Impossible integration

Mathcamp 2024

Glenn Sun

These notes may contain errors,
and should not considered an authoritative source.

Contents

1 Introduction **2**
- 1.1 Prologue . . . 2
- 1.2 Partial fraction decomposition . . . 4
- 1.3 Epilogue . . . 6

2 Differential algebra **9**
- 2.1 Why does calculus feel like algebra? . . . 9
- 2.2 Field extension zoo . . . 11

3 La pièce de résistance **13**
- 3.1 The algebraic case . . . 13
- 3.2 The logarithmic and exponential cases . . . 15

1 Introduction

1.1 Prologue

The *Gaussian function* $f(x) = e^{-x^2}$ is an extremely important function in mathematics, and especially in applied settings. One familiar application might be Gaussian blur for images. With some scaling, it is also known as the normal distribution in statistics.

We would like to do calculus with the Gaussian function. A classic example in multivariable calculus uses polar coordinates to show that

$$\int_{-\infty}^{\infty} e^{-x^2}\,dx = \sqrt{\pi}.$$

It's not trivial, but it's not terribly difficult either. However, no matter how hard you try, it turns out you won't be able to find an expression for the antiderivative of the Gaussian function!

I should clarify a bit. By the fundamental theorem of calculus, the Gaussian function certainly has an antiderivative. Actually, up to a bit of scaling, it is often written $\operatorname{erf}(x)$, for "error function", because it is useful to calculate the probability that a measurement makes an error. Nonetheless, $\operatorname{erf}(x)$ cannot be expressed in our familiar language of polynomials, nth roots, exponentials, logarithms, trigonometry, etc. We call this the language of *elementary functions.*

How does one even begin to try proving something like this? Let's take a look at a few examples of derivatives and integrals to see if we can spot any patterns in their expressions. (To the dismay of calculus teachers around the world, I will omit the $+\,C$ for all antiderivatives in these notes.)

f	$\frac{d}{dx}f$	$\int f\,dx$
$3x^2+5$	$6x$	x^3+5x
$\frac{1}{x+2}$	$-\frac{1}{(x+2)^2}$	$\log(x+2)$
$\log(3x-2)$	$\frac{3}{3x-2}$	$\left(x-\frac{2}{3}\right)\log(3x-2)-x$
$\frac{1}{\sqrt{x^2+1}}$	$-\frac{x}{(x^2+1)^{3/2}}$	$\sinh^{-1}(x)$
e^{-x^2}	$-2e^{-x^2}x$	?

Here's one observation: the derivative of f seems to be made up of all the same "parts" as f, whereas the integral can introduce new things like log or $\sinh^{-1}$. In fact, derivatives can even lose parts like log, but there are never any surprise new parts. Meanwhile, when you integrate, you can get surprise new things like logs and $\sinh^{-1}$. At first glance, this doesn't seem terribly helpful — I think every calculus student knows that derivatives make things less complicated and integrals make things more complicated.

But wait. Isn't sinh made up of exponentials? So, in some way, is $\sinh^{-1}$ also a logarithm? Let's give it a try. We have

$$\sinh(x) = \frac{e^x - e^{-x}}{2}.$$

Solving for x directly is difficult because there is both e^x and e^{-x}. We could try to get rid of e^{-x} by remembering that

$$\cosh(x) = \frac{e^x + e^{-x}}{2} \qquad \text{and} \qquad \cosh^2(x) - \sinh^2(x) = 1.$$

In other words,

$$\sinh(x) + \sqrt{\sinh^2(x) + 1} = e^x.$$

Thus,

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

And in particular, $\sqrt{x^2+1}$ appeared in the original f! This is a logarithm of components that we started with, like the others.

So, maybe integrals aren't so bad after all. Maybe, they can only introduce logarithms. And, it doesn't seem like they introduce any fancy expressions with these new logarithms, like $x\log(x)$ or $\log(x)^2$ or anything like that — just basic logs of components that were in the original expression. (After all, if an antiderivative contains $x\log(x)$, taking the derivative gives $x \cdot \frac{1}{x} + \log(x)$, in which case $\log(x)$ wouldn't be a new component in the antiderivative.)

This is what Joseph Liouville proved in 1833, and it will be the main thing we study in this course.

