TRAGER'S ALGORITHM FOR INTEGRATION OF ALGEBRAIC FUNCTIONS REVISITED

DANIEL SCHULTZ

Abstract. Building on work of Risch in the 1980s and Liouville in the 1840s, Trager presented an algorithm for deciding if a given algebraic function has an elementary antiderivative. While this algorithm is theoretically complete, it is incomplete in the sense that assumptions are made about the function to be integrated in relation to the defining equation for the algebraic irrationality. These assumptions can be justified by a change of variables in the defining equation, but this does not lead to the most natural algorithm for integration. We fill in the 'gaps' in Trager's algorithm for integration in function fields defined over finitely generated extensions of $\mathbb{Q}$. Various extensions to Trager's algorithm are also discussed, including a remedy to several of the possible points of failure in the algorithm as well as the problem of the presence of zero divisors in the algebraic function to be integrated.

1. Introduction

As taught in any second semester calculus course, the integral of $\sqrt{x^2+2x}\,dx$ may be calculated as

$$\int \sqrt{x^2+2x}\,dx = \frac{1}{2}(x+1)\sqrt{x^2+2x} - \frac{1}{2}\log(x+1-\sqrt{x^2+2x}).$$

The form of this answer is consistent with the general case of such integrals. In order to calculate this integral, one first removes the double pole at infinity (this will be explain later) as

$$\int \sqrt{x^2+2x}\,dx = \frac{1}{2}(x+1)\sqrt{x^2+2x} - \frac{1}{2}\int \frac{dx}{\sqrt{x^2+2x}}. \tag{1.1}$$

The resulting intergral has only simple poles and thus can be integrated as a sum of logarithms or arctangents. In this case, the integrand is

$$\frac{dx}{\sqrt{x^2+2x}} = \pm\left((1/x)^{-1} - 1 + O(1/x)\right)d(1/x),$$

which has residue -1 at $x=\infty$ if the positive sign of the square root is taken, and has residue $+1$ at $x=\infty$ if the opposite sign of the square root is taken. One then searches for a function that has a simple zero and a simple pole in these respective situations. Such a function turns out to be $1+x-\sqrt{x^2+2x}$, for if the negative sign is retained in front of the square root, this function approaches 0 like $1/x$ as x approaches ∞, while if it is changed to a positive sign, then the function approaches ∞ like x. Due to the identity

$$(1+x-\sqrt{x^2+2x})(1+x+\sqrt{x^2+2x}) = \text{nonzero constant}, \tag{1.2}$$

it is clear that $1+x-\sqrt{x^2+2x}$ is finite and nonzero for all finite values of x. These properties ensure that the differential

$$\frac{dx}{\sqrt{x^2+2x}} - d\log(1+x-\sqrt{x^2+2x}) \tag{1.3}$$

has no poles at any finite or infinite values of x, which in this case means that it must vanish identically and we have completed the integration procedure.

While this is hardly the approach taken in second semester calculus, this is the appoach that generalizes to any algebraic function. Trager [7] has described such an algorithm, and the purpose here is implement this algorithm efficiently while filling in some of the gaps and inefficiencies along the way. As a result, we can effortlessly compute the remarkable result

$$\begin{aligned}\int \frac{(29x^2+18x-3)dx}{\sqrt{x^6+4x^5+6x^4-12x^3+33x^2-16x}} &= \ln\big(x^{29}+40x^{28}+776x^{27}+9648x^{26}\\ &+85820x^{25}+578480x^{24}+3058536x^{23}+12979632x^{22}+4500490x^{21}+129708992x^{20}\\ &+317208072x^{19}+675607056x^{18}+1288213884x^{17}+2238714832x^{16}+3548250712x^{15}\\ &+5097069328x^{14}+6677210721x^{13}+8106250392x^{12}+9056612528x^{11}+8991685504x^{10}\\ &+7944578304x^9+6614046720x^8+4834279424x^7+2374631424x^6+916848640x^5\\ &+638582784x^4-279969792x^3-528482304x^2+150994944x-134217728\\ &+\big(x^{26}+38x^{25}+699x^{24}+8220x^{23}\\ &+68953x^{22}+436794x^{21}+2161755x^{20}+8550024x^{19}+27506475x^{18}+73265978x^{17}\\ &+165196041x^{16}+324386076x^{15}+570906027x^{14}+914354726x^{13}+1326830817x^{12}\\ &+1731692416x^{11}+2055647184x^{10}+2257532160x^9+2246693120x^8+1939619840x^7\\ &+1494073344x^6+1097859072x^5+640024576x^4+207618048x^3+95420416x^2\\ &+50331648x-50331648)\sqrt{x^6+4x^5+6x^4-12x^3+33x^2-16x}\big).\end{aligned}$$

It is worth noting that a Pellian equation similar (1.2) holds in this case as well.

It is curious that the majority of the following machinery needed to construct a general integration algorithm for algebraic functions is not specifically related to integration and is applicable to a wide variety of problems in algebraic geometry.

(1) If a quantity such as $\sqrt{x^2}$ is present in the integrand, then $x-\sqrt{x^2}$ is a non-zero zero divisor as $(x-\sqrt{x^2})(x+\sqrt{x^2})=0$. Accordingly, $\mathbb{Q}(x)[\sqrt{x^2}]$ is not a field and we must be able to detect these zero divisors to proceed with the integration algorithm. While the case of $\sqrt{x^2}=\pm x$ is quite simple, zero divisors can arise in non-trivial ways and detecting them is equally non-trivial.
(2) We need an integral basis, from which the poles of an algebraic function may be easily located.
(3) We need a way to represent weighted collections of points on a curve (divisors).
(4) We need to able to do arithmetic on divisors efficiently.

Once (2) is accomplished, the integration step in (1.1) is straightforward, and the construction of the logarithmic term in (1.3) follows easily from (3) and (4).

2. Background on algebraic functions

We are interested in the integral $\int R(x,y)\,dx$ where $R(x,y)$ is a rational function of x and y and y satisfies an *irreducible* equation of the form $y^n+p_{n-1}(x)y^{n-1}+\cdots+p_1(x)y+p_0(x)=0$, for

$p_i(x) \in k[x]$, where k is a field of characteristic 0. It will be simplest to assume that $k = \mathbb{C}$ for now, and we follow [3] for basic notions of algebraic curves and their divisors. Near any finite point $x = x_0$ or infinite point $x = \infty$ the n solutions for y can be grouped into cycles of the form

$$\begin{aligned} y &= b_1(x - x_0)^{\mu_1/r} + b_1(x - x_0)^{\mu_1/r} + \cdots \qquad \text{or} \\ y &= b_1(1/x)^{\mu_1/r} + b_2(1/x)^{\mu_2/r} + \cdots, \end{aligned} \tag{2.1}$$

where r and $\mu_1 < \mu_2 < \ldots$ are relatively prime integers so that that this expansion gives r solutions for y. Thus above every point $x = x_0$ or infinite point $x = \infty$ there are a certain number of cycles, also called places, whose values of r total n. Places above $x = x_0$ are called finite places, while places above $x = \infty$ are called infinite places. The integer r is called the ramification index of the place and places with $r > 1$ are called branch places. The variable $t = (x - x_0)^{1/r}$ or $t = (1/x)^{1/r}$ may be used as the local paramter at the place P. This allows us to measure the order of a function $f \in k(x, y)$ (or a differential ω) at a place P, denoted by $\operatorname{ord}_P f$, as the smallest power of t in the expansion of f (or ω). That is,

$$\begin{aligned} f &= t^{\operatorname{ord}_P(f)}(1 + O(t)), \\ \omega &= t^{\operatorname{ord}_P(\omega)}(1 + O(t))dt. \end{aligned}$$

The residue of a differential is defined in a similar fashion as the coefficient of dt/t and denoted by $\operatorname{res}_P(\omega)$. A function or a differential is said to vanish at a place if its order there is positive, be regular at a place if its order is nonnegative, have a pole at a place if its order is negative.

Let $O^\infty(K)$ or simply O^∞ denote the ring of integral functions in $K = k(x, y)$, that is, rational functions of x and y that satsify a monic polynomial over $k[x]$. This is the same as the ring of all functions that are regular at all finite places. As this is a Dedekind domain, we will make extensive use of fractional ideals of O^∞. There is a one-to-one correspondence between the prime ideals of O^∞ and the places of K/k. The correspondence associates to each place P the ideal of functions in O^∞ that vanish at P. A divisor D is a formal product $D = P_1^{\mu_1} \cdots P_s^{\mu_s}$ over places with integer exponents μ_i. An effective divisor is one with all $\mu_i \geq 0$, and we say that $A \geq B$, or A is a multiple of B, if A/B is effective. The degree $\deg(Q)$ of this divisor is $\mu_1 + \cdots + \mu_s$. The divisor of a function (or differential) is defined as

$$\operatorname{div}(f) = \prod_P P^{\operatorname{ord}_P(f)}.$$

Divisors of functions are known as principal divisors, and divisors of differentials are known as canonical divisors. The fact that principal divisors have degree zero is a restatement of the well-known fact that a function has the same number of poles as zero when counting according to multiplicity. There is a similar fact that the sum over all places of the residues of a differential is zero.

The main difficulties in integrating algebraic functions arise from computing the logarithmic portion of the integral. The fundamental problem is the following: given a divisor D of degree zero, determine if there is some integer l such that D^l is principal. Such divisors are called torsion divisors because they correspond to points of finite order on the Jacobian of the curve. For example,

on the curve $y^2 = x^6 + 4x^5 + 6x^4 - 12x^3 + 33x^2 - 16x$ there are two places A and B over $x = \infty$,

$$\begin{aligned} A: &\quad y = +(1/x)^{-3} + 2(1/x)^{-2} + \cdots, \\ B: &\quad y = -(1/x)^{-3} - 2(1/x)^{-2} + \cdots, \end{aligned}$$

and these are the only places where the integrand $(29x^2+18x-3)dx/y$ has a pole. In contrast to the example in the introduction, it turns out that one cannot find a function that has a simple zero A and a simple pole at B. However, there is a function that a zero at A and a pole at B, each of order 29. Thus the divisor A^{29}/B^{28} is principal, and the integration succeeds with the quantity inside the logarithm having degree 29. This example of a hyperelliptic curve defined over $\mathbb{Q}$ with a 29-torsion point is due to Leprévost [9]. Using the methods of [13], it is possible to obtain hyperelliptic curves with torsion points of even higher order, and such an integral is computed in Example 4 of [16]. The methods used in [16] arise from numerical approximations and are non-rigorous in nature. This constrasts with the completely rigourous algorithm of Trager, which can determine that the divisor A/B has order 29 while staying completely in $\mathbb{Q}$ for all computations.

3. Trager's algorithm for integration of algebraic functions

We will breifly outline Trager's algorithm for the integration of algebraic functions before moving to a more general procedure that eliminates two of the assumptions made by Trager. Assume that the integrand can be written as a rational function $R(x, y)$ of x and y where y is related to x by some algebraic curve $F(x, y) = 0$. The basis of this algorithm is a theorem of Liouville which states that if the integral of $R(x, y)$ can be expressed in elementary form, then it can be expressed in the form

$$\int R(x,y)dx = u(x,y) + \sum_i c_i \log(v_i(x,y)) \tag{3.1}$$

where the c_i are constants and the $u(x, y)$ and $v_i(x, y)$ are rational functions.

The process of calculating u and the v_i is quite elementary when the integrand is a rational function of x (i.e. no algebraic irrational functions of x appear). This will be briefly reviewed here as the approach for general algebraic functions is modeled after this. One can calculate the partial fraction expansion of any rational function in the form

$$f(x) = \sum_{i=1}^{m} a_i x^{i-1} + \sum_{i=1}^{k}\sum_{j=1}^{l} \frac{c_{i,j}}{(x-r_j)^{i+1}} + \sum_{j=1}^{l} \frac{c_{1,j}}{(x-r_j)}. \tag{3.2}$$

The integral can be calculated as

$$\int f(x)dx = \sum_{i=1}^{m} a_i \frac{x^i}{i} - \sum_{i=1}^{k}\sum_{j=1}^{l} \frac{c_{i,j}}{i(x-r_j)^i} + \sum_{j=1}^{l} c_{1,j} \log(x-r_j).$$

The parts of this approach that do generalize to algebraic functions are the basic observations that simple poles of the integrand contribute to the logarithmic terms while the poles of higher order generate terms with poles of order one less. The parts of this approach that require more work to generalize are the partial fraction expansion and the construction of the logarithmic terms. The difficulties in constructing the logarithmic terms are not evident in the case of rational functions because this function field has genus zero and correspondingly every divisor of degree zero is principal.

3.1. **The algebraic portion of the integral.** Let Ω denote the space of differential of the function field K. This formally consists of elements of K multiplied by dx. Given a differential $\sigma \in \Omega$ with no poles at infinite places, Trager describes a procedure for calculating a function $f \in K$ so that the equation

$$\int \sigma = f + \int \omega$$

defines ω as another differential with no poles at infinite places and at worst simple poles at finite places. Trager's procedure for calculating f succeeds exactly when such an f exists. It is however possible for such an f to exists and the remaining portion $\int \omega$ to be nonelementary.

The original assumption that σ has no poles at infinite places can be justifed by the change of variable $X = 1/(x - x_0)$, where x_0 is chosen so that the original integrand has no poles at any place above $x = x_0$ and no place above $x = x_0$ is a branch point. In the case of rational functions, Trager's assumption amounts to the substitution of $x = 1/X$ into an integral such as

$$\int \frac{x^{10}}{x^7 + 1} dx$$

so that the new integrand in the variable X is a proper rational function. However, this manipulation is completely unnecessary if we are willing to do the polynomial division

$$\frac{x^{10}}{x^7 + 1} = x^3 - \frac{x^3}{x^7 + 1},$$

and proceed with the integration in x. Therefore, the removal of this assumption will be addressed in Section 4 along with the analogue of proper rational functions to algebraic functions.

3.2. **The logarithmic portion of the integral.** Trager's algorithm as presented becomes impractical when logarithmic terms are necessary to express the integral. First, he does not work with an integral basis of the function field when computing the logarithmic terms. Second, he assumes that the branch places of the curve do not contribute poles to the integrand. Third, he uses two-element representations of ideals (or divisors), which seems to be quite uncomfortable for computations. The first issue is quite easily fixed, while the third issue can be remedied by manipulating divisors by their ideal bases. The second issue is much more subtle. Trager justifies this assumption by a change of variable in the defining equation for x and y. This change of variables necessitates a recomputation of an integral basis and is a blemish on an otherwise elegant algorithm. We will defer a natural remedy of the problem of poles at branch points to Section 4.

It suffices for now to say that Trager constructs a divisor $\delta(z)$ that contains all of the places where the integrand has residue $z \neq 0$. Each place in $\delta(z)$ appears with multiplicity 1. He is able to give a polynomial in z whoose roots are the z-values where $\delta(z)$ is nontrivial. We can thus assume that a list of nonzero residues of the integrand $z_1, \cdots, z_k$ has been construct along with the corresponding divisor of places $\delta(z_k)$.

