := F + cg_{k+1} \text{ with } c \in \mathbb{C} \setminus \{0\} \text{ such that } c \neq \frac{F(\tau_j) - F(\tau_i)}{g_{k+1}(\tau_i) - g_{k+1}(\tau_j)},$$

where the quotient is taken for all $i, j \in \{1, \ldots, \ell\}$ for which the denominator is non-zero. Now we additionally require that

$$c \neq \frac{a_{1,j}}{b_{1,j}} \text{ for all } j \in \{1, \ldots, \ell\} \text{ when } b_{1,j} \neq 0, \tag{88}$$

for $a_{1,j}$ and $b_{1,j}$ coming from the expansions

$$F(\tau) = a_{0,j} + a_{1,j}\phi_j(\tau) + \ldots \text{ and } g_{k+1}(\tau) := b_{0,j} + b_{1,j}\phi_j(\tau) + \ldots.$$

Again it is straightforward to verify that for such a choice f has the properties (83) and (87). The extra requirement (88) is needed to guarantee the first k instances of the latter condition. This completes the proof of the induction step and also of Lemma 14.5. □

Summarizing, by using an integral basis $(1, b_1, \ldots, b_{n-1})$ for $M^\infty(N)$ over $\mathbb{C}[t]$, we constructed an f which proves

Corollary 14.6. *For every $\alpha \in \mathbb{C}$ there is an $f \in M^\infty(N)$ such that f has the separation property for (t, α).*

15. Appendix: Modular Functions - Basic Notions

To make this article as much self-contained as possible, in this section we recall most of the facts we need about modular functions.

The modular group $\mathrm{SL}_2(\mathbb{Z}) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbb{Z}^{2\times 2} : ad - bc = 1\}$ acts on the upper half $\mathbb{H}$ of the complex plane by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\tau := \frac{a\tau+b}{c\tau+d}$; this action is inherited by the congruence subgroups

$$\Gamma_0(N) := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : N \mid c\}$$

where, throughout this paper, N is a fixed positive integer. Note that $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$. These subgroups have a finite index in $\mathrm{SL}_2(\mathbb{Z})$:

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{\text{prime } p|N} \Big(1 + \frac{1}{p}\Big), \quad N \geq 2; \tag{89}$$

see the standard literature on modular forms like [4] or [2]. Particularly related to our context are [8] and [11].

The action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ extends to an action on meromorphic functions $f : \mathbb{H} \to \hat{\mathbb{C}} := \mathbb{C} \cup \{\infty\}$. A *meromorphic modular function for* $\Gamma_0(N)$ is: (i) a meromorphic function $f : \mathbb{H} \to \hat{\mathbb{C}}$ such that (ii) for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$:

$$f\Big(\frac{a\tau + b}{c\tau + d}\Big) = f(\tau), \quad \tau \in \mathbb{H},$$

and (iii) if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ then $f\left(\frac{a\tau+b}{c\tau+d}\right)$ admits a Laurent series expansion with finite principal part in powers of $q^{\gcd(c^2,N)/N}$. We will use the abbreviation $w_N(c) := N/\gcd(c^2, N)$, and $M(N)$ for the set of meromorphic modular functions for $\Gamma_0(N)$.

By (iii) with $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, any $f \in M(N)$ admits a Laurent series expansion in powers of $q = q(\tau) := e^{2\pi i\tau}$ with finite principal part; i.e.,

$$f(\tau) = \sum_{n=-M}^{\infty} f_n q^n. \tag{90}$$

Hence in view of $\lim_{\mathrm{Im}(\tau)\to\infty} q(\tau) = 0$, one can extend f to $\mathbb{H} \cup \{\infty\}$ by defining $f(\infty) := \infty$, if $M > 0$, and $f(\infty) := f_0$, otherwise. Subsequently, a Laurent expansion of f as in (90) will be also called *q-expansion of f at infinity.*[15]

[15]This expansion and also those for $f(\gamma\tau)$ are required to converge for all $\tau \in \mathbb{H}$ with $\mathrm{Im}(\tau)$ sufficiently large.