Theorem 1.1 (Liouville's theorem, informally). *If a function f has an elementary antiderivative, then it looks like*

$$\int f\,dx = g + c_1 \log(h_1) + \cdots + c_n \log(h_n),$$

where $g, h_1, \ldots, h_n$ are all functions made of the same "parts" as f. If we choose to differentiate the above, we may equivalently write

$$f = g' + c_1 \frac{h_1'}{h_1} + \cdots + c_n \frac{h_n'}{h_n}.$$ ⌟

Liouville's theorem tells us the form that every elementary antiderivative must have, so to show that e^{-x^2} has no elementary antiderivative, it just remains to show that nothing of this form works.

Exercises

1. When you differentiate or integrate $\sin(x)$, you get something with $\cos(x)$. How can we think of these two things as actually made of the same "parts"? (Note: writing $\cos(x) = \sin(x + \frac{\pi}{2})$ does not resolve this, because we only put "parts" together with $+$, $-$, $\cdot$, and $/$, not function composition. I will make this more explicit in a couple days, for now, ask me if it's confusing.)
2. Show that the following functions are also secretly just logs:
   (a) $\tanh^{-1}(x)$
   (b) $\sin^{-1}(x)$

1.2 Partial fraction decomposition

Because it will be useful at various points and doesn't really fit in anywhere else, I wanted to spend a minute talking about partial fraction decomposition first. This is a very useful technique that writes a rational function (a fraction of polynomials) as a sum of rational functions with smaller denominators. It is often covered in calculus classes as an integration technique, too.

To demonstrate how it works, take

$$\frac{3x^2-4x-2}{x^3-4x^2+5x-2} = \frac{3x^2-4x-2}{(x-1)^2(x-2)}.$$

For no apparent reason yet, I will assert that there exist constants A, B, and C such that

$$\frac{3x^2-4x-2}{(x-1)^2(x-2)} = \frac{A}{x-1} + \frac{B}{(x-1)^2} + \frac{C}{x-2}.$$

We multiply through to get

$$\begin{aligned} 3x^2-4x-2 &= A(x-1)(x-2) + B(x-2) + C(x-1)^2 \\ &= A(x^2-3x+2) + B(x-2) + C(x^2-2x+1) \\ &= (A+C)x^2 + (-3A+B-2C)x + (2A-2B+C). \end{aligned}$$

This leaves us with the system of equations

$$\begin{cases} A \phantom{{}+B} + C = 3 \\ -3A + B - 2C = -4 \\ 2A - 2B + C = -2 \end{cases}.$$

Solving the system yields $A = 1$, $B = 3$, and $C = 2$. We say that

$$\frac{1}{x-1} + \frac{3}{(x-1)^2} + \frac{2}{x-2}$$

is the *partial fraction decomposition* of our original rational function.

In general, we have the following theorem.

Theorem 1.2 (partial fraction decomposition)**.** *Consider a rational function $\frac{f}{g}$, and let $g = q_1^{a_1} \cdots q_n^{a_n}$ be a factorization into distinct irreducibles. Then there exist polynomials p_{ij} with $\deg(p_{ij}) < \deg(q_i)$ and s such that*

$$\begin{aligned} \frac{f}{g} = s + \frac{p_{11}}{q_1} + \cdots + \frac{p_{1a_1}}{q_1^{a_1}} &+ \\ \vdots \\ \frac{p_{n1}}{q_n} + \cdots + \frac{p_{na_n}}{q_n^{a_n}}&. \end{aligned}$$

⌟

To clarify, the p_i are linear factors if we are working over $\mathbb{C}$, and linear or quadratic over $\mathbb{R}$. That means for these two cases, the numerators are either constants or linear functions (when the denominator is quadratic). In general though, we might consider other fields with higher degree irreducibles, for example we may consider rational functions in x and y to be rational functions in y with coefficents being rational functions in x.

Partial proof. I will only prove the case of no repeated roots over $\mathbb{C}$, and specifically for $n = 3$. You can imagine how it works for general n. The cases of repeated roots and other fields is left as an (optional) homework exercise.