Suppose that the divisors $\delta(z_k)$ are principal so that there there are functions f_k with $\delta(z_k) = \operatorname{div}(f_k)$. In this case the equation

$$\int \sigma = \sum_k z_k \log f_k + \int \theta \tag{3.3}$$

defines θ as a differential without poles. There are two problem with this equation. First, we don't require $\delta(z_k)$ to be principal but only require some integer power of it to be principal via

$\delta(z_k)^{c_k} = \operatorname{div}(f_k)$. This changes the equation to

$$\int \sigma = \sum_k \frac{z_k}{c_k} \log f_k + \int \theta. \tag{3.4}$$

Next, it is possible for the residues z_k to be linearly dependent over $\mathbb{Q}$ and that the integration can only be performed by combining several of these logarithmic terms into one term. Consider, for example, the integral

$$\int \frac{2(3x^3 - 10x^2 + 4x + 2)dx}{(2x-1)(x^3 - 2x^2 + 1)\sqrt{x^3+1}} = \sqrt{2} \log \left(\frac{\sqrt{2}(x-2) - (2x-3)\sqrt{x^3+1}}{\sqrt{2}(x-2) + (2x-3)\sqrt{x^3+1}} \right). \tag{3.5}$$

The integrand has residues $\pm 2\sqrt{2}$ at certain places A_1 and B_1 and residues $\pm\sqrt{2}$ at certain places A_2 and B_2. However, neither the divisor A_1/B_1 nor the divisor A_2/B_2 is torsion. Hence the integration cannot be carried out in the form (3.4), or $2\sqrt{2}/c_1 \log(f_1) + \sqrt{2}/c_2 \log(f_2)$, for any integers c_1 and c_2. However it turns out that $A_1^2 A_2/(B_1^2 B_2)$ is torsion so that the integral can be expressed in the form $\sqrt{2}\log(g_1)$. This is due to the fact that underlying curve is $y^2 = x^3 + 1$. Since the genus of this curve is nonzero, not every divisor is principal, and the decomposition $g_1 = f_1^2 f_2$ is simply not possible. Therefore, when the genus of the algebraic function field is nonzero, insteading of considering merely the residues, it is necessary to consider a $\mathbb{Q}$-basis $b_1, \ldots, b_l$ for their $\mathbb{Q}$-span. There is then a matrix $m \in \mathbb{Z}^{k \times l}$ such that $z_i = \sum_j m_{i,j} b_j$. This is the computationally intractable step of the integration algorithm, since it requires computation in the field $k(z_1, \ldots, z_k)$, but let's assume that this has been done. Further define $\Delta_j = \prod_i \delta(z_i)^{m_{i,j}}$, which collects the divisors from the residues into their basis element. We must have $\Delta_j^{c_j} = \operatorname{div}(F_j)$ for some integers c_j and functions F_j in order for the integral to be elementary. In this case,

$$\int \sigma = \sum_j \frac{b_j}{c_j} \log F_j + \int \theta,$$

where θ has no poles whatsoever. The integral is elementary if and only if θ is zero.

The computer algebra system FriCAS [2] has a fairly complete implementation of Trager's algorithm. Since an absolutely complete implementation of the algorithm is computationally infeasible, there are some shortcomings in the integration capabilities of FriCAS, some of which may be related to the second issue above. The integral (3.5) is not evaluated by FriCAS simply because it does not look for linear $\mathbb{Q}$-relations among the residues. FriCAS also produces wildly complicated answers, presumably due to in part to the second issue. For example, the integrand in

$$\int \frac{x + \sqrt{x^2+x}}{x^2+x} dx = 2\log(x + \sqrt{x^2+x})$$

has poles at a branch place of the curve $y^2 = x^2 + x$. FriCAS produces the much more complicated (but still correct) result

$$\int \frac{x + \sqrt{x^2+x}}{x^2+x} dx = \log(x) - \log(2x + 1 - 2\sqrt{x^2+x}).$$

In summary, the problem of integrating algebraic functions meets the practical obstacle of calculation in the full splitting field of a polynomial, and the theoretical obstacle of determining if some power of a divisor is principal. Due to fairly recent advances in the reduction of divisors to

finite fields, this second problem has a complete solution, as described by Trager. This power can be quite large as the example in the introduction shows.

4. Integration of algebraic functions in the general case

We are now going to remove the assumption that the integrand has no poles at infinite places or branch places.

4.1. **Divisors supported at infinite places.** Let us consider how to represent a divisor of the function field $K = k(x, y)$ that contains both finite and infinite places. For this it is necessary to introduce the local ring at infinity

$$k[[1/x]] = \left\{ \frac{f(x)}{g(x)} \in k(x) \middle| \deg(g) \geq \deg(f) \right\}.$$

It is a slight abuse of notation to identify this with the formal power series $k[[1/x]]$, since the formal powers series ring contains power series that cannot be represented by elements of $k(x)$. What we want is formal power series in $1/x$ whose coefficients eventually satisfy a linear reccurence relation. The ring $k[[1/x]]$ has a unique maximal ideal $(1/x)$ and elements with nonzero constant term (equivalently $\deg(g) = \deg(f)$) are units. We then let O_∞ denote the integral closure of $k[[1/x]]$ in K. Thus far we have the two rings $k[x]$ and $k[[1/x]]$ and Dedekind domains

$$\begin{aligned} O^\infty &= \{f \in K | \operatorname{ord}_P(f) \geq 0 \text{ for all finite places } P\}, \\ O_\infty &= \{f \in K | \operatorname{ord}_P(f) \geq 0 \text{ for all infinite places } P\}. \end{aligned}$$

For any divisor D we have the O^∞-fractional ideal D^∞ and the O_∞-fractional ideal D_∞.

$$\begin{aligned} D^\infty &= \{f \in K | \operatorname{ord}_P(f) \geq D \text{ for all finite places } P\}, \\ D_\infty &= \{f \in K | \operatorname{ord}_P(f) \geq D \text{ for all infinite places } P\}. \end{aligned} \tag{4.1}$$

Thus divisors should be maintained as a pair of ideals D^∞ and D_∞. Arithmetic on divisors entails arithmetic on each of these ideals, which requires matrix arithmetic in $k[x]$ and $k[[1/x]]$. The operations of multiplication, division, addition and intersection on ideals correspond respectively to the operations of addition, subtraction, minimum, and maximum on the exponents in the prime factorization of these ideals.

$$\begin{aligned} \operatorname{ord}_P(I \cdot J) &= \operatorname{ord}_P(I) + \operatorname{ord}_P(J), \\ \operatorname{ord}_P(I/J) &= \operatorname{ord}_P(I) - \operatorname{ord}_P(J), \\ \operatorname{ord}_P(I + J) &= \min(\operatorname{ord}_P(I), \operatorname{ord}_P(J)), \\ \operatorname{ord}_P(I \cap J) &= \max(\operatorname{ord}_P(I), \operatorname{ord}_P(J)). \end{aligned}$$

The choice of the separating element x for the function field K entails several other pieces of data that are worth mentioning. The first is the degree $n = [K : k(x)]$. This allows us to represent elements of K as rational functions of x and y where y satisfies some equation of degree n over $k(x)$. Next there is the degree of the constant field extension $c = [k_0 : k]$. The function field K is an extension of k with transcendence degree 1. However, there might be extra constants in the constant subfield k_0 of K. This arises when the function field is, for example, $\mathbb{Q}(x, y)$ over $\mathbb{Q}$ with defining equation $y^2 - 2x^2 = 0$. In this case the constant function y/x generates k_0 over $\mathbb{Q}$ and $c = 2$. Finally there is the genus g, which can be defined by $2c(g - 1) = \deg(\operatorname{div}(dx))$. Note that $c \leq n$ and that c and g are independent of the choice of the separating element x.

If we want to know if there are any functions in

$$\mathfrak{R}(D) := D^\infty \cap D_\infty = \{f \in K | \operatorname{ord}_P(f) \geq D \text{ for all places } P\}, \tag{4.2}$$

Lemma 4.1 (Theorem 5.1 and Corollary 5.5 of [6]) is useful. It is important to note that what is called $\mathfrak{R}(D)$ here is actually called $L(D^{-1})$ in [6], and this space is known as the Riemann-Roch space for D^{-1}. The reason for this discrepancy is that we are manipulating divisors by the two ideals D^∞ and D_∞, where the definition (4.1) is most comfortable.

Lemma 4.1. *For any divisor D, there is a $k[x]$-basis $\phi_1, \ldots, \phi_n$ of D^∞ and a $k[[1/x]]$-basis $\psi_1, \ldots, \psi_n$ of D_∞ such that*

$$\psi_i = x^{-d_i}\phi_i,$$

for some integers $d_1, \ldots, d_n$. These integers d_i are unique up to a permuation and d_i is called the exponent of the basis element ϕ_i. Furthermore,

$$\mathfrak{R}(D) \text{ has } k\text{-basis } \{x^j\phi_i\}_{\substack{1\leq i\leq n \\ 0\leq j\leq -d_i}},$$
$$d_1 + \cdots + d_n - \deg(D) = n + c(g-1).$$

We will mainly be applying Lemma 4.1 to test if a divisor of degree zero is principal. In this case, we are simply checking if there are any nonpositive d_i in Lemma 4.1. For the purposes of integration is also necessary to compute the divisor of dx, whose factorization is

$$\operatorname{div}(dx) = \prod_{P \text{ finite}} P^{r(P)-1} \prod_{P \text{ infinite}} P^{-r(P)-1},$$

where $r(P)$ is the ramification index of P. The reason for this factorization is

$$d(x_0 + t^r) = +rt^{r-1}dt \quad \text{for finite places,}$$
$$d(t^{-r}) = -rt^{-r-1}dt \quad \text{for infinite places.}$$

The product is well-defined since only finitely many finite places have ramification index greater than 1. The dual divisor $\overline{D}$ to the divisor D is defined by

$$\overline{D} = (D \cdot \operatorname{div}(dx))^{-1}.$$

Lemma 4.2. *As in Lemma 4.1, let a $k[x]$-basis $\phi_1, \ldots, \phi_n$ of D^∞ and a $k[[1/x]]$-basis $\psi_1, \ldots, \psi_n$ of D_∞ be related by $\psi_i = x^{-d_i}\phi_i$. Let $\overline{\phi}_1, \ldots, \overline{\phi}_n$ and $\overline{\psi}_1, \ldots, \overline{\psi}_n$ be determined by*

$$\operatorname{Trace}_{K/k[x]}(\phi_i\overline{\phi}_j) = \delta_{i,j}, \tag{4.3}$$
$$\overline{\psi}_i = x^{d_i-2}\overline{\phi}_i. \tag{4.4}$$

Then, $\overline{\phi}_1, \ldots, \overline{\phi}_n$ is a $k[x]$-basis of $\overline{D}^\infty$ and $\overline{\psi}_1, \ldots, \overline{\psi}_n$ is a $k[[1/x]]$-basis of $\overline{D}_\infty$.

Finally we have the important theorem of Riemann and Roch. As

$$\mathfrak{R}(D) = \{f \in K \mid \operatorname{div}(f) \geq D\},$$
$$\mathfrak{R}(D^{-1}\operatorname{div}(dx)^{-1}) = \{f \in K \mid \operatorname{div}(fdx) \geq D^{-1}\},$$

this theorem relates the dimension of the space of functions with zeros at least D to the dimension of the space of differentials with poles at worst D.

Theorem 4.3. *For any function field K over $k(x)$, set g to be its genus and c the degree of the constant field extension. For any divisor D,*

$$\dim \mathfrak{R}(D^{-1}\operatorname{div}(dx)^{-1}) - \dim \mathfrak{R}(D) = \deg(D) + c(g-1).$$

For the remainder of the integration algorithm we fix, in accordance with Lemma 4.1, a $k[x]$-basis of $\eta_1, \ldots, \eta_n$ of O^∞ and (nonnegative) integers δ_i so that $x^{-\delta_1}\eta_1, \ldots, x^{-\delta_n}\eta_n$ is a $k[[1/x]]$-basis of O_∞. This basis is known as a normal integral basis. It is called integral basis because the set of functions that are regular at all finite places coincides with the set of $k[x]$-linear combinations of $\eta_1, \ldots, \eta_n$. It is further called a normal integral basis because the set of functions that are regular at all infinite places coincides with the set of $k[[1/x]]$-linear combinations of $x^{-\delta_1}\eta_1, \ldots, x^{-\delta_n}\eta_n$. Although Lemma 4.1 implies the existence of such a basis, the machinery in [6] used to calculate the basis for an arbitrary divisor is built from the existence of a such a basis for the trivial divisor. Hence, a method to calculate a normal integral basis of a function field is included in Section 7. Applying Lemma 4.1 to the trivial divisor gives the invariants c and g of the function field as

$$\begin{aligned} \#\{i|\delta_i = 0\} &= c, \\ \delta_1 + \cdots + \delta_n &= n + c(g-1). \end{aligned} \tag{4.5}$$

A given divisor D with functions $\phi_1, \ldots, \phi_n$ as a $k[x]$-basis for D^∞ and functions $\psi_1, \ldots, \psi_n$ as a $k[[1/x]]$-basis for D_∞ may be represented by two matrices $(a_{i,j}) \in k(x)^{n\times n}$ and $(b_{i,j}) \in k(x)^{n\times n}$ such that

$$\phi_i = \sum_j a_{i,j}\eta_j, \qquad \psi_i = \sum_j b_{i,j}x^{-\delta_j}\eta_j.$$

This representation is unique up to unimodular row operations on $(a_{i,j})$ in $k[x]$ and unimodular row operations on $(b_{i,j})$ in $k[[1/x]]$. Hence integral ideals may be uniquely identified once both matrices have been put into Hermite Normal Form, which dictates that the matrix $(a_{i,j})$ is upper triangular, entries on the diagonal are monic, and entries above some diagonal element have degree less than that diagonal element. Similarly, for the matrix $(b_{i,j})$, we can also require the entries on the diagonal to be monomials. It is now possible to define the norm of D as a divisor of $k(x)$ via

$$\begin{aligned} \operatorname{Norm}_{K/k(x)}(D^\infty) &= \det(a_{i,j}) \cdot k[x], \\ \operatorname{Norm}_{K/k(x)}(D_\infty) &= \det(b_{i,j}) \cdot k[[1/x]], \end{aligned}$$

which are ideals of $k[x]$ and $k[[1/x]]$, respectively. If D has the the prime factorization

$$D = \prod_{P \text{ finite}} P^{e_P} \prod_{P \text{ infinite}} P^{e_P},$$

then generators of these ideals are given by

$$\begin{aligned} \det(a_{i,j}) &= \prod_{P \text{ finite}} (x - x(P))^{e_P}, \\ \det(b_{i,j}) &= \prod_{P \text{ infinite}} (1/x)^{e_P}, \end{aligned}$$

respectively, where $x(P)$ is the x-coordinate of a place P.