Given $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $f \in M(N)$, consider the Laurent series expansion of $f(\gamma\tau)$ in powers of $q^{1/w_N(c)}$,

$$f(\gamma\tau) = \sum_{n=-M}^{\infty} g_n q^{n/w_N(c)}. \tag{91}$$

In view of $\gamma\infty = \lim_{\mathrm{Im}(\tau)\to\infty} \gamma\tau = a/c$, we say that (91) is a *q-expansion of f at a/c*. Understanding that $a/0 = \infty$, this also covers the definition of q-expansions at ∞. Concerning uniqueness of such expansions, let $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$ be such that $\gamma'\infty = \gamma\infty = a/c$. Then the q-expansion of $f(\gamma'\tau)$ differs from that of $f(\gamma\tau)$ only by a root-of-unity factor in the coefficients. Namely, then $\gamma' = \gamma \left(\begin{smallmatrix} \pm 1 & m \\ 0 & \pm 1 \end{smallmatrix}\right)$ for some $m \in \mathbb{Z}$, which implies

$$f(\gamma'\tau) = \sum_{n=-M}^{\infty} g_n \left(e^{\pm 2\pi i m/w_N(c)}\right)^n q^{n/w_N(c)}.$$

As a consequence, one can extend f from $\mathbb{H}$ to $\hat{\mathbb{H}} := \mathbb{H} \cup \{\infty\} \cup \mathbb{Q}$ by defining $f(a/c) := \lim_{\mathrm{Im}(\tau)\to\infty} f(\gamma\tau)$ where $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ is chosen such that $\gamma\infty = a/c$. Another consequence is that the q-expansions of f at ∞ are uniquely determined owing to

$$\gamma\infty = \infty \Leftrightarrow \gamma = \left(\begin{smallmatrix} \pm 1 & m \\ 0 & \pm 1 \end{smallmatrix}\right) \text{ and } w_\ell(0) = 1. \tag{92}$$

Next, notice that the action of $\mathrm{SL}_2(\mathbb{Z})$, and thus of $\Gamma_0(N)$, extends in an obvious way to an action on $\hat{\mathbb{H}}$. The orbits of the $\Gamma_0(N)$ action are denoted by

$$[\tau]_N := \{\gamma\tau : \gamma \in \Gamma_0(N)\}, \quad \tau \in \hat{\mathbb{H}}.$$

In cases where N is clear from the context, one also writes $[\tau]$ instead of $[\tau]_N$. The set of all such orbits is denoted by

$$X_0(N) := \{[\tau]_N : \tau \in \hat{\mathbb{H}}\}.$$

The $\Gamma_0(N)$ action maps $\mathbb{Q}\cup\{\infty\}$ to itself, and owing to (89) each $\Gamma_0(N)$ produces only finitely many orbits $[\tau]_N$ with $\tau \in \mathbb{Q} \cup \{\infty\}$; such orbits are called *cusps* of $X_0(N)$. One has, for example,

Lemma 15.1. *For any prime ℓ,*

(1) *$X_0(\ell)$ has two cusps: $[\infty]_\ell$ and $[0]_\ell$;*

(2) *$X_0(\ell^2)$ has $\ell+1$ cusps: $[\infty]_{\ell^2}, [0]_{\ell^2}$, and $[k/\ell]_{\ell^2}$, $k = 1, \ldots, \ell-1$.*

Proof. This fact can be found in many sources; a detailed description of how to construct a set of representatives for the cusps of $\Gamma_0(N)$, for instance, is given in [15, Lemma 5.3]. □

Suppose the domain of $f \in M(N)$ is extended from $\mathbb{H}$ to $\hat{\mathbb{H}}$ as described above; i.e., $f : \mathbb{H} \to \hat{\mathbb{C}}$ is extended to $f : \hat{\mathbb{H}} \to \hat{\mathbb{C}}$, where we keep the same name for the extended function. Then using this extension gives rise to a function $f^* : X_0(N) \to \hat{\mathbb{C}}$, which is defined as follows:

$$f^*([\tau]_N) := f(\tau), \quad \tau \in \hat{\mathbb{H}}.$$

The fact that f^* is well-defined follows from our previous discussion. We say that f^* is induced by f.