In particular, let r be the remainder of division $\frac{f}{g}$, then we can verify that the following equation is true:

$$\begin{aligned}\frac{r(x)}{(x-a)(x-b)(x-c)} = &\frac{r(a)}{(a-b)(a-c)}\frac{1}{x-a} + \\ &\frac{r(b)}{(b-a)(b-c)}\frac{1}{x-b} + \\ &\frac{r(c)}{(c-a)(c-b)}\frac{1}{x-c}.\end{aligned}$$

Clear denominators to get

$$\begin{aligned}r(x) = &\frac{r(a)}{(a-b)(a-c)}(x-b)(x-c) + \\ &\frac{r(b)}{(b-a)(b-c)}(x-a)(x-c) + \\ &\frac{r(c)}{(c-a)(c-b)}(x-a)(x-b).\end{aligned}$$

Recall that there is a unique polynomial of degree n that passes through any given $n+1$ points. Plug in a, b, and c in the above RHS to see that it passes through the points $(a, r(a))$, $(b, r(b))$, and $(c, r(c))$, just like the LHS $r(x)$. By uniqueness, this means the LHS is equal to the RHS. (This construction is sometimes also known as the *Lagrange interpolating polynomial*.) □

Exercises

1. Compute the partial fraction decomposition over $\mathbb{R}$ and over $\mathbb{C}$ of

$$\frac{2x^3}{(x+1)^2(x^2+1)}.$$

2. In the partial proof above, we claimed but didn't prove that there exists a unique polynomial of degree n that passes through any given $n+1$ points. Actually, the Lagrange interpolating polynomial proves the existence. Prove the uniqueness.

3. In this problem, you will complete the proof of the general case of Theorem 1.2 (partial fraction decomposition).

   (a) Prove that if q_1 and q_2 are relatively prime, then for all f with $\deg(f) < \deg(q_1 q_2)$, there exist p_1 and p_2 with $\deg(p_1) < \deg(q_2)$ and $\deg(p_2) < \deg(q_2)$ such that

   $$\frac{f}{q_1 q_2} = \frac{p_1}{q_1} + \frac{p_2}{q_2}.$$

   (b) Show that for all f with $\deg(f) < \deg(q^k)$ and irreducible q, there exist p with $\deg(p) < \deg(q)$ and f^* such that

   $$\frac{f}{q^k} = \frac{r}{q^k} + \frac{p}{q^{k-1}}.$$

   (c) Conclude Theorem 1.2.

1.3 Epilogue

In the interest of making sure I get to the punchline by the end of the course, I've decided to say the punchline at the start of the course. Let's assume Liouville's theorem and prove that e^{-x^2} has no elementary antiderivative! We'll then spend the rest of the course proving Liouville's theorem.

Corollary 1.3. *Let a and b be rational functions with b non-constant. Then, the following are equivalent:*

1. *The function $a(x)e^{b(x)}$ has an elementary antiderivative.*
2. *There exists a rational function $c(x)$ such that*

$$a(x) = c'(x) + c(x)b'(x)$$ ⌟

Proof. ($\Longleftarrow$) We have that

$$\int a(x)e^{b(x)}\,dx = \int (c'(x) + c(x)b'(x))e^{b(x)}\,dx = c(x)e^{b(x)}.$$

($\Longrightarrow$) Liouville's theorem tells us that

$$ae^b = g' + c_1\frac{h_1'}{h_1} + \cdots + c_n\frac{h_n'}{h_n}.$$

Without loss of generality, we may assume that the h_i have leading coefficient 1 and are distinct. Furthermore, we may assume that they are irreducible, because $\log(ab) = \log(a) + \log(b)$ implies that

$$\frac{(h_1h_2)'}{h_1h_2} = \frac{h_1'}{h_1} + \frac{h_2'}{h_2}.$$

Now, I haven't defined exactly what it means to for $g, h_1, \ldots, h_n$ to be "made up of the same parts" as $a(x)e^{b(x)}$, but I will ask you to believe me for now about one of its consequences: you can think about $g, h_1, \ldots, h_n$ as rational functions in the "variable" $e^{b(x)}$ and the other "parts" as coefficients. Consider the partial fraction decomposition of g with respect to the e^b.

Claim 1.4. *The only denominators in the partial fraction decomposition of g are powers of e^b, and the only possible $h_1, \ldots, h_n$ involving e^b is e^b.* ⌟

Proof. Let $\frac{p}{q^k}$ be a term in the partial fraction decomposition of g with respect to the variable e^b. Then, g' contains the following terms:

$$\frac{p'q^k - kq^{k-1}q'p}{q^{2k}} = \frac{p'}{q^k} - k\frac{pq'}{q^{k+1}}.$$

However, recall that

$$g' = ae^b - \left(c_1\frac{h_1'}{h_1} + \cdots + c_n\frac{h_n'}{h_n}\right),$$

where the h_i's are irreducible, and notably, they only appear raised to the first power. Therefore, either $k = 1$, or $p'q^k - kq^{k-1}q'p = 0$.