The places of the function field, which were originally defined by the Puiseux series (2.1), may be now be given a simple description in term of the integral basis. If P is a prime ideal of O^∞ of degree 1, that is, $\operatorname{Norm}_{K/k(x)}(P) = x - a$ for some $a \in k$, then consider the possibilities for an ideal

basis of P. Without loss of generality, we may assume $\eta_n = 1$ in our integral basis. The Hermite Normal Form of a ideal basis of P has the upper triangular form

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ 0 & a_{1,2} & \cdots & a_{1,n} \\ \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \cdots & a_{n,n} \end{pmatrix} \begin{pmatrix} \eta_1 \\ \eta_2 \\ \vdots \\ \eta_n \end{pmatrix}.$$

Since the product of the diagonal elements is $x - a$ and $\eta_n = 1$, we must have $a_{n,n} = x - a$ and the remaining diagonal elements must be 1 since P does not contain 1. Thus, the entries above these first $n-1$ diagonal elements are all 0 and the entries above the last diagonal element are all in k. In short, P has a $k[x]$-basis $x - a, \eta_1 - a_1, \ldots, \eta_{n-1} - a_{n-1}$ for some $a_1, \ldots, a_{n-1} \in k$. Such a description of a prime ideal P allows functions in O^∞ to be evaluated at P to give an element of k via the substitutions $x \to a, \eta_1 \to a_1, \ldots, \eta_{n-1} \to a_{n-1}, \eta_n \to 1$. However, if k is not algebraically closed, it is generally not possible to find $a_i \in k$ so that $x - a, \eta_1 - a_1, \ldots, \eta_{n-1} - a_{n-1}$ generate a prime ideal of O^∞ as the a_i must arise from the values of algebraic functions. For this reason, whenever we refer to a place P of the function field K/k over some $x = a$, we assume that k has been extended if necessary to accommodate the values of the functions in the integral basis. The terms "finite place" and "degree 1 prime ideal of O^∞" become synonymous as well as "infinite place" and "degree 1 prime ideal of O_∞".

4.2. **Torsion divisors.** A necessary operation in the computation of the logarithmic term is the determination of an integer l such that the divisor D^l is principal. We should also be able to determine when this is not possible. This is accomplished by Trager via the reduction of D modulo p. After reducing the function field and our respresentation of D to some finite field of size q, the reduced divisor has some finite order bounded by $(\sqrt{q}+1)^{2g}$, which is Weil's bound [17] on the size of the divisor class group of curves over finite fields. By reducing modulo two separate primes, we can determine if the orders of the two reduced divisors are compatible with the origial divisor having finite order.

The prime for reduction must be chosen where the function field has good reduction. For example, the elliptic curve $y^2 = x^3 + px$ becomes the rational curve $y^2 = x^3$ after reducing modulo the rational prime p. This is unsatisfactory because every divisor of degree zero is principal on this reduced curve, thus the reduced divisors give no information about the original divisors on $y^2 = x^3 + px$. Sufficient conditions for the function field to have good reduction are given in [8]:

- The prime p should be greater than the degree n of the extension $K/k(x)$.
- Let $\Delta(x)$ be the monic generator of $\mathrm{Norm}_{K/k(x)}(\mathrm{div}(dx)^\infty)$. Then $\Delta(x)$ should be reducible modulo p.
- The squarefree factorization of $\Delta(x)$ should remain a square free factorization after reduction.

This last condition is the main point and ensures that the genus remains constant across the reduction process. For the function field defined over $\mathbb{Q}$ by $y^2 = x^3 + px$, the norm of (dx) is $(x^3 + px)$, which is also a squarefree factorization over $\mathbb{Q}$. After reduction modulo p, the shape of the square free factorization changes to $(x)^3$.

4.3. **The algebraic portion of the integral.** The first step in integrating an algebraic function is the removal of poles of order greater than 2 from the integrand. This is always possible for the

finite places. However, in doing so we may introduce some poles at infinite places and it may not be possible to remove all of the poles of order greater than 2 at infinite places. Thus the integration algorithm can fail at this first step.

We will always represent the integrand as a $k(x)$-linear combination of the basis $\eta_1, \ldots, \eta_n$ for O^∞. Recall that these basis elements have associated exponents $\delta_1, \ldots, \delta_n$ in the sense of Lemma 4.1. Lemma 4.4 gives the analogue of proper rational functions to the case of algebraic functions. It is the goal of this step of the integration algorithm to reduce the integral to one of this form.

Lemma 4.4. *Suppose that $b(x), a_1(x), \ldots, a_n(x)$ are relatively prime polynomials in $k[x]$. The differential $\omega = \sum_i \frac{a_i(x)}{b(x)} \eta_i dx$*

1. *satisfies $\operatorname{ord}_P(\omega) \geq -1$ at all finite places if and only if $b(x)$ is squarefree.*
2. *satsfies $\operatorname{ord}_P(\omega) \geq -1$ at all infinite places if and only if $\deg(a_i) + \delta_i < \deg(b)$ for all i.*

Proof. It is clear that ω has no poles at finite places that are not over the roots of $b(x)$. Suppose that $b(x) = (x - x_0)^k c(x)$ where $c(x)$ does not vanish at $x = x_0$. At a finite place with local coordinate $x = x_0 + t^r$, the differential has the expansion

$$\omega = \sum_i \frac{a_i}{c(x)(x - x_0)^{k-1}} \eta_i \frac{r dt}{t}.$$

Therefore,

$$\begin{aligned}
\forall_{P \text{ finite}} \operatorname{ord}_P \omega \geq -1 &\iff \forall_{P \text{ finite}} \operatorname{ord}_P \sum_i \frac{a_i}{\operatorname{Gcd}(b, b')} \eta_i \geq 0 \\
&\iff \sum_i \frac{a_i}{\operatorname{Gcd}(b, b')} \eta_i \in O^\infty \\
&\iff \forall_i \frac{a_i}{\operatorname{Gcd}(b, b')} \in k[x] \\
&\iff \operatorname{Gcd}(b, b') = 1,
\end{aligned}$$

by the assumption that $\operatorname{Gcd}(b, a_1, \ldots, a_n) = 1$ and that the η_i are an integral basis.

Similarly, at an infinite place with local coordinate $x = t^{-r}$, the differential has the expansion

$$\omega = \sum_i \frac{x a_i}{b} \eta_i \frac{-r dt}{t}.$$

Therefore,

$$\begin{aligned}
\forall_{P \text{ infinite}} \operatorname{ord}_P \omega \geq -1 &\iff \forall_{P \text{ infinite}} \operatorname{ord}_P \sum_i \frac{x a_i}{b} \eta_i \geq 0 \\
&\iff \sum_i \frac{x a_i}{b} \eta_i \in O_\infty \\
&\iff \forall_i \frac{x^{1+\delta_i} a_i}{b} \in k[[1/x]] \\
&\iff \forall_i \deg(a_i) + \delta_i < \deg(b).
\end{aligned}$$

□

Lemma 4.5 is Lemma 4.1 in [7] and is quite easy to prove. The E appearing here is actually computed in Lemma 4.6 below.

Lemma 4.5. *There is a squarefree polynomial $E \in k[x]$ and a matrix $M \in k[x]^{n\times n}$ so that*

$$Ed\eta_i = \sum_j M_{i,j}\eta_j dx.$$

As the removal of poles of order greater than 1 can always be accomplished at finite places, let us describe Trager's procedure for accomplishing this. Let the integrand be

$$\omega = \sum_i \frac{a_i(x)}{b(x)}\eta_i dx,$$

and assume that $b(x)$ is not squarefree. There exists relatively prime polynomials $U, V \in k[x]$ such that $b = UV^{l+1}$ for some $l > 0$. We seek an equation of the form

$$\int \sum_i \frac{a_i}{UV^{l+1}}\eta_i dx = \sum_i \frac{f_i}{V^l}\eta_i + \int \sum_i \frac{g_i}{UV^l}\eta_i dx, \tag{4.6}$$

which lowers the order of the multiple poles by one. A step such as this is called *Hermite Reduction*, named after Hermite [5] who introduced this technique to integrate rational functions without computing the full partial fraction decomposition in (3.2). One problem with this equation is that after differentiation, the second term may introduce poles not present in the first or last terms. All of these extra poles are contained in the square free polynomial E. Hence we must assume that the a_i and U have been multiplied by a common factor to ensure that $E|UV$. Since E is squarefree this is always possible while keeping the assumption that $\mathrm{Gcd}(U, V) = 1$. Thus assume that there is another polynomial T with $ET = UV$. Differentiating both sides of (4.6) and substituting the matrix $M_{i,j}$ in Lemma 4.5 and equating coefficients of η_i produces equations of the form

$$a_i = -lUV'f_i + T\sum_j f_j M_{j,i} \mod V.$$

Trager shows that this equation has a unique solution for the f_i modulo V (i.e. $\deg(f_i) < \deg(V)$).

We can now assume that the integrand is

$$\omega = \sum_i \frac{a_i(x)}{b(x)}\eta_i dx,$$

where $b(x), a_1(x), \ldots, a_n(x)$ are relatively prime and $b(x)$ is squarefree. This will have only simple poles at infinite places if the further hypothesis $\deg(a_i) + \delta_i < \deg(b)$ holds. If this is not the case, we seek an equation of the form

$$\int \sum_i \frac{a_i}{b}\eta_i dx = \sum_i f_i\eta_i + \int \sum_i \frac{g_i}{b}\eta_i dx, \tag{4.7}$$

for polynomials f_i and g_i with $\deg(g_i) + \delta_i < \deg(b)$. At an infinite place P with ramification index r, we have

$$\mathrm{ord}_P\left(\frac{a_i}{b}\eta_i dx\right) \geq -rN - 1, \tag{4.8}$$

where $N = \max_i(\deg(a_i) + \delta_i + 1 - \deg(b))$. Comparing the orders with those in the second term of (4.7), we arrive at

$$\deg(f_i) \leq N - \delta_i. \tag{4.9}$$

As before, we need to assume further that $E|b$ when actually solving for the f_i and g_i. Therefore, we multiply the a_i and b by a suitable common factor so that there there is a polynomial T with $b = ET$. Differentiating (4.7) produces the system of equations

$$a_i = ETf_i' + T\sum_j f_j M_{i,j} + g_i.$$

The bound in (4.9) along with the desired bound $\deg(g_i) < \deg(b) - \delta_i$ gives a linear system to be solved for the coefficients of the f_i and g_i. If this system does not have a solution, the integral is not elementary.

4.4. **The logarithmic portion of the integral.** If the algorithm of the previous section succeeds, we are left an integrand that has at worst simple poles. In order to try to cancel these poles with logarithmic terms, it is necessary to compute the locations of each of these poles. As this can be tricky when branch places are taken into account, let D_l be the divisor that collects, with multiplicity one, all places in the function field where the ramification index is exactly l. That is, we will leave D_1 undefined for now and let

$$D_l = \prod_{r(P)=l} P.$$

Lemma 4.6. *The divisors D_l are defined over k and may be computed as follows.*

- *Compute* $\operatorname{div}(dx)$ *by computing the inverse of the dual of the trivial divisor.*
- *Compute* $E(x) = \operatorname{Norm}_{K/k(x)}(\operatorname{div}(dx)^\infty)$ *and remove multiple factors via*
$$E(x) \leftarrow E(x)/\operatorname{Gcd}(E(x), E'(x))$$
- *Intialize the sequence of K-Divisors A_1 and B_1 by*
$$(A_1)^\infty = E(x)O^\infty, \quad (B_1)^\infty = (A_1)^\infty/\operatorname{div}(dx)^\infty,$$
$$(A_1)_\infty = (1/x)O_\infty, \quad (B_1)_\infty = \operatorname{div}(dx)_\infty^{-1}/(A_1)_\infty.$$
- *Define the rest of the sequences A_n and B_n by*
$$A_{n+1} = A_n/B_n, \qquad B_{n+1} = B_n + A_{n+1}.$$
- *The divisor D_n is then given by B_n/B_{n+1}.*

Proof. Let S denote the set of places over ∞ and the places over roots of $E(x)$. All of the places with ramification index greater than 1 are members of S. The claim that $D_n = B_n/B_{n+1}$ follows from the factorizations,

$$A_{n+1} = \prod_{\substack{P\in S\\ r(P)>n}} P^{r(P)-n},$$
$$B_{n+1} = \prod_{\substack{P\in S\\ r(P)>n}} P.$$

□

Now suppose that the integrand is given by the differential

$$\omega = \sum_i \frac{a_i(x)}{b(x)} \eta_i dx,$$

where $b(x)$ is squarefree and $\deg(a_i) + \delta_i < \deg(b)$ so that ω has at most simple poles. The finite places with ramification index r where ω has a simple pole must occur over the roots of $b(x)$. The ideal $b(x)O^\infty + (D_r)^\infty$ is exactly a product of these places when $r \geq 2$. In order for this formula to work correctly when $r = 1$, the ideal $(D_1)^\infty$ must be the product of the places over the root of $b(x)$ with ramification index 1. That is,

$$(D_1)^\infty = b(x)O^\infty / (b(x)O^\infty + (D_2^2)^\infty (D_3^3)^\infty \cdots),$$

where, of course, the product appearing in this formula is well-defined because it eventually terminates in O^∞. If $(D_1)_\infty$ is defined as the places over $x = \infty$ with ramification index 1, then $(D_1)_\infty$ is computed correctly in Lemma 4.6.

As the local parameter t satisfies $x = x_0 + t^r$ at a finite place P over $x = x_0$ (a root of $b(x)$) and $x = t^{-r}$ at infinite place P over $x = \infty$, the expansion of the integrand in each of these case is

$$\omega = \sum_i \frac{a_i(x)}{b'(x)} \eta_i \Big|_P \cdot \frac{r dt}{t} + \cdots, \quad \text{or}$$

$$\omega = \sum_i \frac{a_i(x) x}{b(x)} \eta_i \Big|_P \cdot \frac{-r dt}{t} + \cdots,$$

where $|_P$ denotes the value of the function at the place P, which is well-defined at these places since the function is regular there. Therefore, the differential ω has residue $z \neq 0$ at a place P if any only if P is a factor of the divisor $\delta_r(z)$, whose parts are given by

$$\delta_r(z)^\infty = (b'(x)z - r \sum_i a_i(x)\eta_i) O^\infty + b(x)O^\infty + (D_r)^\infty,$$

$$\delta_r(z)_\infty = (\frac{b(x)}{x^{\deg(b)}} z + r \sum_i \frac{a_i(x) x^{1+\delta_i}}{x^{\deg(b)}} \frac{\eta_i}{x^{\delta_i}}) O_\infty + (D_r)_\infty.$$

In order to complete the calculation of $\delta_r(z)$, it is necessary to compute a list of values of residues $z_1, \ldots, z_k$ of ω, that is, a polynomial whose roots are values of z where $\delta_r(z)$ is nontrivial. For finite places this equation is

$$\mathrm{Res}_x \left(\mathrm{Norm}(b'(x)z - r \sum_i a_i(x)\eta_i), \mathrm{Norm}(b(x)O^\infty + (D_r)^\infty) \right) = 0. \tag{4.10}$$

It must be remarked that the first norm in this equation is of an integral function in $K[z]$ hence produces a polynomial in $k[x][z]$. The presence of the transcendent z poses no problem to the calculation of this norm. The second norm is of an integral O^∞-ideal hence produce an integral ideal of $k[x]$, which we then identify with its generator. If z is a residue of the integrand, then these two polynomials in x must have a common root, so the resultant with respect to x must give a polynomial for all such residues. A similar equation for residues at infinite places holds too,

$$\mathrm{Res}_{1/x} \left(\mathrm{Norm}(\frac{b(x)}{x^{\deg(b)}} z + r \sum_i \frac{a_i(x) x^{1+\delta_i}}{x^{\deg(b)}} \frac{\eta_i}{x^{\delta_i}}), \mathrm{Norm}((D_r)_\infty) \right) = 0. \tag{4.11}$$

As before, this first norm is an element of $k[[1/x]][z]$ while the second should be interpreted as a nonegative power of $1/x$. If this power of $1/x$ is positive, the resultant should be evaluated by taking the constant term of the first norm. Otherwise, equation (4.11) is the trivial equation $1 = 0$. Now that we have constructed the divisor

$$\delta(z) = \delta_1(z)\delta_2(z)\cdots \tag{4.12}$$

in the most general case, the integration may proceed as in Section 2. This requires extending the field k by the roots z_i of the polynomials in (4.10) and (4.11), which is the smallest extension of k required to express the integral in the case that it is elementary.