As described in detail in [4], $X_0(N)$ can be equipped with the structure of a compact Riemann surface. This analytic structure turns the induced functions f^* into meromorphic functions on $X_0(N)$. The following classical lemma [10, Thm. 1.37], a Riemann surface version of Liouville's theorem, is crucial for zero recognition of modular functions:

Lemma 15.2. *Let X be a compact Riemann surface. Suppose that $g : X \to \mathbb{C}$ is a holomorphic function on all of X. Then g is a constant function.*

Being meromorphic, modular functions form fields. A classic example is that $M(N) = \mathbb{C}(j(\tau), j(N\tau))$, e.g., [4, Prop. 7.5.1], where j is the modular invariant (Klein j function). The subset

$$M^!(N) := \{f \in M(N) : f^* \text{ has poles only at } [\tau]_N \text{ with } \tau \in \mathbb{Q} \cup \{\infty\}\},$$

which is important for our context, obviously is not a field but a $\mathbb{C}$-algebra.[16] In this case, owing to the definition of induced functions f^*, all possible poles of f^* can be spotted by checking whether $f^*([a/c]) = f(a/c) = \infty$ for $a/c \in \mathbb{Q} \cup \{\infty\}$. Because of (89), $\mathbb{Q} \cup \{\infty\}$ splits only into a *finite* number of cusps,

$$\mathbb{Q} \cup \{\infty\} = [a_1/c_1]_N \cup \cdots \cup [a_k/c_k]_N.$$

Hence knowing all the cusps $[a_j/c_j]$ reduces the task of finding all possible poles to the inspection of q-expansions of f at a_j/c_j; i.e., of q-expansions of $f(\gamma_j\tau)$ as in (91) with $\gamma_j \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma_j\infty = a_j/c_j$. We call these expansions also local q-expansions of f^* at the cusps $[a_j/c_j]_N$; $w_N(c_j)$ is called the width of the cusp $[a_j/c_j]_N$. It is straightforward to show that it is independent of the choice of the representative a_j/c_j of the cusp $[a_j/c_j]_N$, and that $w_N(c_j) = N/\gcd(c_j^2, N)$ for relatively prime a_j and c_j. Note that $[\infty]_N = [1/0]_N$.

Definition 15.3 (order and ϕ-order)**.** *Let $f = \sum_{n=m}^{\infty} a_n q^n$ with $m \in \mathbb{Z}$ such that $a_m \neq 0$. Then we define the order of f as*

$$\operatorname{ord} f := m.$$

[16] A $\mathbb{C}$-algebra is a commutative ring with 1 which is also a vector space over $\mathbb{C}$.

More generally, if $\phi = \sum_{n\geq 1}^{\infty} b_n q^{n/w}$ *for some fixed* $w \in \mathbb{Z}_{>0}$, *and* $F = f \circ \phi := \sum_{n=m}^{\infty} a_n \phi^n$, *then we define the* ϕ*-order of* f *as*

$$\operatorname{ord}_\phi f := m.$$

(E.g., if $m = \operatorname{ord} f = -1$ *and* $\phi = q^2$, *then* $\operatorname{ord}_\phi F = -1$ *but* $\operatorname{ord} F = -2$*; if* $m = \operatorname{ord} f = -2$ *and* $\phi = q^{1/2}$, *then* $\operatorname{ord}_\phi F = -2$ *but* $\operatorname{ord} F = -1$*.) And, more generally, we extend this definition of* ϕ*-order to the case where* $\phi := \phi_{\tau_0}(\tau)$ *is one of the charts as in* (37), (38), *and* (39).

The order $\operatorname{ord}_{[a/c]_\ell} f^*$ of f^* at a cusp $[a/c]_\ell$ is defined to be the $q^{1/w_\ell(c)}$-order of a local q-expansion of f^* at $[a/c]_N$; i.e.,

$$\operatorname{ord}_{[a/c]_N} f^* := \operatorname{ord}_{q^{1/w_N(c)}} f(\gamma\tau) \text{ where } \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}).$$

It is straightforward to verify that $\operatorname{ord}_{[a/c]} f^*$ is well-defined. For a concrete example, see Ex. 2.1.