In the first case, we have

$$\frac{p'}{q} - \frac{pq'}{q^2},$$

and by the same reasoning we must have that pq' contains a factor of q. Since q is irreducible and $\deg(p) < \deg(q)$, this means q must divide q'. We will show later that an irreducible polynomial over e^b with leading coefficient 1 that divides its derivative must be e^b itself. (At least for one direction, note that e^b certainly divides its derivative $b'e^b$.)

In the second case, we have $p'q^k - kq^{k-1}q'p = 0$, which implies $p'q = kpq'$. In particular, again pq' contains a factor of q, so by the same reasoning (dependent on a yet-unproven lemma), $q = e^b$. Then recall that

$$c_1\frac{h_1'}{h_1} + \cdots + c_n\frac{h_n'}{h_n} = ae^b - g',$$

where we now know g' is the sum of terms with denominators e^{kb}. But the h_i are required to be irreducible with leading coefficient 1 (or "constants", i.e. expressions not involving e^b), so the only possibility is $h_i = e^b$. □

We're almost done. Note that the above claim implies that unless h_i already doesn't involve e^b,

$$\frac{h_i'}{h_i} = \frac{b'e^b}{e^b} = b',$$

which also does not involve e^b. So, if we are to regard both sides of

$$ae^b = g' + c_1\frac{h_1'}{h_1} + \cdots + c_n\frac{h_n'}{h_n}$$

as rational functions in e^b, the RHS is g' plus a constant. The claim further tells us that

$$g = s + (\text{some terms with powers of } e^b \text{ in the denominator})$$

Furthermore, we have $(te^{kb})' = t'e^{kb} + tkb'e^{kb}$. Comparing the coefficient of e^b, we see that $a = c' + cb'$, where c is the coefficient of e^b in s. □

Theorem 1.5. *The Gaussian function $f(x) = e^{-x^2}$ has no elementary antiderivative.* ⌟

Proof. We apply the corollary above with $a = 1$ and $b = -x^2$. Thus, assume for contradiction there exists a rational function $c(x)$ such that

$$1 = c' - 2xc.$$

Write $c(x) = \frac{p(x)}{q(x)}$ with $p(x)$ and $q(x)$ relatively prime, so the above equation becomes

$$1 = \frac{p'q - pq'}{q^2} + 2x\frac{p}{q}.$$

Clearing denominators gives

$$q^2 = p'q - pq' + 2xpq,$$

which rearranges into

$$q(q - p' - 2xp) = -pq'.$$

From this, we see that q divides pq', and because p and q are relatively prime, this means q divides q'. Now, in this theorem, q and q' are ordinary polynomials with coefficients in $\mathbb{C}$ (or $\mathbb{R}$ if you like), so this can only happen if q is a constant, in other words, c was originally a polynomial.

Circling back to $1 = c' - 2xc$, consider the degree of the two sides of this equation. The LHS has degree 0, whereas the RHS has degree $\deg(xc) = 1 + \deg(c)$, a contradiction. □

Exercises

1. Using Corollary 1.3, prove that the following functions do not have elementary antiderivatives:
   (a) $\frac{e^x}{x}$
   (b) $\frac{\sin(x)}{x}$
   (c) $\frac{1}{\log(x)}$

2 Differential algebra

2.1 Why does calculus feel like algebra?

Okay! It's time to start the actual class, which is about proving Liouville's theorem. The first thing we need to do is clarify what the actual statement is, giving a formal definition for what it means to be "made of the same parts" as f.

Along the way, we'll also answer a puzzling question that you might have wondered before: at least in my high school, people always said that calculus is easy because it feels like just doing algebra. Precalculus and geometry were the actual "harder" courses, especially for people who don't do so much math. But here at Mathcamp and as you might see in college, calculus is formalized as real analysis, and algebra leads into ring theory, which are not similar at all. So why did they feel similar in high school?