5. Failing in style

We would like to present a extension to the integration algorithm in Section 4 that cannot fail. Recall the three ways the integration algorithm can fail:

(1) A nonzero integrand remains after all poles have been removed.
(2) Multiple poles at infinite places could not be removed by the algebraic portion.
(3) Simple poles in some places could not be removed by the logarithmic portion.

Since there is an infinity of places where the integrand could have simple poles, the third problem is only solvable in general by introducing normalized differentials of the third kind and working over an extension of k. This will not be pursued here. However, it will be seen that there is a choice of $2g$ integrals of the first and second kind, depending only on the given algebraic curve, such that the first and second problems can be completely avoided. More precisely, if we are allowed to add linear combinations of integrals of the second kind, then all multiple poles from the integrand can be removed. Furthermore, if the logarithmic terms successfully remove all simple poles from the integrand, then what remains is a linear combination of integrals of the first kind.

An important property of the integration algorithm thus far as described in Section 4 has been that it is rational, that is, we only compute in extensions of the base field k when it is absolutely necessary in the logarithmic terms. We will continue this trend here as well by requiring that the $2g$ integrals are defined over k and the coefficients of the relevent linear combinations are also in k. The computation of both of these should also not use any extensions of k. The only thing we assume here is that k is in fact the constant field of K, so the c in Theorem 4.3 is 1.

The procedure is immediate for elliptic integrals, which arise from the curve $y^2 = (1-x^2)(1-mx^2)$ for some complex number $m \neq 0, 1$. Any integral of the form

$$\int R(x, \sqrt{1-x^2}\sqrt{1-mx^2})dx$$

can be reduced with elementary functions to a linear combination of the standard forms

$$\begin{aligned} F(x|m) &= \int \frac{dx}{\sqrt{1-x^2}\sqrt{1-mx^2}}, \\ E(x|m) &= \int (1-mx^2)\frac{dx}{\sqrt{1-x^2}\sqrt{1-mx^2}}, \\ \Pi(x,a|m) &= \int \frac{1}{1-ax^2}\frac{dx}{\sqrt{1-x^2}\sqrt{1-mx^2}}, \end{aligned}$$

which are known as Legendre's normal elliptic integrals of the first, second, and third kinds, respectively. The integral of the third kind has another parameter a which controls the locations of the simple poles of the integrand.

In order to make an integration algorithm that can never fail on differentials with simple poles over arbitrary function fields, it would be necessary to define a collection of differentials of the third kind for an arbitrary place. These would be analogous to Legendre's integral of the third kind $\Pi(x, a|m)$. However, we will simply focus on generalizing the integrals $F(x|m)$ and $E(x|m)$ to arbitrary function fields and allow (3) above as a possible point of failure. The space of differentials, Ω, can classified into the following subspaces.

$$\begin{aligned}
\Omega_1 &= \text{first kind differentials} = \{\omega \in \Omega \mid \operatorname{ord}_P(\omega) \geq 0 \text{ for all places } P\},\\
\Omega_2 &= \text{second kind differentials} = \{\omega \in \Omega \mid \operatorname{res}_P(\omega) = 0 \text{ for all places } P\},\\
\Omega_3 &= \text{third kind differentials} = \{\omega \in \Omega \mid \operatorname{ord}_P(\omega) \geq -1 \text{ for all places } P\},\\
\Omega_{\text{ex}} &= \text{exact differentials} = \{df \mid f \in K\}.
\end{aligned}$$

Note that Ω_{ex} has only zero in common with either Ω_1 or Ω_3, while Ω_1 is the intersection of Ω_2 and Ω_3. It will also be useful to name the following subspaces, which contain differentials that are regular at the finite places.

$$\begin{aligned}
\Omega^\infty &= \{\omega \in \Omega \mid \operatorname{ord}_P(\omega) \geq 0 \text{ for all finite places } P\},\\
\Omega_2^\infty &= \{\omega \in \Omega_2 \mid \operatorname{ord}_P(\omega) \geq 0 \text{ for all finite places } P\},\\
\Omega_3^\infty &= \{\omega \in \Omega_3 \mid \operatorname{ord}_P(\omega) \geq 0 \text{ for all finite places } P\},\\
\Omega_{\text{ex}}^\infty &= \{\omega \in \Omega_{\text{ex}} \mid \operatorname{ord}_P(\omega) \geq 0 \text{ for all finite places } P\}.
\end{aligned}$$

5.1. **Spliting differentials into second and third kinds.** The normal integral basis $\eta_1, \ldots, \eta_n$ that we have been using thus far to represent functions and differentials is not sufficient anymore because we need to recognize differentials that are regular at certain places. Over $x = \infty$ there are certain places $P_1, \ldots, P_m$ whose number is $m > 0$. The divisor I that collects each of the infinite places with multiplicity one can be computed from the D_i in Lemma 4.6:

$$\begin{aligned}
I^\infty &= O^\infty,\\
I_\infty &= (D_1)_\infty (D_2)_\infty \cdots.
\end{aligned}$$

Although each of the places $P_1, \ldots, P_m$ might be defined over an extension of k, the divisors D_i are defined over k and so I is as well. By Lemma 4.1 there are is a $k[x]$-basis $\epsilon_1, \ldots, \epsilon_n$ of I^∞ and integers $\rho_1, \ldots, \rho_n$ such that $x^{-\rho_1}\epsilon_1, \ldots, x^{-\rho_n}\epsilon_n$ is a $k[[1/x]]$-basis of I_∞. The two basis may be summarized as follows.

- $\{\eta_i\}$ is a $k[x]$-basis for the functions that are regular at finite places.
- $\{x^{-\delta_i}\eta_i\}$ is a $k[[1/x]]$-basis for the functions that are regular at infinite places.
- $\{\epsilon_i\}$ is a $k[x]$-basis for the functions that are regular at finite places.
- $\{x^{-\rho_i}\epsilon_i\}$ is a $k[[1/x]]$-basis for the functions that vanish at infinite places.

The δ_i satisfy $\delta_i \geq 0$ since the two spaces have a nontrivial intersection (the constants). However, the ρ_i satisfy $\rho_i \geq 1$ since the two spaces have a trivial intersection. This important property is used in splitting up a differential into two differentials of second and third kinds. As in Lemma 4.2, the properties of the complementary bases $\overline{\eta}_1, \ldots, \overline{\eta}_n$ and $\overline{\epsilon}_1, \ldots, \overline{\epsilon}_n$ to each of the basis $\eta_1, \ldots, \eta_n$

and $\epsilon_1, \dots, \epsilon_n$, respectively, are recorded for convenience in the following lemma, which should be compared with Lemma 4.4.

Lemma 5.1. *Suppose that $b(x), a_1(x), \dots, a_n(x)$ are relatively prime polynomials in $k[x]$. The differential $\omega = \sum_i \frac{a_i(x)}{b(x)} \overline{\eta}_i dx$*

1. *satisfies $\operatorname{ord}_P(\omega) \geq 0$ at all finite places if and only if b is constant.*
2. *satisfies $\operatorname{ord}_P(\omega) \geq 0$ at all infinite places if and only if $\deg(a_i) + 2 - \delta_i \leq \deg(b)$ for all i.*

The differential $\omega = \sum_i \frac{a_i(x)}{b(x)} \overline{\epsilon}_i dx$

1. *satisfies $\operatorname{ord}_P(\omega) \geq 0$ at all finite places if and only if b is constant.*
2. *satisfies $\operatorname{ord}_P(\omega) \geq -1$ at all infinite places if and only if $\deg(a_i) + 2 - \rho_i \leq \deg(b)$ for all i.*

We will choose the most convenient of the bases $\{\eta_i\}, \{\overline{\eta}_i\}, \{\epsilon_i\}, \{\overline{\epsilon}_i\}$ for the given task at hand as there are matrices in $k(x)^{n \times n}$ for easily converting from one to the other.

Lemma 5.2. *Assume that k is the constant field of K (the c in Theorem 4.3 is 1) and let $m = \deg(I)$ denote the number of places over $x = \infty$. Then,*

1. *The k-dimension of the space Ω_1 is g.*
2. *The k-dimension of the space Ω_3^∞ is $g + m - 1$.*
3. *Let $\pi_1, \dots, \pi_{m-1}$ denote a k-basis for Ω_3^∞ modulo Ω_1. Given any $\omega \in \Omega^\infty$, there is a unique choice of the constants $r_1, \dots, r_{m-1} \in k$ so that*

$$\omega - r_1\pi_1 - \cdots - r_{m-1}\pi_{m-1} \in \Omega_2^\infty.$$

Proof. The first two assertions result from applying Theorem 4.3 to the divisors $D = 1$ and $D = I$, respectively. To cancel the residues from an arbitrary differential $\omega \in \Omega^\infty$, we can change the variable from x to $\xi := 1/x$. The local basis $x^{-\delta_1}\eta_1, \dots, x^{-\delta_n}\eta_n$ at $x = \infty$ becomes a local basis at $\xi = 0$, and Hermite Reduction (4.6) can be used to reduce the poles over $\xi = 0$ to simple poles. In doing so, we may introduce poles over $x = 0$, but these are poles from an exact differential, hence do not contribute any residues. Thus, assume now that we have a function $f \in K$ and another differential $\sigma \in \Omega$ with at worst simple poles over $x = \infty$ with

$$\omega = df + \sigma.$$

The constants $r_1, \dots, r_{m-1} \in k$ need to be chosen so that

$$\sigma - r_1\pi_1 - \cdots - r_{m-1}\pi_{m-1}$$

has no poles at infinite places. By the first part of Lemma 5.1, enforcing this condition is equivalent to solving linear equations over k for the r_i. □

Lemma 5.3. *Given any $\omega \in \Omega$ there are $f \in K$ and $\omega_2^\infty \in \Omega_2^\infty$ and $\omega_3 \in \Omega_3$ such that*

$$\omega = df + \omega_2^\infty + \omega_3. \tag{5.1}$$

The resulting ω_3 is unique up to the addition of first kind differentials.

Proof. Note that we may assume ω has at worst simple poles at the finite places by Hermite Reduction (4.6). The removal of the multiple poles at finite places contributes to the term df in (5.1). Now that ω has at worst simple poles at finite places, set $f = 0$ and write ω in the form

$$\omega = \sum_i \frac{a_i(x)}{b(x)} \overline{\epsilon}_i dx,$$

where $b(x), a_1(x), \ldots, a_n(x)$ are relatively prime polynomials in $k[x]$. There are unique polynomials f_i and g_i in $k[x]$ with $\deg(g_i) < \deg(b)$ and $a_i = bf_i + g_i$. Thus,

$$\omega = \sum_i f_i \overline{\epsilon}_i dx + \sum_i \frac{g_i}{b} \overline{\epsilon}_i dx.$$

This is not necessarily the form required by the lemma as the first term on the right hand side may have nonzero residues. These can be eliminated by an application of Lemma 5.2. Thus there are constants $r_1, \ldots, r_{m-1} \in k$ such that

$$\omega_2^\infty = \sum_i f_i \overline{\epsilon}_i dx - r_1\pi_1 - \cdots - r_{m-1}\pi_{m-1} \in \Omega_2^\infty,$$
$$\omega_3 = \sum_i \frac{g_i}{b} \overline{\epsilon}_i dx + r_1\pi_1 + \cdots + r_{m-1}\pi_{m-1} \in \Omega_3.$$

The first term in ω_3 has at worst simple poles at infinite places by the second part of Lemma 5.1 and the requirement $\deg(g_i) < \deg(b)$ (recall that the ρ_i are positive). There are no multiple poles at finite places in ω_3 because of the assumption on ω and the construction of ω_2^∞. □

5.2. **Resolving second kind differentials into normal forms.** In Section 5.1 an arbitrary differential was split into an exact differential (Ω_{ex}), a differential with poles only at the infinite places and no residues (Ω_2^∞), and a differential with at worst simple poles (Ω_3). We would now like to compute differentials $\gamma_1, \ldots, \gamma_g \in \Omega_2^\infty$ so that any $\omega \in \Omega_2^\infty$ can be represented in the form

$$\omega = df + c_1\gamma_1 + \cdots + c_g\gamma_g \tag{5.2}$$

for some $f \in K$ and $c_i \in k$. We will first follow the standard construction over the algebraic closure of k [18] and then see how these γ_i can be chosen over k. The construction starts with g (distinct) places $P_1, \ldots, P_g$ such that the divisor $N = P_1 \cdots P_g$ is nonspecial. A divisor N is called special if there is a differential of the first kind that vanishes at all the places of N, or more precisely,

$$\dim \mathfrak{R}(N \operatorname{div}(dx)^{-1}) > 0.$$

Select g basis elements $\mu_1 \ldots, \mu_g$ of Ω_1. The divisor $P_1, \ldots, P_g$ is special if and only if there are constants $c_1, \ldots, c_g$, not all zero, such that $c_1\mu_1 + \cdots + c_g\mu_g$ vanishes at the places $P_1, \ldots, P_g$, or

$$\det \begin{vmatrix} \mu_1|_{P_1} & \cdots & \mu_g|_{P_1} \\ \vdots & \ddots & \vdots \\ \mu_1|_{P_g} & \cdots & \mu_g|_{P_g} \end{vmatrix} = 0$$

This determinant cannot vanish for generic places $P_1, \ldots, P_g$, for otherwise the differentials $\mu_1 \ldots, \mu_g$ would not be linearly independent. We can thus choose places $P_1, \ldots, P_g$, defined over some finite Galois extension $\overline{k}$ of k, such that this determinant is nonzero. The function field K and space of differentials $\Omega, \Omega_1, \ldots$ extend naturally to $\overline{K}$ and $\overline{\Omega}, \overline{\Omega}_1, \ldots$ via this extension of the constant field. One only needs to check that an integral basis for K/k remains an integral basis for $\overline{K}/\overline{k}$, which is true by the hypothesis that k is the exact constant field of K.

Recall that $N = P_1 \cdots P_g$. Applying Theorem 4.3 to the divisor $D = N$ produces

$$\dim(\mathfrak{R}(N^{-1} \operatorname{div}(dx)^{-1})) - 0 = 2g - 1,$$

while applying it again to the divisor $D = N^2$ produces

$$\dim(\mathfrak{R}(N^{-2} \operatorname{div}(dx)^{-1})) - 0 = 3g - 1.$$

Thus there are linearly independent differentials $\overline{\gamma}_1, \ldots, \overline{\gamma}_g \in \overline{\Omega}_2$ with double poles at the places $P_1, \ldots, P_g$ (and zero residue).