16. Appendix: Meromorphic Functions on Riemann Surfaces - Basic Notions

To make this article as much self-contained as possible, in this second appendix section we recall most of the facts we need about meromorphic functions on Riemann surfaces. For the terminology we basically follow [6]; other classic texts are [5] and [10].

Lemma 15.2 states the fundamental fact that any analytic function on a compact Riemann surface is constant. In Ex. 2.1 we have seen that z_5^* has its only zero of order 1 at $[\infty]_5$ and its only pole at $[0]_5$ with multiplicity 1; i.e., z_5^* has order -1 at $[\infty]_5$.[17] This is also in accordance with Lemma 16.1, a corollary of another fundamental fact which says that meromorphic functions on compact Riemann surfaces have exactly as many zeroes as poles (counting multiplicities); see, for instance, [10, Prop. 4.12]:

Lemma 16.1. *Let* g *be a non-constant meromorphic function on a compact Riemann surface* X*. Then*

$$\sum_{x\in X} \operatorname{ord}_x g = 0.$$

Here $\operatorname{ord}_{x_0} g$ is defined as follows. Suppose $g(x) = \sum_{n=m} c_n(\varphi(x) - \varphi(x_0))^n$, $c_m \neq 0$, is the local Laurent expansion of g at x_0 using the local coordinate chart $\varphi : U_0 \to \mathbb{C}$ which homeomorphically maps a neighborhood U_0 of $x_0 \in X$ to an open set $V_0 \subseteq \mathbb{C}$. Then $\operatorname{ord}_{x_0} g := m$.

[17] Notice that we also say that z_5^* has pole order 1 at $[\infty]_5$.

Let $\mathcal{M}(S)$ denote the field of meromorphic functions $f : S \to \hat{\mathbb{C}}$ on a Riemann surface S.[18] Let $f \in \mathcal{M}(S)$ be non-constant: then for every neighborhood U of $x \in S$ there exist neighborhoods $U_x \subseteq U$ of x and V of $f(x)$ such that the set $f^{-1}(v) \cap U_x$ contains exactly k elements for every $v \in V \setminus \{f(x)\}$. This number k is called the multiplicity of f at x; notation: $k = \operatorname{mult}_x(f)$.[19] If S is compact, $f \in \mathcal{M}(S)$ is surjective and each $v \in \hat{\mathbb{C}}$ has the same number of preimages, say n, counting multiplicities; i.e., $n = \sum_{x \in f^{-1}(v)} \operatorname{mult}_x(f)$; see, e.g., [6, Thm. 4.24]. This number n is called the degree of f; notation: $n = \operatorname{Deg}(f)$. One of the consequences is that non-constant functions on compact Riemann surfaces have as many (finitely many) zeros as poles counting multiplicities; this is Lemma 16.1.

$\operatorname{RamiPts}(f) := \{x \in S : \operatorname{mult}_x(f) \geq 2\}$ denotes the set of ramification points of f; $\operatorname{BranchPts}(f) := f(\operatorname{RamiPts}(f)) \subseteq \hat{\mathbb{C}}$ denotes the set of branch points of f. Ramification points, and also branch points, of a function f form sets having no accumulation point. Hence for functions on compact Riemann surfaces these sets have finitely many elements.

17. Conclusion

In this article we present the first proof of the Weierstrass gap theorem (for modular functions) without using the Riemann-Roch theorem. The main ingredient in our proof is the concept of order-reduction polynomials which corresponds to the discriminant of a field extension of $\mathbb{Q}$ in the setting of algebraic number theory; see, for instance, [9, III,§3]. In the field case the structure of this discriminant is related to the ramification index [9, III, §2, Prop. 8, and III, §3, Prop. 14]. Analogously, in Prop. 11.5, we give a factorization of the order-reduction polynomial which in direct fashion relates to the branch points of the modular function t. This relation allows us to connect the degree of this polynomial to the genus of $X_0(N)$. This observation is crucial for our proof of the Weierstrass gap theorem.