If you think carefully, even though we formally define calculus using epsilons and deltas, the way we compute derivatives is entirely based on algebraic-feeling rules. After you discovered the sum, product, quotient, power, and chain rules, and you learned how to differentiate certain particular functions like $\sin(x)$, $\log(x)$, and e^x, you never touched epsilons and deltas again, relying only the rules.

This realization led people to try doing calculus by taking the rules as axioms, rather than consequences of epsilon-delta proofs.

Definition 2.1. A *differential field* $(F, +, \cdot, ')$ is a field with an additional unary operator $'$ called the derivative, satisfying for all $a, b \in F$:

1. $(a+b)' = a' + b'$, and
2. $(ab)' = a'b + ab'$.

The constants of F, denoted $\mathrm{const}(F)$, is the set of $f \in R$ satisfying $f' = 0$. ⌟

Examples of differential rings include:

- The field of rational functions in $\mathbb{C}$, denoted $\mathbb{C}(x)$, with the standard derivative.
- The field of analytic functions $f(x, y)$ over $\mathbb{R}^2$, with either partial derivative or any directional derivative.
- Any ring with the trivial derivative, defined $f' = 0$ for all $f \in R$.

You can also prove a surprising amount from just the two rules in the definition of differential ring.

Proposition 2.2. *Let F be a differential field. Let $f, g \in F$, $c \in \mathrm{const}(F)$, and $n \in \mathbb{N}$.*

1. $1' = 0$.
2. $(cf)' = cf'$.
3. $(f^n)' = nf'f^{n-1}$.
4. $(\frac{f}{g})' = \frac{f'g - fg'}{g^2}$. ⌟

Proof. For (1), note that $1' = (1 \cdot 1)' = 1' \cdot 1 + 1 \cdot 1' = 1' + 1'$. Subtracting $1'$ from both sides gives $1' = 0$. The remaining are left as homework exercises. □

The above proposition shows that pretty much every rule that you're used to using in traditional differential calculus can also be used here. The one exception is the chain rule. The chain rule talks about function composition, which is not an operation that we have in our field. However, it turns out we will pretty much always be able to avoid it.

Let's try to imagine the smallest field of functions that includes $\mathbb{C}(x)$ and e^x. Because it is a field, we can multiply and divide by e^x, so all of the following must be in this field:

- e^{3x},
- $\frac{(x-1)e^x}{x^2}$, and
- e^{x+1} (because $e^{x+1} = e \cdot e^x$ and $e \in \mathbb{C}$).

The key is that expressions requiring the chain rule to differentiate, such as e^{x^2} and e^{e^x} are *not* in this field. We have the following characterization (the above example uses $F = \mathbb{C}(x)$ and $t = e^x$).

Proposition 2.3. *Let F be a field and let t be a new symbol (i.e. expression). The smallest field containing both F and t is the set of all*

$$\frac{a_0 + a_1 t + \cdots + a_n t^n}{b_0 + b_1 t + \cdots + b_m t^m},$$

where the a_i and b_i are in F, that is, rational functions in t with coefficients in F. ⌟

Definition 2.4. In the context of the previous proposition, we call the new field a *simple extension* of F, and denote it $F(t)$. ⌟

Furthermore, we may make the simple observation once we know how to compute t', the sum, product, power, and quotient rules tell us how to compute the derivative of anything in $F(t)$. In this way, we avoid needing the chain rule. In other words, if we have $\mathbb{C}(x, e^x)$ and want to compute e^{x^2}, we will need to explicitly add e^{x^2} as a new t to our field of functions, resulting in $\mathbb{C}(x, e^x, e^{x^2})$, along with the instruction that $(e^{x^2})' = 2xe^{x^2}$.

A note: although the notation $F(t)$ uniquely defines a field by Proposition 2.3, it does not uniquely define a differential field. That is, when adjoining t to a F, we need to always remember to specify what is t'. From the field's perspective, there is nothing wrong with me writing $(e^x)' = \frac{1}{x}$, after all, e^x is just a symbol to the field, it knows nothing about what e^x means in analysis. For our sanity, we will usually define t' to be what we expect from analysis.

And a remark that I can finally say what I meant by "f is made of the same parts as g"! It means that whenever F is a field containing g, the field also contains f.

Exercises

1. Prove the remaining items in Proposition 2.2.
2. Can you come up with another differential ring with a non-standard derivative?
3. Prove Proposition 2.3.

2.2 Field extension zoo

Here are some useful definitions:

Definition 2.5. Let $F(t)$ be a simple differential field extension.