Lemma 5.4. *The differentials $\overline{\gamma}_1, \ldots, \overline{\gamma}_g$ are a basis for $\overline{\Omega}_2/(\overline{\Omega}_{\text{ex}} + \overline{\Omega}_1)$*

Proof. Applying Theorem 4.3 to the divisor $D = N^{-1}$ gives

$$0 - \dim \mathfrak{R}(N^{-1}) = -g + g - 1$$

where we have used the construction $\dim \mathfrak{R}(N \operatorname{div}(dx)^{-1}) = 0$. Thus $\mathfrak{R}(N^{-1})$ has dimension 1 and consists of only the constants, and there are no functions whose differentials can cancel even one pole from any linear combination of the $\overline{\gamma}_i$. This means that the $\overline{\gamma}_i$ are linearly independent modulo $\overline{\Omega}_{\text{ex}} + \overline{\Omega}_1$. Next take any differential $\omega \in \overline{\Omega}_2$ and assume that its divisor of poles has the form

$$P_1^{e_1+1} \cdots P_g^{e_g+1} P_{g+1}^{e_{g+1}+1} \cdots P_l^{e_l+1},$$

where each e_i is at least 1. This assumption on the e_i for $i \leq g$ can be assured by adding $\overline{k}$-linear combinations of the $\overline{\gamma}_i$ to ω. Set $M = P_1^{e_1} \cdots P_l^{e_l}$. Applying Theorem 4.3 to the divisor $D = M^{-1}$ gives

$$0 - \dim \mathfrak{R}(M^{-1}) = -(e_1 + \cdots + e_l) + g - 1,$$

where we have used the fact that M is a multiple of N and hence also non-special. Thus

$$\dim \mathfrak{R}(M^{-1}) = 1 + (e_1 - 1) + \cdots + (e_g - 1) + e_{g+1} + \cdots + e_l.$$

This provides enough functions to guarantee that we can cancel one of the poles of ω by an exact differential df (where $f \in \mathfrak{R}(M^{-1})$) and thus reduce one of the e_i by 1. If we first reduce the e_i for $i > g$ and then reduce the e_i for $i \leq g$ we can inductively produce exact differentials that reduce ω to double poles at the places $P_1, \ldots, P_g$, in which case it is a linear combination of the $\overline{\gamma}_i$ and differentials of the first kind. □

Having chosen differentials $\overline{\gamma}_1, \ldots, \overline{\gamma}_g$ over some extension $\overline{k}$ of k that are a basis for $\overline{\Omega}_2/(\overline{\Omega}_{\text{ex}}+\overline{\Omega}_1)$, we may apply Hermite Reduction (4.6) to assume that $\overline{\gamma}_1, \ldots, \overline{\gamma}_g$ have poles only at the infinite places and are thus a basis for $\overline{\Omega}_2^{\infty}/(\overline{\Omega}_{\text{ex}}^{\infty} + \overline{\Omega}_1)$. It is now a relatively simple matter to compute the differentials $\gamma_1, \ldots, \gamma_g$ as required in (5.2).

Lemma 5.5. *Set $r = \max_i \delta_i$ and let $M \in k[x]^{n \times n}$ denote the derivative matrix of the basis $\{\eta_i\}$ in the basis $\{\overline{\epsilon}_i\}$, that is, $d\eta_i = \sum_j M_{i,j}\overline{\epsilon}_j dx$. A set $\gamma_1, \ldots, \gamma_g$ of representatives of the differentials of the second kind may be chosen from the set*

$$S := \{x^{l+\rho_i-1}\overline{\epsilon}_i dx\}_{\substack{1 \leq i \leq n \\ 0 \leq l \leq r-1}}.$$

The representatives need to be chosen so that they are linearly independent over k modulo the k-span of the set

$$T := \{[lx^{l-1}]_i \overline{\epsilon}_i dx + \sum_j [x^l M_{i,j}]_j \overline{\epsilon}_j dx\}_{\substack{1 \leq i \leq n \\ 0 \leq l \leq r-\delta_i}},$$

where $[\sum_{j \geq 0} c_j x^j]_i$ denotes $\sum_{j \geq \rho_i - 1} c_j x^j$. After choosing such representatives from S, the residues at the infinite places need to be removed via Lemma 5.2.

Proof. The elements of T are representatives for $d(x^l\eta_i)$ modulo Ω_3^∞, while by Lemma 5.1 the elements of S are linearly independent modulo Ω_3^∞. Hence it suffices to show that the dimension of $\mathrm{span}_k(S)$ modulo $\mathrm{span}_k(T)$ is exactly g.

Differentials in Ω_2^∞ that have too many poles may be removed from consideration as Hermite Reduction is possible once a large number of poles are present. It see this, set $\theta_i = x^{-\delta_i}\eta_i$ and $\xi = 1/x$. The θ_i are a $k[\xi]$-basis for the function that are regular everywhere except possibly at the places over $x = 0$. If we are given a differential $\omega \in \Omega^\infty$ with $x^{-l-1}\omega$ regular at the infinite places, then Hermite Reduction implies an equation of the form

$$\int \omega = \int \sum_i \frac{a_i}{\xi^{l+1}}\theta_i d\xi = \sum_i \frac{f_i}{\xi^l}\theta_i + \int \sum_i \frac{g_i}{\xi^l}\theta_i d\xi.$$

The first term on the right hand side (and hence the second as well) will be regular at the finite places provided $l \geq \delta_i$ for each i. Thus, if r denotes the maximum δ_i, the set

$$\Omega_2^\infty(r) = \{\omega \in \Omega^\infty \mid x^{-r}\omega \text{ is regular at all infinite places}\}$$

still spans the entire space $\Omega^\infty/\Omega_{\mathrm{ex}}^\infty$. Note that we still get a spanning set via

$$\{\omega \in \Omega^\infty \mid \mathrm{ord}_P(x^{-r}\omega) \geq -1 \text{ for all infinite places } P\},$$

and S gives a basis for this space modulo Ω_3^∞ by the second part of Lemma 5.1. For a function f that is regular at all finite places, the condition that $\mathrm{ord}_P(x^{-r}df) \geq -1$ for all infinite places P is certainly implied by the condition that $x^{-r}f$ be regular at all infinite places. This latter space of functions is exactly $\mathrm{span}_k(T)$. Hence we have shown that $\mathrm{span}_k(S)$ spans $\Omega^\infty/(\Omega_3^\infty + \Omega_{\mathrm{ex}}^\infty)$ and any linear combination of elements of S that are an exact differential modulo Ω_3^∞ must be in $\mathrm{span}_k(T)$.

Now that an effective procedure has been given for choosing $\gamma_1, \ldots, \gamma_g$, we must show that exactly g differentials are obtained. First let us show that at least g differentials are obtained. The differentials $\overline{\gamma}_1, \ldots, \overline{\gamma}_g \in \overline{\Omega}$ are contained in $\overline{\Omega}_2^\infty(l)$ for some l. As $\Omega_2^\infty(l)$ has a basis $\gamma_1, \ldots, \gamma_j \in \Omega$, if all sets of g differentials in $\Omega_2^\infty(l)$ were linearly dependent over k (modulo $\Omega_{\mathrm{ex}}^\infty + \Omega_1$), then the differentials $\overline{\gamma}_1, \ldots, \overline{\gamma}_g$ could not be linearly independent over $\overline{k}$ (modulo $\overline{\Omega}_{\mathrm{ex}}^\infty + \overline{\Omega}_1$) as they are $\overline{k}$-linear combinations of $\gamma_1, \ldots, \gamma_j$ (modulo $\Omega_{\mathrm{ex}}^\infty + \Omega_1$).

Finally, let us show that no more than g differentials are obtained. Suppose $\gamma_1, \ldots, \gamma_{g+1} \in \Omega_2^\infty$ were k-linearly independent modulo $\Omega_{\mathrm{ex}}^\infty + \Omega_1$. As they are $\overline{k}$-linearly dependent modulo $\overline{\Omega}_{\mathrm{ex}}^\infty + \overline{\Omega}_1$, there are constants $c_i \in \overline{k}$, a function $f \in \overline{K}$ and a differential of the first kind $\omega \in \overline{\Omega}_1$, such that

$$\gamma_1 + c_2\gamma_2 + \cdots + c_g\gamma_g + c_{g+1}\gamma_{g+1} = df + \omega,$$

where the coefficient of γ_1 has been assumed to be 1 without loss of generality. If σ denotes an automorphism of $\overline{k}/k$, then, as the γ_i are in Ω and hence fixed by σ, there is an equation of the form

$$\gamma_1 + \sigma(c_2)\gamma_2 + \cdots + \sigma(c_g)\gamma_g + \sigma(c_{g+1})\gamma_{g+1} = d\sigma(f) + \sigma(\omega).$$

Summing this equation over all automorphisms σ of $\overline{k}/k$ shows that $\gamma_1, \ldots, \gamma_{g+1}$ are k-linearly dependent modulo $\Omega_{\mathrm{ex}}^\infty + \Omega_1$.

□

5.3. **Resolving third kind differentials into normal forms.** We begin with the fundamental result that if the residues of a differential of the third kind are all integers, then the poles and residues can be arbitrarily prescribed as long as the sum of the residues is zero.

Lemma 5.6. *Let D be a degree zero divisor of $K/k(x)$. Up to the addition of differentials of the first kind, there exists a unique differential $\omega \in \Omega_3(K)$ with*

$$\operatorname{res}_P \omega = \operatorname{ord}_P D,$$

for all places P.

Proof. First let us extend k (and K) to $\overline{k}$ so that each place with $\operatorname{ord}_p D \neq 0$ is defined over $\overline{k}$. Let

$$L = \prod_{\operatorname{ord}_P D \neq 0} P.$$

The desired ω, if it exists, is an element of $\mathfrak{R}(L^{-1}(dx)^{-1})$. Since this space modulo $\Omega_1(\overline{K})$ has dimension $\deg L - 1$, it is easy to see that there a unique ω whose order at the places P in L have residue $\operatorname{ord}_P(D)$. For example, we can force all but one of the places to have to correct residue since we have $\deg L - 1$ independent differentials to work with. Once this is accomplished, the remaining place has the correct residue because the sum of the residues of any differential is zero and D is a divisor of degree zero. The differential ω just constructed is also defined over k (up to the addition of integrals of the first kind) because if $\sigma \in \operatorname{Gal}(\overline{k}/k)$ then

$$\operatorname{res}_P \sigma(\omega) = \operatorname{res}_{\sigma^{-1}(P)} \sigma(\omega) = \operatorname{ord}_{\sigma^{-1}(P)} D = \operatorname{ord}_P D,$$

because D itself is defined over k. Thus ω is fixed by all $\sigma \in \operatorname{Gal}(\overline{k}/k)$ and so is defined over k. □

Now consider the problem of computing the ω of Lemma 5.6 while staying in k for all calculations. First write

$$D = \prod_{i \neq 0} A_i^i, \quad A_i \geq 0, \quad A_i + A_j = 1,$$
$$L = \prod_{i \neq 0} A_i.$$

This squarefree decomposition can be performed over k using the algorithm for computing the radical of a divisor in Chapter 2 of [7]. Thus, assume that we have $\deg(L) - 1 + g$ functions $f_j \in O_\infty$ and a squarefree common denominator $b \in k[x]$ so that $\{f_j/b\}_j$ is a k-basis for $\mathfrak{R}(L^{-1}(dx)^{-1})$. Set $F = \sum_j c_j f_j$ for some constants c_j that are yet to be determined. Since the formula for the residues of F/b at a place P depends on the ramification index of P, it will be necessary to further decompose each A_j as $A_j = \prod_{r=1}^n A_{j,r}$ where $A_{j,r} = A_j \cap D_r$ for $r > 1$ (recall that D_r is the divisor of places with ramification index r and is computed in 4.6). The condition $\operatorname{res}_P F/b dx = \operatorname{ord}_P(D)$ for all places P is now equivalent to

$$rF - ib' \in (A_{i,r})^\infty,$$
$$x^{-\deg b}(rxF + ib) \in (A_{i,r})_\infty.$$

Since the condition that a function $g \in O^\infty$ vanish at all finite places of a squarefree integral divisor A is equivalent to $g \in A^\infty$. If the ideal basis for A is given in upper triangular form as

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ 0 & a_{1,2} & \cdots & a_{1,n} \\ \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \cdots & a_{n,n} \end{pmatrix} \begin{pmatrix} \eta_1 \\ \eta_2 \\ \vdots \\ \eta_n \end{pmatrix},$$

and g is written as $\sum_i g_i \eta_i$, then

$$\begin{aligned} g_1 &= h_1 a_{11} \\ g_2 &= h_1 a_{12} + h_2 a_{22} \\ g_n &= h_1 a_{1n} + h_2 a_{2n} + \cdots + h_n a_{nn} \end{aligned}$$

for some $h_i \in k[x]$. These conditions (i.e. g_1 is divisible by a_{11}, $g_2 - (g_1/a_{11})a_{12}$ is divisible by a_{22}, ect.) translate to linear conditions on the constants c_j. Since we know this system has a solution space of dimension $g+1$, we can solve for the constants c_j over k by simple linear algebra and recover a solution for ω.