In addition, our approach gives new algebraic and algorithmic insight based on module presentations of modular function algebras, in particular, the usage of integral bases. For example, our proof also gives a method to compute the order-reduction polynomial by using Puiseux series expansions at infinity. Another new feature concerns the gap bound: the main task of our proof is to show that there are exactly g gaps for any modular function algebra. The proof that the corresponding pole orders are bounded by $2g - 1$, with the help of an elementary combinatorial argument turns out to be an immediate consequence of our

[18] In this context $\hat{\mathbb{C}} := \mathbb{C} \cup \{\infty\}$ is understood to be a compact Riemann surface isomorphic to the Riemann sphere.

[19] If x is a pole of f: $\operatorname{mult}_x f = -\operatorname{ord}_x f$; otherwise, $\operatorname{mult}_x f = \operatorname{ord}_x(f - f(x))$.

approach. Another by-product of our framework is a natural explanation of the genus $g = 0$ case as a consequence of the reduction to an integral basis.

Summarizing, our setting generalizes ideas from algebraic number theory but still stays close to "first principles." Hence we feel our approach has potential for further extensions and applications. For example, we are planning to exploit the algorithmic content of our approach for computer algebra applications, for instance, for the effective computation of suitable module bases for modular function algebras.

Acknowledgement. In November 2018, while working on parts of this paper, the first named author enjoyed the overwhelming hospitality of Bill Chen and his team at the Applied Center for Mathematics, Tianjin University.

References

[1] Andrea Del Centina. Weierstrass points and their impact in the study of algebraic curves: a historical account from the "Lückensatz" to the 1970s. *Ann. Univ. Ferrara*, 54:37–59, 2008.
[2] Henri Cohen and Fredrik Strömberg. *Modular Forms: A Classical Approach*, volume 179 of *Grad. Stud. Math.* AMS, 2017.
[3] Richard Dedekind and Heinrich Weber. *Theory of Algebraic Functions in One Variable. Translated and introduced by John Stillwell.* History of Mathematics, Vol. 39. American Mathematical Society, 2012.
[4] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms.* Springer, 2005.
[5] Hershel M. Farkas and Irwin Kra. *Riemann Surfaces*, volume 71 of *Graduate Texts in Mathematics.* Springer, 1980.
[6] Otto Forster. *Lectures on Riemann Surfaces.* Springer, 1981.
[7] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete Mathematics - A Foundation for Computer Science, 2nd ed.* Addison-Wesley, 1994.
[8] Marvin I. Knopp. *Modular Functions in Analytic Number Theory.* American Mathematical Society, 1993.
[9] Serge Lang. *Algebraic Number Theory, 2nd ed.* Springer, 1994.
[10] Rick Miranda. *Algebraic Curves and Riemann Surfaces*, volume 5 of *Grad. Stud. Math.* AMS, 1995.
[11] Ken Ono. *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-series.* CBMS Regional Conference Series in Mathematics, Number 102, 2004.
[12] Peter Paule and Cristian-Silviu Radu. A new witness identity for $11|p(11n+6)$. In George E. Andrews and Frank Garvan, editors, *Analytic Number Theory, Modular Forms and q-Hypergeometric Series*, pages 625–640. Springer, 2016.
[13] Peter Paule and Cristian-Silviu Radu. A unified algorithmic framework for Ramanujan's congruences modulo powers of 5, 7, and 11. 2018. Submitted.
[14] Cristian-Silviu Radu. An algorithmic approach to Ramanujan-Kolberg identities. *Journal of Symbolic Computation*, 68(1):225–253, 2015.
[15] Cristian-Silviu Radu. An algorithm to prove algebraic relations involving eta quotients. *Annals of Combinatorics*, 22:377–391, 2016.

[16] Heinrich Weber and Richard Dedekind. Theorie der algebraischen Functionen einer Veränderlichen. *Journal für die reine und angewandte Mathematik*, 92:181–290, 1882.

Research Institute for Symbolic Computation (RISC), Johannes Kepler University, A-4040 Linz, Austria

Email address: Peter.Paule@risc.uni-linz.ac.at

Research Institute for Symbolic Computation (RISC), Johannes Kepler University, A-4040 Linz, Austria

Email address: Silviu.Radu@risc.uni-linz.ac.at