- If t satisfies a polynomial with coefficients in F, we call t an *algebraic extension.*
- If t satisfies no polynomial relationship, then we call it a *transcendental extension.* Furthermore,
  - If $t' = \frac{s'}{s} \neq 0$ for some $s \in F$, we call it a *logarithmic extension.*
  - If $t' = s't \neq 0$ for some $s \in F$, we call it a *exponential extension.*
- If t is an algebraic, logarithmic, or exponential extension, we say that is an *elementary extension.*

A function f is *elementary* if there exists elementary extensions $t_1, \ldots, t_n$ such that $f \in \mathbb{C}(x, t_1, \ldots, t_n)$ (or $\mathbb{R}$, if you like). ⌟

Keep a few canonical examples of these simple extensions in mind. In the following, let $F = \mathbb{C}(x)$, $g \in \mathbb{C}(x)$, and all simple extensions use the standard derivative on x.

1. $F(\sqrt{x})$ is an algebraic extension. With $t = \sqrt{x}$, it satisfies $t^2 - x = 0$.
2. $F(\log(g))$ is a logarithmic extension. With $t = \log(g)$, it satisfies $t' = \frac{g'}{g}$.
3. $F(e^g)$ is an exponential extension. With $t = e^g$, it satisfies $t' = g't$.
4. $F(y)$ is a transcendental extension that is neither logarithmic nor exponential. Remember, we chose to define $'$ as the (partial) derivative with respect to x, so it satisfies $y' = 0$.

Thus, any function our normal vocabulary of polynomials, nth roots, exponentials, logarithms, and trigonometry (using the fact that $e^{ix} = \cos(x) + i\sin(x)$ to derive expressions for sin and cos using exponentials) is elementary. Actually, elementary functions involve some additional functions that we typically don't consider part of our normal vocabulary. For example, you might have heard that degree 5 polynomials have roots that are not possible to write down with nth roots. But these are still allowed as algebraic extensions.

The following proposition illustrates a stark difference between algebraic and transcendental extensions. Whereas we previously noted that from the field's perspective, e^x is a just a symbol so it is legal to declare $(e^x)' = \frac{1}{x}$, one cannot declare such things at will if the field already has information about t. In particular, the definition of $'$ cannot change for elements of the base field that can be written in terms of t.

Proposition 2.6. *If $F(t)$ is an algebraic extension, there is only one possible definition for t'.* ⌟

Proof. Suppose t satisfies the polynomial $a_0 + a_1 t + \cdots + a_n t^n = 0$, where each $a_i \in F$. We differentiate to get

$$a_0' + (a_1' t + a_1 t') + \cdots + (a_n' t^n + n a_n t' t^{n-1}) = 0.$$

Rearranging, we get

$$t' = -\frac{a_0' + a_1' t + \cdots + a_n' t^n}{a_1 + \cdots + n a_n t^{n-1}}.$$ □

The last thing that we'll do in this section is prove the lemma that we used in the epilogue.

Lemma 2.7. *Suppose $F(t)$ is an exponential extension. Let $f \in F[t]$ be irreducible with leading coefficient 1, and suppose f divides f'. Then $f = t$.* ⌟

Proof. Write $t' = s't$ and $f = a_0 + a_1 t + \cdots + a_{n-1}t^{n-1} + t^n$, where we have $s', a_0, \ldots, a_{n-1} \in F$. Directly computing the derivative, we have

$$\begin{aligned} f' &= a_0' + (a_1't + a_1t') + \cdots + (a_{n-1}'t^{n-1} + (n-1)a_{n-1}t't^{n-2}) + (nt't^{n-1}) \\ &= a_0' + (a_1' + a_1s')t + \cdots + (a_{n-1}' + (n-1)a_{n-1}s')t^{n-1} + (ns't^n), \end{aligned}$$

from which we see that $\deg(f) = \deg(f')$. Therefore, because f divides f', we must have $f' = cf$ for some $c \in F$, not $F(t)$.

It suffices to show that f is a monomial, and the only irreducible monomial with leading coefficient 1 is just t. Suppose for contradiction that f has at least 2 terms, a_it^i and a_jt^j. The above says that when differentiating, both terms are scaled by the same amount. That's weird — the scaling is usually different, depending on the exponent of t, so intuitively this should not be possible.