6. Examples

Example 6.1. *This first example is meant only to illustrate several of the data structures used by the integration algorithm; no integration will be performed. Consider the function field $\mathbb{Q}(x,y)/\mathbb{Q}(x)$ defined by the curve*

$$x^3 y + x + y^3 = 0.$$

A normal integral basis is given by $\eta_1 = 1, \eta_2 = y, \eta_3 = y^2$ with the corresponding exponents $\delta_1 = 0, \delta_2 = 2, \delta_3 = 3$. We have $c = 1$, which means that there are no new constants in $\mathbb{Q}(x,y)$. The genus of the curve is also given by (4.5) as $g = 3$. The matricies $((a_{i,j}),(b_{i,j}))$ for the divisors D_1, D_2 and D_3 as computed in Lemma 4.6 are

$$D_1 = \left(\begin{pmatrix} 1 & 0 & -\frac{x^4}{9} \\ 0 & 1 & -\frac{x^2}{3} \\ 0 & 0 & x^7 + \frac{27}{4} \end{pmatrix}, \begin{pmatrix} 1/x & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right),$$

$$D_2 = \left(\begin{pmatrix} 1 & 0 & -\frac{4x^4}{9} \\ 0 & 1 & \frac{2x^2}{3} \\ 0 & 0 & x^7 + \frac{27}{4} \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1/x \end{pmatrix} \right),$$

$$D_3 = \left(\begin{pmatrix} x & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right).$$

From these divisors we can gather the important information:

- *There is one place with $r = 1$ and another place with $r = 2$ over each of the roots of $4x^3 + 27 = 0$.*
- *There is one place with $r = 1$ and another place with $r = 2$ over $x = \infty$.*
- *There is one place with $r = 3$ over $x = 0$.*

Setting I to be the divisor of places at infinity, we find that $\epsilon_1 = 1, \epsilon_2 = y, \epsilon_3 = y^2$ is a normal basis for I as in Lemma 4.1 with exponents $\rho_1 = 1, \rho_2 = 2, \rho_3 = 4$. A basis of the differentials of the first kind (Ω_1) is given by

$$\begin{aligned} -\overline{\eta}_2 dx &= \frac{2x^5y + 6x^3 + 9y^2}{4x^8 + 27x} dx, \\ \overline{\eta}_3 dx &= \frac{4x^5 + 6x^2y^2 - 9y}{4x^8 + 27x} dx, \\ x\overline{\eta}_3 dx &= \frac{4x^5 + 6x^2y^2 - 9y}{4x^7 + 27} dx. \end{aligned}$$

As there are two place over $x = \infty$, the single differential of the third kind (a basis for Ω_3^∞/Ω_1) is given by

$$x^2\overline{\eta}_3 dx = \frac{4x^6 + 6x^3y^2 - 9xy}{4x^7 + 27} dx.$$

The derivatives of the functions $\{x^l\eta_i\}_{0\le l\le 3-\delta_i}$ modulo Ω_3^∞ are given in the rows of the following matrix in terms of the basis $\overline{\eta}_1, \overline{\eta}_2, \overline{\eta}_3$.

$$\begin{pmatrix} 3 & 0 & -2x^3 \\ 6x & 0 & -4x^4 \\ 9x^2 & 0 & -6x^5 \\ 0 & -3x^2 & 0 \\ 0 & -5x^3 & 0 \\ -6x^2 & 0 & 6x^5 \end{pmatrix}$$

We can then choose a basis for the differentials of the second kind ($\Omega_2^\infty/(\Omega_{\text{ex}}^\infty + \Omega_3^\infty)$) from the differentials $\{x^l\overline{\eta}_i\}_{\rho_i-1\le l\le\rho_i+1}$. By choosing these to be linearly independent over $\mathbb{Q}$ from the rows of the above matrix, we find a possible basis as

$$\begin{aligned} \overline{\eta}_1 dx &= \frac{4x^7 + 4x^4y^2 - 6x^2y + 9}{4x^7 + 27} dx, \\ -x\overline{\eta}_2 dx &= \frac{2x^5y + 6x^3 + 9y^2}{4x^7 + 27} dx, \\ x\overline{\eta}_1 dx &= \frac{4x^8 + 4x^5y^2 - 6x^3y + 9x}{4x^7 + 27} dx. \end{aligned}$$

Note that the number of these differentials is the same as the genus of the curve (3).

Example 6.2. *We will split the integral*

$$\int \sqrt{x(x+5)(x-4)(x-3)}dx$$

into a algebraic term, an integral of the second kind, a logarithmic term, and an integral of the first kind. The function field is $K = \mathbb{Q}(x, y)$ where $y^2 = x(x+5)(x-4)(x-3)$. A normal integral basis for $K/\mathbb{Q}(x)$ is given by

$$\begin{aligned} \eta_1 = 1, \quad \eta_2 = y, \\ \delta_1 = 0, \quad \delta_2 = 2. \end{aligned}$$

By (4.5)*, we have* $c = 1$ *and* $g = 1$*. The matricies* $((a_{i,j}), (b_{i,j}))$ *for the divisors* D_1 *and* D_2 *as computed in Lemma 4.6 are*

$$D_1 = \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1/x & 0 \\ 0 & 1/x \end{pmatrix} \right),$$
$$D_2 = \left(\begin{pmatrix} x(x+5)(x-4)(x-3) & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right).$$

Since the genus is 1*, there is one differential of the first kind and one differential of second kind. Since there are two infinite places, there is also one differential of third kind.*

$$\frac{y}{x(x+5)(x-4)(x-3)}dx \text{ is a basis of } \Omega_1$$
$$\frac{xy}{x(x+5)(x-4)(x-3)}dx \text{ is a basis of } \Omega_3^\infty/\Omega_1$$
$$\frac{(x^2-x)y}{x(x+5)(x-4)(x-3)}dx \text{ is a basis of } \Omega_2^\infty/(\Omega_{\text{ex}}^\infty + \Omega_3^\infty)$$

The multiple poles over infinite places cannot be removed without using this differential of the second kind. That is,

$$\int y dx = \frac{(2x-1)y}{6} - \frac{49}{6}\int \frac{(x^2-x)y}{x(x+5)(x-4)(x-3)}dx + \int \frac{(18x+5)y}{x(x+5)(x-4)(x-3)}dx.$$

This last integral has at worst simple poles by Lemma 4.4. We can now attempt to remove the simple poles by logarithmic terms. Equation (4.11) *with* $r = 1$ *is*

$$\begin{aligned} &\text{Norm}\left(\frac{x(x+5)(x-4)(x-3)z + (18x+5)xy}{x^4}\right)\Big|_{x=\infty} \\ &= \left(z^2 - 324\right) + \frac{468 - 4z^2}{x} + \frac{7787 - 42z^2}{x^2} + \cdots\Big|_{x=\infty} \\ &= z^2 - 324 = 0. \end{aligned}$$

Therefore, the integrand has residues ± 18 *above the two infinite places. A* $\mathbb{Q}$*-basis of the residues is given by* $b_1 = 18$ *and the matrix* m *is* $\binom{+1}{-1}$*. In our double matrix representation the divisor* $\frac{\delta(+18)}{\delta(-18)}$ *is*

$$\frac{\delta(+18)}{\delta(-18)} = \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} x & x+1 \\ 0 & 1/x \end{pmatrix} \right).$$

Normal bases for powers of this divisor in the sense of Lemma 4.1 are given along with their exponents in the following table.

divisor	*normal basis*	*exponents*
$\frac{\delta(+18)}{\delta(-18)}$	1	1
	$x^2 - x + y$	1
$\frac{\delta(+18)^2}{\delta(-18)^2}$	$x^2 - x + y - 12$	1
	$2x^3 + x^2 - 27x + (2x+3)y$	1
$\frac{\delta(+18)^3}{\delta(-18)^3}$	$x^3 + 2x^2 - 15x - 18 + (x+3)y$	0
	$2x^3 + x^2 - 27x + (2x+3)y$	2

Since the third power has a basis element with nonpositive exponent,

$$\frac{\delta(+18)^3}{\delta(-18)^3} = \operatorname{div}(x^3 + 2x^2 - 15x - 18 + (x+3)y),$$

and the poles at infinite places may be eliminated with logarithmic terms. It follows that

$$\int \frac{(18x+5)y}{x(x+5)(x-4)(x-3)}dx = 6\log(x^3 + 2x^2 - 15x - 18 + (x+3)y) + 35\int \frac{y}{x(x+5)(x-4)(x-3)}dx,$$

and the remaining integral is the integral of the first kind for this function field.

Example 6.3. *In this example we briefly indicate how*

$$\int \frac{2x^2 - x}{\sqrt{x^6 + 6(x-1)^3}}dx$$

may be shown to be nonelementary. There are two infinite places A and B in the relevent function field $\mathbb{Q}(x, \sqrt{x^6 + 6(x-1)^3})$ where the integrand has nonzero residue. Set $D = A/B$. Then after reducing D modulo 11, we find that it has order 24. Also, after reducing D modulo 13, we find that it has order 39. When a divisor of finite order is reduced modulo p, its order can only decrease by a factor that is a nonnegative power of p. Since the order 24 results after reduction modulo 11 and the order 39 results after modulo 13, the original divisor D cannot have finite order as $24 \cdot 11^a = 39 \cdot 13^b$ is not solvable in nonnegative integers a and b.

Example 6.4. *We evaluate*

$$\int \frac{54x^7 - 27x^5y + 27x^4y^3 + 108x^4 + 36x^3y^2 + 48x^2y + 144xy^3 + 320x + 192y^2}{x^2(27x^6 + 256)}dx$$

on $y^4 + x^3y - x^2 = 0$, which was discussed in [11, Section 5.2].

7. Representation of function fields and integral bases

The workhorse of the integration algorithm is the integral bases for the function field. Once such a basis has been found, the integration algorithm is essentially a large problem in polynomial linear algebra over the base field k or possible finite extensions thereof. This section presents methods to recognize functions fields and calculate their integral bases.

7.1. **Function algebras.** In general, the functions to be integrated will be presented as $R(x, y_1, y_2, ...)$, with some defining polynomials for the y_i with coefficients in $k(x)$. This immediately presents the problem of zero divisors. Suppose we adjoin y_1 with defining equation $(y_1^2 - x)^2 - x = 0$ and adjoin y_2 with defining equation $y_2^4 - x = 0$. Using only the defining equations, the element $x - y_1^2 - y_2^2$ is seen to be nonzero. However, it is a zero divisor as

$$(x - y_1^2 - y_2^2)(x - y_1^2 + y_2^2) \equiv 0 \mod ((y_1^2 - x)^2 - x, y_2^4 - x).$$

Thus, the functions to be integrated should be consided as elements of what we will call a *function algebra*, which generalizes function fields to allow zero divisors. We only require that the defining equations are squarefree. The following definition is essentially that of an étale algebra over $k(x)$ as presented in Proposition 2.1.1 of [14].

Definition 7.1. *A is called a function algebra over $k(x)$ if A is a finite-dimensional commutative $k(x)$-algebra with any of the following three equivalent properties.*

1. *A has no nonzero nilpotent elements.*
2. *The equation $a^2 = 0$ in A implies $a = 0$.*
3. *The minimum polynomial over $k(x)$ of any element $a \in A$ is squarefree.*

As mentioned in [14, pg. 50], there are two main ways of representing function fields. The first of these methods uses matrices to represent the multiplication of basis elements, and we call it the matrix representation (M). The second method uses a defining polynomial for a primitive element, and we call this the polynomial representation (P). Both representations have advantages and disadvantages with respect to the operations required for integration.

Lemma 7.2. *A function algebra of dimension n may be identified by either of the following equivalent data.*

(M) *A list of $k(x)$-basis elements $e_1, \ldots, e_n$ along with n^3 elements $a_{i,j,l}$ of $k(x)$ such that $e_i e_j = \sum_l a_{i,j,l} e_l$.*

(P) *A primitive element y such that $A \simeq k(x)[y]/T(y)$ where $T(y) \in k(x)[y]$ is a monic squarefree polynomial (but not necessarily irreducible).*

The following procedure for composing two function algebras is essentially Proposition 2.1.7 of [14]. The adaptation from number fields to function fields (or even function algebras) follows through without any difficulties.

Lemma 7.3. *The compositum A_1A_2 of two functions algebras A_1 and A_2 may be calculated as follows.*

(M) *Suppose that $e_1, \ldots, e_n$ is a $k(x)$-basis of A_1 with multiplication array a and that $f_1, \ldots, f_m$ is a $k(x)$-basis of A_2 with multiplcation array b. The mn elements $\{e_i f_{i'}\}_{i,i'}$ are a $k(x)$-basis of A_1A_2. The rule for multiplying these basis elemens may be derived from the rules for multiplying the e_i and f_j by*

$$\begin{aligned}(e_i f_{i'})(e_j f_{j'}) &= (e_i e_j)(f_{i'} f_{j'}) \\ &= \sum_l a_{i,j,l} e_l \sum_{l'} b_{i',j',l'} f_{l'} \\ &= \sum_{l,l'} a_{i,j,l} b_{i',j',l'} e_l f_{l'}.\end{aligned}$$

(P) *Let A_1 have primitive element y_1 with defining polynomial T_1 and let A_2 have primitive element y_2 with defining polynomial T_2. There is an integer l such that*

$$T(y) = \mathrm{Res}_{y_1}(T_1(y_1), T_2(y - ly_1))$$

is squarefree and is a defining polynomial for A_1A_2. The primitive element for A_1A_2 may be identified with $ly_1 + y_2$.

Let A be a function algebra of dimension n over $k(x)$ with basis $e_1, \ldots, e_n$. Each function f in A operates on a basis of A by matrix multiplication, that is,

$$fe_i = \sum_j M_{i,j} e_j, \text{ where } M = M(f) \in k(x)^{n \times n}.$$

As the characteristic polynomial of M is independent of the basis used, we may define the norm and trace of f as

$$\begin{aligned}\mathrm{Trace}(f) &= \mathrm{trace}(M),\\ \mathrm{Norm}(f) &= \det(M).\end{aligned}$$

In the process of recognizing the function fields inside of a function algebra, it will be necessary to compute the places of the function algebra. This is trivial in the polynomial representation as places may be identified by their $(x = a, y = b)$ coordinates as long as the denominators of the elements of the integral basis do not vanish at $x = a$. This is a slightly subtler issue in the matrix representation. Recall from Section 4.1 that calculating the places over $x = a$ amounts to calculating $a_1, \ldots, a_n \in k$ so that $x - a, \eta_1 - a_1, \ldots, \eta_n - a_n$ generate a proper ideal of O^∞, where η_i is an integral basis. The two functions $x - a$ and $\eta_i - a_i$ generate all of O^∞ unless the polynomial $\mathrm{Norm}(\eta_i - a_i) \in k[x]$ has $x = a$ as a root. Let $M_i \in k[x]^{n\times n}$ be the matrix above describing the operation of η_i on the basis $\eta_1, \ldots, \eta_n$. As each a_i must be an eigenvalue of $M_i|_{x=a}$, there is a finite list of possible values of each the a_i. Suppose that $a_1, \ldots, a_r$ with $r < n$ have been chosen so that $x - a, \eta_1 - a_1, \ldots, \eta_r - a_r$ generate a proper ideal Q. Choose one of the possibilities for a_{r+1} so that adding $(\eta_{r+1} - a_{r+1})O^\infty$ to Q still gives a proper ideal. All of the places over $x = a$ may be enumerated in this way, and the process is fairly efficient as the entries of Q never exceed linear polynomials when expressed in Hermite Normal Form.

Let us return to the example of the compositum of the function fields defined by $(y_1^2 - x)^2 - x = 0$ and $y_2^4 - x = 0$. The problem is that there are two *components* where either $x - y_1^2 - y_2^2$ or $x - y_1^2 + y_2^2$ is zero. As zero divisors would cause problems when performing the integration algorithm, we need to recognize these two components so that the algorithm may proceed over a field. The key to recognizing the components lies in the constants of the function algebra. If the defining equation for the function algebra has m absolutely irreducible factors, we call the function fields defined by each of these factors the components of the function algebra. However, it is not necessary to compute a defining polynomial for the function algebra and then directly factor it over the algebraic closure of its coefficient field. This is due to the following obsevation, as used in [4]: the number of components of the function algebra is the same as the dimension of its space of constants. For example, the function fields defined by $(y_1^2 - x)^2 - x = 0$ and $y_2^4 - x = 0$ have respective normal integral bases $\{1, y_1, y_1^2, y_1^3 - xy_1\}$ and $\{1, y_2, y_2^2, y_2^3\}$ with exponents $\{0, 1, 1, 1\}$ in both cases. If we form the compositum by the first method of Lemma 7.3 and then calculate a normal integral basis by Lemma 7.5, the resulting basis elements and exponents are given by

basis element	1	$\frac{xy_2^2 - y_1^2y_2^2}{x}$	y_2	y_2^3	y_1	y_1y_2	$y_1y_2^2$	$\frac{y_1y_2^3}{x}$
exponent	0	0	1	1	1	1	1	1
basis element	y_1^2	$y_1^2y_2 - xy_2$	$\frac{y_1^2y_2^2}{x}$	$\frac{y_1^2y_2^3}{x}$	$y_1^3 - xy_1$	$\frac{y_1^3y_2 - xy_1y_2}{x}$	$\frac{y_1^3y_2^2 - xy_1y_2^2}{x}$	$\frac{y_1^3y_2^3 - xy_1y_2^3}{x}$
exponent	1	1	1	1	1	1	1	1

The first two elements in this basis have exponent 0, which means that they are integral over both $k[x]$ and $k[1/x]$. As $k[x] \cap k[1/x] = k$, they must be constants on each component of the curve.

The the prime ideals over $x = 0$ are found to be

$$(x, 1-1, \frac{xy_2^2 - y_1^2y_2^2}{x} + 1, y_2 - 0, \dots, y_1^2 + 1, \dots),$$
$$(x, 1-1, \frac{xy_2^2 - y_1^2y_2^2}{x} + 1, y_2 - 0, \dots, y_1^2 - \sqrt{-1}, \dots),$$
$$(x, 1-1, \frac{xy_2^2 - y_1^2y_2^2}{x} - 1, y_2 - 0, \dots, y_1^2 + \sqrt{-1}, \dots),$$
$$(x, 1-1, \frac{xy_2^2 - y_1^2y_2^2}{x} - 1, y_2 - 0, \dots, y_1^2 - 1, \dots).$$

It can now be seen that the constants 1 and $\frac{xy_2^2-y_1^2y_2^2}{x}$ in the integral basis take the values 1 and -1 on one component and the values 1 and 1 on the other component. It follows that

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ \frac{xy_2^2-y_1^2y_2^2}{x} \end{pmatrix} = \begin{pmatrix} \frac{-y_1^2y_2^2+xy_2^2+x}{2x} \\ \frac{y_1^2y_2^2-xy_2^2+x}{2x} \end{pmatrix}$$

is a basis of the constants with the further property that each function in this basis is 1 on a certain component and 0 on all others. We call such a basis of the constants a *basis of indicator functions*. This method of calculating the components of a function algebra is summarized in the following lemma.

Lemma 7.4. *Any function algebra A is isomorphic to the direct product of function fields, which we will also call the components of the function algebra. Lemma 7.5 gives a list of functions $\eta_1, \dots, \eta_n$ along with exponents $\delta_1, \dots, \delta_n$. Let $\eta_1, \dots, \eta_m$ be the subset of these functions with $\delta_i = 0$. The number of components of A is exactly m, which can be identified in each representation as follows.*

- (M) *Calculate the places over $x = 0$, and use these places to calculate a basis $\hat{\eta}_1, \dots, \hat{\eta}_m$ of indicator functions. A component associated to the indicator function $\hat{\eta}_1$ is then given by $A/(\hat{\eta}_2, \dots, \hat{\eta}_m)$.*
- (P) *Let $T(x, y) \in k(x)[y]$ be a defining polynomial for A. Select an $x_0 \in k$ for which $T(x_0, y) = 0$ has n distinct solutions $y_1, \dots, y_n$ in some extension $\overline{k}$ of k. Use these places over $x = x_0$ to calculate a basis of indicator functions $\hat{\eta}_1, \dots, \hat{\eta}_m \in \overline{k}(x)[y]$. Then, $\mathrm{Gcd}_y(T, \hat{\eta}_2, \dots, \hat{\eta}_m)$ is an absolutely irreducible factor of $T(y)$ and defines a function field component of A corresponding to the indicator function $\hat{\eta}_1$.*

It is to be noted that the extension of k used in the polynomial representation certainly contains the exact constant field of the function algebra but might also be bigger. The matrix representation also uses an extension of k that might be bigger than necessary as it computes the values of all of the integral basis elements at the places over $x = 0$ while only the values of the constants are used.

7.2. **Integration on function algebras.** In general, an element f of a function algebra A may be integrated as long f may be reduced to each of the components of A and each reduction to a component may be integrated. This means that we exclude from consideration integrals such as $\int dx/(x + \sqrt{x^2})$ since the integrand may not be reduced to the component where $\sqrt{x^2} = -x$. The general procedure of integrating an element of a function algebra will be apparent from the treatment of the following simple example. Consider integrating $\int y dx$ where y is defined by

$$(y^2 - x)(y^3 - x) = 0. \tag{7.1}$$

In some sense this amounts to integrating $\sqrt{x}$ and $x^{1/3}$ *at the same time*. Notice that the equation

$$\int y dx = \frac{9x^2y + x^2 - xy^3 - 8xy - y^4}{12(x-1)} \tag{7.2}$$

gives the expected correct results when either $y = \sqrt{x}$ or $y = x^{1/3}$ is substituted. It is also true that when both sides of (7.2) are differentiated using the formal relation (7.1), the identity $y = y$ results. For this reason we shall consider (7.2) to be the correct way of integrating ydx on the function algebra defined by (7.1).

The algorithm of Lemma 7.5 returns the following normal integral basis and exponents for this function algebra.

basis element	1	y	y^2	$\dfrac{xy + x - y^4 - y^3}{x(x-1)}$	$\dfrac{xy^3 - xy - x + y^4}{x(x-1)}$
exponent	0	1	1	0	1

Since there are two constants we know the function algebra has two components, which is also obvious from the factorization of the defining equation (7.1). We can take $\mathbb{Q}$-linear combinations of the constants to get the indicator functions for each component. These are constant functions that are 1 on the desired component and 0 on all other components.

component	indicator function
$y^2 - x = 0$	$\dfrac{-xy - x + y^4 + y^3}{x(x-1)}$
$y^3 - x = 0$	$\dfrac{x^2 + xy - y^4 - y^3}{x(x-1)}$

To integrate $y\,dx$ on the function algebra defined by (7.1), we first integrate it on each component as

$$\int y\,dx = \frac{2xy}{3} \qquad \text{on } y^2 - x = 0,$$
$$\int y\,dx = \frac{3xy}{4} \qquad \text{on } y^3 - x = 0.$$

A valid integral on the entire function algebra defined by $(y^2 - x)(y^3 - x) = 0$ is obtained by combining these component-wise results using the indicator functions as

$$\begin{aligned}\int ydx &= \frac{-xy - x + y^4 + y^3}{x(x-1)} \cdot \frac{2xy}{3} + \frac{x^2 + xy - y^4 - y^3}{x(x-1)} \cdot \frac{3xy}{4} \\ &= \frac{9x^2y + x^2 - xy^3 - 8xy - y^4}{12(x-1)} \mod (y^2 - x)(y^3 - x).\end{aligned}$$

7.3. **Normal integral bases for function algebras.** The whole of the integration algorithm has now been reduced to the calculation of the type of basis for a function algebra as described in Lemma 7.5. The *reduction algorithm* is the algorithm implied in Corollary 4.4 of [6] and finds $k[x]$-unimodular row operations and $k[[1/x]]$-unimodular column operations to reduce a given matrix in $k(x)^{n\times n}$ to a diagonal matrix with powers of x on the diagonal. This reduction algorithm is similar to the Smith normal form for matrices over $\mathbb{Z}$ and is also used in Lemma 4.1 to compute a normal basis for an arbitrary divisor.

Lemma 7.5. *Let A be a function algebra over $k(x)$. A normal integral basis for A, that is, a basis $\eta_1, \ldots, \eta_n$ along with nonegative integers $\delta_1, \ldots, \delta_n$ that satisfies*

- *The $k[x]$-span of the η_i is the integral closure of $k[x]$ in A.*
- *The $k[1/x]$-span of the $x^{-\delta_i}\eta_i$ is the integral closure of $k[1/x]$ in A.*

may be calculated as follows.

1. *Calculate a basis $e_1, \ldots, e_n$ of the integral closure of $k[x]$ in A using Lemma 7.6.*
2. *Calculate a basis $f_1, \ldots, f_n$ of the integral closure of $k[[1/x]]$ in A using Lemma 7.6. The whole algorithm works with $k[[1/x]]$ in place of $k[x]$. Furthermore, the discriminant in Step 2 of Lemma 7.6 is simply a nonnegative power of $(1/x)$.*
3. *Let the change of basis matrix be M with $e_i = \sum_j M_{i,j} f_j$. Run the reduction algorithm by changing the basis $\{e_i\}$ (which corresponds to $k[x]$-unimodular row operations on M) and changing the basis $\{f_i\}$ (which corresponds to $k[[1/x]]$-unimodular column operations on M). The δ_i are the powers of x on the diagonal of M after it has been reduced.*

We now present Trager's algorithm, which is an adaptation of the Round 2 algorithm of Zassanhaus and Ford [15]. Although originally stated only for function fields, Trager's algorithm applies equally well to the more general setting of function algebras, and we will briefly explain the method, which appears in Chapter 2 of [7]. The algorithm for computing an integral basis of a function algebra A starts with an arbitrary $k[x]$-order R of A and progressively enlarges R until the maximum order (the integral closure) is obtained. The first tool used accomplish this is the discriminant of a $k[x]$-order R, defined by

$$\mathrm{Disc}_{k[x]}(R) = \det\left(\mathrm{Trace}(e_i e_j)\right)_{i,j}, \text{ for a } k[x]\text{-basis } \{e_i\} \text{ of } R.$$

This is an element of $k[x]$ and is defined up to multiplication by units of $k[x]$. The second tool is the order of a ideal Λ of R, also called the idealizer in [7],

$$\mathrm{Idealizer}(\Lambda) = \{f \in A \mid f\Lambda \subset \Lambda\}.$$

The important property of the idealizer is that it is the largest ring in which Λ is still and ideal, and as long as Λ contains a non-zero divisor, $\mathrm{Idealizer}(\Lambda)$ is a $k[x]$-order of A. The final tool is the q-radical of R, defined for $q \in k[x]$ by

$$\mathrm{Radical}_q(R) = \{u \in R \mid \mathrm{Trace}(uv) \equiv 0 \mod q \text{ for all } v \in R\}.$$

As shown by Trager, this is the product of all prime ideals of R that lie above q. The facts that make the algorithm work are collected here.

1. If R is not integrally closed, then there is some prime ideal P lying over the discriminant $d = \mathrm{Disc}_{k[x]}(R)$ that is not invertible. This prime ideal is caught in $\Lambda = \mathrm{Radical}_q(R)$ where q is the product of the distinct prime factors of d. Since the idealizer of P is strictly bigger than R, the idealizer of Λ is also strictly bigger than R.
2. If R is integrally closed, then, by definition of the idealizer, it holds that $R = \mathrm{Idealizer}(\mathrm{Radical}_q(R))$ for any q.

Lemma 7.6. *Let A be a function algebra over $k(x)$. The following procedure calculates a basis for the integral closure R of $k[x]$ in A.*

Step 1 *Start with arbitrary basis of A and, if necessary, multiply each element in the basis by suitable elements of $k(x)$ so that the basis consists of elements that are integral over $k[x]$. Let R denote the $k[x]$-module with this bases.*

Step 2 *Set* $a = d = \mathrm{Disc}_{k[x]}(R)$.

Step 3 *Let* q *be the product of the primes* p *in* $k[x]$ *such that* $p|a$ *and* $p^2|d$. *Only a squarefree factorization of* a *and* d *is required to compute* q.

Step 4 *Set* $R' = \mathrm{Idealizer}(\mathrm{Radical}_q(R))$ *and let* $a \in k[x]$ *be the determinant of the change of basis matrix from* R *to* R'.

Step 5 *If* a *is a unit, then return* R. *Otherwise set* $R = R'$, *set* $d = d/a^2$, *and goto Step 3.*

Example 7.7. *Let us compute the integral closure of* $\mathbb{Q}[x]$ *in* $\mathbb{Q}(x, y)$ *where* y *is defined by* $y^4 = x^3(x+1)^2$. *The idealizer and* q*-radicals are computed directly from the definition. In general, these should be computed using the algorithms presented in Chapter 2 of* [7]. *We first start with the basis* $1, y, y^2, y^3$ *of the order* R. *The discriminant is given by*

$$d = \det \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4x^3(x+1)^2 \\ 0 & 0 & 4x^3(x+1)^2 & 0 \\ 0 & 4x^3(x+1)^2 & 0 & 0 \end{pmatrix} = x^9(x+1)^6.$$

We need to look at the radical of $x(x+1)$, *which is*

$$\begin{aligned} \Lambda = \mathrm{Radical}_q(R) &= \{u = a + by + cy^2 + dy^3 \mid \begin{array}{l} \mathrm{Trace}(u \cdot 1) \equiv 0 \mod x(x+1) \\ \mathrm{Trace}(u \cdot y) \equiv 0 \mod x(x+1) \\ \mathrm{Trace}(u \cdot y^2) \equiv 0 \mod x(x+1) \\ \mathrm{Trace}(u \cdot y^3) \equiv 0 \mod x(x+1) \end{array} \} \\ &= \{a + by + cy^2 + dy^3 \mid \begin{array}{l} a \equiv 0 \mod x(x+1) \\ x(x+1)d \equiv 0 \mod x(x+1) \\ x(x+1)c \equiv 0 \mod x(x+1) \\ x(x+1)b \equiv 0 \mod x(x+1) \end{array} \} \\ &= \mathbb{Q}[x] \text{ span of } \{x(x+1), y, y^2, y^3\}. \end{aligned}$$

We next need to compute the idealizer of Λ, *which is*

$$\begin{aligned} \mathrm{Idealizer}(\Lambda) &= \{f = a + by + cy^2 + dy^3 \mid f \cdot x(x+1), f \cdot y, f \cdot y^2, f \cdot y^3 \in \Lambda\} \\ &= \{f = a + by + cy^2 + dy^3 \mid a, b, c, x(x+1)d \in \mathbb{Q}[x]\} \\ &= \mathbb{Q}[x] \text{ span of } \{1, y, y^2, \frac{y^3}{x(x+1)}\}. \end{aligned}$$

Thus the basis of R *has been enlarged to* $\{1, y, y^2, \frac{y^3}{x(x+1)}\}$ *after one iteration of the algorithm. After the second iteration, the basis is* $\{1, y, \frac{y^2}{x(x+1)}, \frac{y^3}{x^2(x+1)}\}$ *and the third iteration does improve on this, hence this is an integral basis.*

8. Conclusion and Some practical considerations

Recall that logarithmic terms of the form

$$\sum_{j=1}^{m} \frac{b_j}{c_j} \log f_j \tag{8.1}$$

may be required to express the integral and that the constants b_j and functions f_j are in general defined over a finite Galois extension, say k_2, of k. As there is great flexibility in choosing the representation of k_2, there is a great deal of arbitrariness in the form the answer may take. For this reason, it is desirable to average (8.1) over all elements of the Galois group $G = \mathrm{Gal}(k_2/k)$ to produce an equation of the form

$$\frac{1}{|G|}\sum_{\sigma\in G}\sum_{j=1}^{m}\frac{b_j}{c_j}\log f_j = \sum_i \sum_{\theta:g_i(\theta)=0}\theta\log F_j(\theta). \tag{8.2}$$

For some set of irreducible $g_i(\theta) \in k[\theta]$ and $F_j(\theta)$ in $K(\theta)$. The g_i are nothing but the minimal polynomials of the residues (or some rational multiple of the residues). Since the residues are determined by the given function to integrate, this eliminates much of the arbitrariness with which the answer could have been presented. There still however remains a great deal of freedom in choosing the $\mathbb{Q}$-basis $\{b_j\}$ of the residues.