To prove this formally, we differentiate a_it^i and a_jt^j and equate the scaling factors to get $(a_i' + ia_is')a_j = (a_j' + ja_js')a_i$. Then,

$$\left(\frac{a_it^i}{a_jt^j}\right)' = \frac{(a_i' + ia_is')a_jt^{i+j} - (a_j' + ja_js')a_it^{i+j}}{a_j^2t^{2j}} = 0.$$

Thus, a_it^i is a constant multiple of a_jt^j, which is impossible because t is a transcendental extension. □

Exercises

1. Show that the following function is elementary by constructing a sequence of elementary extensions of $\mathbb{C}(x)$:

$$x^x + \sin(x) + \sqrt{\log(\cos(x))}.$$

2. Show that logarithmic and exponential extensions are transcendental, or at least that $F(e^x)$ and $F(\log(x))$ are transcendental. (Hint: There exists both an analytic proof using growth rates and a purely algebraic proof, pick your favorite.)
3. Give an example of a transcendental extension that is not logarithmic, not exponential, and does not introduce any new constants.

3 La pièce de résistance

3.1 The algebraic case

We are ready to prove Liouville's theorem. It will be a little long!

Theorem 3.1. *Let F be a differential ring (on top of $\mathbb{C}(x)$ or $\mathbb{R}(x)$) and $f \in F$. If there exists elementary extensions $F(t_1) \subseteq \cdots \subseteq F(t_1, \ldots, t_\ell)$ and $y \in F(t_1, \ldots, t_\ell)$ such that $y = \int f$ (or formally $y' = f$), then*

$$f = g' + c_1 \frac{h_1'}{h_1} + \cdots + c_n \frac{h_n'}{h_n}$$

for some $g, h_1, \ldots, h_n \in F$. ⌟

Proof. Backwards induction on the sequence of elementary extensions. The base case is $F(t_1, \ldots, t_\ell)$, where we can take $g = y$ and no h's. This means $f = g' = y'$, and we have written f in the desired form, with all the g's and h's in $F(t_1, \ldots, t_\ell)$.

For the inductive step, we will remove the t's one by one. We are assuming that

$$f = g' + c_1 \frac{h_1'}{h_1} + \cdots + c_n \frac{h_n'}{h_n}$$

for some $g, h_1, \ldots, h_n \in F(t_1, \ldots, t_i)$ and $f \in F$, and we want to rewrite the equation into something of the same form where all the polynomials belong to $F(t_1, \ldots, t_{i-1})$. For conciseness, rename $F = F(t_1, \ldots, t_{i-1})$ and $t = t_i$. In particular, $f \in F$.

In the claims to follow, we will construct such an equation in the cases where t is algebraic, logarithmic, and exponential. □

Before we jump into the algebraic case, let me do a little sidequest to explain something cool about algebraic extensions. For motivation, let's think about $\mathbb{C} = \mathbb{R}(i)$, an algebraic extension of $\mathbb{R}$ by i satisfying $i^2 + 1 = 0$.

The key point is that the definition of this extension didn't allow the field to distinguish i and $-i$: both of these satisfy $i^2 + 1 = 0$. That means we can define a function φ that swaps i and $-i$, and this function will be a *automorphism of* $\mathbb{C}$ *fixing* $\mathbb{R}$. That means $\varphi(a) = a$ for all $a \in \mathbb{R}$, and the structure of $\mathbb{C}$ is the same before and after φ (it is a *homomorphism*), more specifically, for all $a, b \in \mathbb{C}$,

1. $\varphi(a + b) = \varphi(a) + \varphi(b)$,
2. $\varphi(ab) = \varphi(a)\varphi(b)$,
3. $\varphi(1) = 1$, and
4. if this were a differential field, $\varphi(a)' = \varphi(a')$.