The algorithm for integration of a differential $f\,dx$ may be sumarized as follows.

(1) Represent f as an element of the function algebra K over $k[x]$.
(2) For each function field component K_0,
   (a) Compute K_0, the exact constant field k_0 of K_0, and the indicator function of K_0 inside K.
   (b) Represent f as an element of K_0 and remove the multiple poles of f using Hermite Reduction and the integrals of the second kind for K_0.
   (c) Let $z_1, \ldots, z_n$ be the roots of the polynomials in (4.10) and (4.11). Compute the splitting field $k_2 = k_0(z_1, \ldots, z_n)$ and the Galois group $G = \mathrm{Gal}(k_2/k_0)$. Extend the function field $K_0/k_0[x]$ to $K_2/k_2[x]$ by this extension of the constant field.
   (d) Compute $\mathbb{Q}$-linearly independent elements $b_1, \ldots, b_m \in k_2$ and a matrix $M \in \mathbb{Z}^{n\times m}$ such that $z_i = \sum_j M_{i,j}b_j$.
   (e) For $1 \le j \le m$, compute functions f_j and integers c_j such that

$$\mathrm{div}(f_j) = \left(\prod_{i=1}^{n}\delta(z_i)^{M_{i,j}}\right)^{c_j}, \ (\delta(z_i) \text{ defined in (4.12)}).$$

   (f) Up to addition of integrals of the first kind, the integral may now be expressed as (8.1). Average over all elements of G to write it in the form of the right hand side of (8.2). The integral is now expressed as a sum of terms where each term is the sum over all embeddings of some intermediate number field k_1/k_0.
(3) Obtain the final result by combining the indicator functions of (2a) with the sum of the results in (2a) and (2f).

The only step that may fail is (2e) as the divisor $\prod_{i=1}^{n}\delta(z_i)^{M_{i,j}}$ may not be torsion. The averaging in step (2f) may also be done in step (2e), which will most likely result in testing for torsion a divisor defined over a much smaller field (k_1 instead of k_2).

There is one other significant simplification worth mentioning that occurs when the function field has genus zero. In this case, step (2e) always succeeds with $c_j = 1$. In fact, we can avoid computing in the splitting field k_2 altogether. Recall that the divisor $\delta(z_i)$ consists of the places where the integrand has residue z_i. Let $d_i = \deg(\delta(z_i))$. If we can find another divisor D of degree -1 and

defined over k_0, then it holds that

$$\int f = \sum_i z_i \log f_i, \quad \text{where} \quad \operatorname{div}(f_i) = \delta(z_i) D^{d_i}.$$

Methods for finding a divisor of degree -1 for genus zero function fields are discussed, for example, in [10]. As the degree of the canonical divisor $\operatorname{div}(dx)$ is -2, it is always possible to to find a divisor D of degree -2 defined over k_0. In this case, the equation could be

$$\int f = \sum_i \frac{(2, d_i)}{2} z_i \log f_i, \quad \text{where} \quad \operatorname{div}(f_i) = \delta(z_i)^{\frac{2}{(2,d_i)}} D^{\frac{2d_i}{(2,d_i)}}.$$

9. Selected Algorithms

9.1. **Prime Factorization of Ideals.** Given an irreducible $p(x) \in k[x]$ the goal is to compute prime ideals $P_1, \ldots, P_d \in O(K)_\infty$ such that

$$(p(x)) = P_1^{e_1} \cdots P_d^{e_d}$$

with $\operatorname{Norm}(P_i) = p(x)^{f_i}$.

Lemma 9.1. *Let $p(x)$ be a monic irreducible element of $k[x]$. Suppose that I is an integral ideal with $(p(x)) \subseteq I$, and let M be the matrix for the Hermite Normal Form of I.*

- *The diagonal entries of M are either 1 or $p(x)$.*
- *Above each 1 on the diagonal of M are only zeros.*
- *To the right of each $p(x)$ on the diagonal are only zeros.*

Proof. The second assertion is immedate. Suppose for concreteness $p(x) = x$ and we have in Hermite Normal Form,

$$\operatorname{HNF}(p(x)) = N = \begin{pmatrix} x & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x \end{pmatrix}, \qquad \operatorname{HNF} I = M = \begin{pmatrix} x & 1 & 0 \\ 0 & x & 0 \\ 0 & 0 & x \end{pmatrix}$$

The diagonal entries of M can only be 1 or $p(x)$ because NM^{-1} must have entries in $k[x]$ since $(p(x)) \subseteq I$. Now further suppose that a row of M containing a digonal $p(x)$ has another non-zero entry as in the chosen M above. Since

$$(p(x)) + I \sim \begin{pmatrix} x & 1 & 0 \\ 0 & x & 0 \\ 0 & 0 & x \\ x & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x \end{pmatrix} \sim \begin{pmatrix} x & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & x \end{pmatrix},$$

we have $(p(x)) + I \neq I$. This is a contradiction because $(p(x)) \subseteq I$.

□

Lemma 9.2. *To find all prime ideals of $O(K)_\infty$ over an irreducible monic $p(x) \in k[x]$:*

(M)
- *Extend k to $k_0 = k(\phi)$ where $p(\phi) = 0$.*
- *Iterate the following procedure for $i = 1$ to $i = n$.*
  - *Factor $\operatorname{Norm}(\eta_i - \lambda)$ in $k_{i-1}[\lambda]$ and non-deterministically choose a factor.*

    * *Let a_i be a root of the chosen factor and extend k_{i-1} to $k_i = k_{i-1}(a_i)$.*
    * *If $(x - \phi, \eta_1 - a_1, \ldots, \eta_i - a_i)$ is not a proper ideal, return "FAIL".*
  - *Let M be the matrix in reduced row echelon form whose rows $\vec{b}_i$ form a k_0-basis of the solutions to $\vec{b} \cdot \vec{a} = 0$, where $\vec{a} = (a_1, \ldots, a_n)$.*
  - *Write each entry of M, which is an element of k_0, uniquely as a polynomial over k in ϕ (modulo $p(\phi)$), and replace ϕ by x.*
  - *Insert rows into M that, besides having $p(x)$ in one position, consist entirely of zeros. Insert such rows so that M satisfies the conditions of Lemma 9.1, and return "SUCCESS - prime ideal M found".*

(P) *Let $y \in O(K)$ with $K = k(x, y)/f(x, y)$ where f is the minimal polynomial for y. The rest of the procedure applies if $p(x)$ does not divide [[???]]. Factor $f(x, y) \in k[x, y]$ modulo $p(x)$ and choose and irreducible factor $f_0(x, y)$. The ideal $(p(x)) + (f_0(x, y))$ is a prime factor above $p(x)$.*

If Q is any prime ideal over $p(x)$, there is some path through the (M) procedure that will output Q in Hermite Normal Form. Assuming that a y has been chosen and $p(x)$ does not divide [[???]], there is a path though the (P) program that outputs Q in two-element form.

Although the matrix procedure looks daunting compared with the polynomial proceedure, the two are equivalent in difficulty. Factoring modulo $p(x)$ in the polynomial representation is replaced by extending k to k_0 in the matrix representation. Furthermore, factoring $f(x, y)$ of degree n in y in (P) is replaced by finding a field k_n in (M). Of course, $[k_n : k_0] \leq n$ so that the matrix representation is no more difficult than the polynomial represention. The former has the benefit of working without restriction on $p(x)$.

Example 9.3. *Relative to the integral basis $1, y, y^2$ for the function field defined by $y^3 = 3+3x+3x^2$ over $\mathbb{Q}$, the prime factorization of $x^3 - 2$ is given by*

$$(x^3 - 2) = \begin{pmatrix} 3 & 0 & 1 - x \\ 0 & 3 & -1 + x - x^2 \\ 0 & 0 & x^3 - 2 \end{pmatrix} \cdot \begin{pmatrix} 3 & 1 - x + x^2 & -1 + x^2 \\ 0 & x^3 - 2 & 0 \\ 0 & 0 & x^3 - 2 \end{pmatrix}.$$

9.2. **Puiseux Series.** We are going to be looking at the field of fractional power series in the variable X, which consists of formal series of the form

$$s = \sum_{i=l}^{\infty} c_i X^{i/e}, \quad c_l \neq 0,$$

for some natural number e and integer l. Set $\|s\| = l/e$.

Lemma 9.4. *Let $a \in k$ and suppose $P = (x - a, \eta_1 - a_1, \ldots, \eta_n - a_n)$, where the a_i are in some extension of k, is a place of ramification index e over $(x - a)$. If $y \neq 0$ is a function in K, then the expansion of y at P is of the form*

$$y = \sum_{j \geq l}^{\infty} c_j (c(x - a))^{j/e}$$

where all of the coefficients c, c_j lie in $k_P = k(a_1, \ldots, a_n)$. Different choice of the e^{th} root give rise to (at most) e distinct series for y at P.

Proof. We first begin by finding a uniformizer at P. This is some function t that has a simple zero at P, and such a function can be selected from $P \setminus P^2$. Since $x-a$ vanishes to order e at P, we have, for some nonzero c and d_j in k_P, an equation of the form

$$\frac{t^e}{x-a} = c + d_1 t + d_2 t^2 + \cdots$$

or

$$t = \sqrt[e]{c(x-a)} + \frac{d_1}{ce}(\sqrt[e]{c(x-a)})^2 + \cdots.$$

This allows us to convert laurent series in the variable t into fraction power series in the variable $c(x-a)$. □

Expansions in fractional powers of the variable $X = c(x-a)$ are a way to standardize the series of expansions of algebraic functions since the choice of the uniformizer t in Lemma 9.4 is quite arbitrary. Also, since computing such an expansion in Lemma 9.4 is a slow operation, it is necessary to give a faster method.

Lemma 9.5. *Let P be a place over $x=a$. Assume that the first few terms of the series expansions of a given function calculated as fractional powers series in the variable $X = c(x-a)$ by the techniques of Lemma 9.4. The full series can then be computed quickly in each representation as follows.*

(M) *To calculate the series expansion of the elements of the integral basis at a place P, find the elements $a_{ijk} \in k[x]$ such that $\eta_i \eta_j = \sum_{k=1}^{n} a_{ijk}\eta_k$. Of the $n(n+1)/2$ functions*

$$\begin{array}{l} y_1 y_1 - a_{111}y_1 - \cdots - a_{11n}y_n \\ y_1 y_2 - a_{121}y_1 - \cdots - a_{12n}y_n \\ \quad \vdots \\ y_i y_j - a_{ij1}y_1 - \cdots - a_{ijn}y_n \quad i \le j \\ \quad \vdots \\ y_n y_n - a_{nn1}y_1 - \cdots - a_{nnn}y_n \end{array},$$

choose n functions and put them into a vector-valued function $\vec{F}(\vec{y})$. These n functions need to be chosen so that the Jacobian matrix $\frac{\partial \vec{F}}{\partial \vec{y}}(\vec{\eta})$ is non-singular. If $\vec{y}_1$ is a vector of series expansions of the elements of $\vec{\eta}$ at P calculated sufficiently precise so that $\|\vec{y}_1 - \vec{\eta}\| > \|\det \frac{\partial \vec{F}}{\partial \vec{y}}(\vec{y}_1)\|$, then Newton's method

$$\vec{y}_{i+1} = \vec{y}_i - (\tfrac{\partial \vec{F}}{\partial \vec{y}}(\vec{y}_i))^{-1}\vec{F}(\vec{y}_i)$$

will produce a sequence of approximations to $\vec{\eta}$ with

$$\|\vec{y}_i - \vec{\eta}\| \ge \|\det \tfrac{\partial \vec{F}}{\partial \vec{y}}(\vec{y}_1)\| + 2^{i-1}(\|\vec{y}_1 - \vec{\eta}\| - \|\det \tfrac{\partial \vec{F}}{\partial \vec{y}}(\vec{y}_1)\|).$$

(P) *Let $y \in O(K)_\infty$ and $f(y) \in k[x][y]$ be its minimal polynomial. If Newton's method is initialized with an approximate solution y_1 satisifying $\|y_1 - y\| > \|f'(y_1)\|$, then the iteration*

$$y_{i+1} = y_i - \frac{f(y_i)}{f'(y_i)}$$

converges quadratically to y with errors satisfying

$$\|y_i - y\| \geq \|f'(y_1)\| + 2^{i-1}(\|y_1 - y\| - \|f'(y_1)\|).$$

References

[1] H. T. Kung, J. F. Traub, All algebraic functions can be computed fast, July 1976

[2] `http://axiom-wiki.newsynthesis.org/FrontPage`.

[3] G. A. Bliss, Algebraic Functions and Their Divisors.

[4] D. Duval, Absolute Factorization of Polynomials: A Geometric Approach, SIAM J. Comput., 20(1), 1–21.

[5] E. Hermite. Sur l'intgration des fractions rationelles. Nouvelles Annales de Mathematiques (2eme srie), 11:145–148, 1872.

[6] F. Hess, Computing Riemann-Roch spaces in algebraic function fields and related topics, J. Symbolic Computation (2001) 11, 1–000.

[7] B. M. Trager, Integration of algebraic functions, Ph.D. Thesis, MIT.

[8] A. Poteaux and M. Rybowicz, Good reduction of Puiseux series and applications, Journal of Symbolic Computation 47(1):32–63, January 2012.

[9] Franck Leprv́ost, Michael Pohst, and Andreas M. Schöpp. Rational torsion of $J_0(N)$ for hyperelliptic modular curves and families of Jacobians of genus 2 and genus 3 curves with a rational point of order 5, 7 or 10. Abh. Math. Sem. Univ. Hamburg, 74:193–203, 2004.

[10] M. V. Hoeij, Computing Parametrizations of Rational Algebraic Curves, In ISSAC-94, 1994, 187–190, ACM Press

[11] M. V. Hoeij, An algorithm for computing the Weierstrass normal form, In ISSAC-95, 1995, 90–95, ACM Press ISSAC '95 Proceedings of the 1995 international symposium on Symbolic and algebraic computation Pages 90-95

[12] N. D. Elkies. `http://www.math.harvard.edu/~elkies/g2_tors.html`.

[13] E. V. Flynn. Large rational torsion on abelian varieties. J. Number Theory, 36(3):257–265, 1990.

[14] H. Cohen, Advanced Topics in Computational Number Theory, Graduate Texts in Mathematics 193, Springer, New York, 2000.

[15] D. J. Ford, On the Computation of the Maximal Order in a Dedekind Domain, Ph.D. thesis, Ohio State University, Depart. of Mathematics, (1978).

[16] B. Deconinck, M. S. Patterson, Computing the Abel map, Physica D: Nonlinear Phenomena, 237(24), December 2008, 3214–3232.

[17] A. Weil, Courbes algebriques et varietes abeliennes, Hermann, Paris, (1971), first published (1948) in Actualites Scienti ques et Industrielles, nos. 1041 and 1064.

[18] M. Rosenlicht, Differentials of the Second Kind for Algebraic Function Fields of One Variable, Annals of Mathematics, Second Series, Vol. 57, No. 3 (May, 1953), 517–523.