In general, when t is an algebraic extension satisfying a minimal polynomial $p(t)$, you can get automorphisms of $F(t)$ fixing F by swapping t and any root of $p(t)$. The roots of $p(t)$ are called conjugates of t. One small caveat is that these conjugates may not be expressible in t (in general, this is only possible with *algebraically closed* fields), but it is a fact from any ring theory course that there is a universe in which these conjugates exist. This does not seem helpful, until you consider the following fact:

Proposition 3.2. *Let $F(t)$ be a field and let $t_1, t_2, \ldots, t_m$ (with $t = t_1$) be conjugates of t in the algebraic closure of $F(t)$. Then any symmetric rational function of $t_1, \ldots, t_m$ (with coefficients in $F(t)$) actually lies in F.* ⌟

Proof. This is a consequence of the fundamental theorem of symmetric polynomials, which states that any symmetric function can be made from the following basic symmetric functions:

$$\begin{aligned} s_1(t_1, \ldots, t_m) &= t_1 + t_2 + \cdots + t_m \\ s_2(t_1, \ldots, t_m) &= t_1 t_2 + t_1 t_3 + \cdots + t_{m-1} t_m \\ &\vdots \\ s_m(t_1, \ldots, t_m) &= t_1 t_2 \cdots t_m \end{aligned}$$

We just note that these are exactly Vieta's relations that express the coefficients of $p(t)$ as mentioned before in terms of the roots, and the coefficients were in F. □

Suddenly, not only did the extra elements from the algebraic closure go away, so did t itself! This is not exactly surprising, since we are familiar with facts like the sum of two complex conjugates being real, etc. This is exactly what we need for our proof here.

Claim 3.3. *When $F(t)$ is algebraic, $f \in F$, and*

$$f = g' + c_1 \frac{h_1'}{h_1} + \cdots + c_n \frac{h_n'}{h_n}$$

for some $g, h_1, \ldots, h_n \in F(t)$, then an equation of this form is true with polynomials in F. ⌟

Proof. Let $t_1, \ldots, t_m$ be the conjugates of t (with $t_1 = t$), and note that we may work with them as elements of a differential field because each t_i' is uniquely defined by Proposition 2.6.

As previously noted, it is allowed to swap t with any t_i, and the resulting equation will still be true. I will denote the swap as you expect in the following:

$$f = g(t_i)' + c_1 \frac{h_1(t_i)'}{h_1(t_i)} + \cdots + c_n \frac{h_n(t_i)'}{h_n(t_i)}.$$

In order to get symmetric polynomials that cancel out t, we can do the following trick:

$$\begin{aligned} f &= \frac{1}{m} \sum_{i=1}^{m} f \\ &= \frac{1}{m} \sum_{i=1}^{m} \left(g(t_i)' + c_1 \frac{h_1(t_i)'}{h_1(t_i)} + \cdots + c_n \frac{h_n(t_i)'}{h_n(t_i)} \right) \\ &= \frac{1}{m} (g(t_1) + \cdots + g(t_m))' + \\ &\qquad \frac{c_1}{m} \frac{(h_1(t_1) \cdots h_1(t_m))'}{h_1(t_1) \cdots h_1(t_m)} + \cdots + \frac{c_n}{m} \frac{(h_n(t_1) \cdots h_n(t_m))'}{h_n(t_1) \cdots h_n(t_m)}. \end{aligned}$$

Since these are symmetric polynomials, by Proposition 3.2 we are done. □

3.2 The logarithmic and exponential cases

In many ways, these two cases will feel very similar to how we argued Corollary 1.3, especially to start: we will notice that when we write

$$f = g' + c_1 \frac{h_1'}{h_1} + \cdots + c_n \frac{h_n'}{h_n},$$

we may take the h_i's to be irreducible, monic, and distinct, and we may take the partial fraction decomposition of g with respect to t, so that each term of the decomposition looks like

$$\frac{p}{q^k},$$

where p and q are polynomials in $F[t]$, q is irreducible, and $\deg(p) < \deg(q)$. Such terms have derivative

$$\left(\frac{p}{q^k}\right)' = \frac{p'q^k - kpq'q^{k-1}}{q^{2k}} = \frac{p'}{q^k} - k\frac{pq'}{q^{k+1}}.$$

Claim 3.4. *When $F(t)$ is logarithmic, $f \in F$, and*

$$f = g' + c_1 \frac{h_1'}{h_1} + \cdots + c_n \frac{h_n'}{h_n}$$

for some $g, h_1, \ldots, h_n \in F(t)$, then an equation of this form is true with polynomials in F. ⌟

Proof. I would like to show that $\frac{pq'}{q^{k+1}}$ cannot be simplified further, that is, q does not divide pq'. Because q is irreducible, and q does not divide p as $\deg(p) < \deg(q)$, it suffices to show that q cannot divide q'.

Simply calculate that if $q = a_0 + a_1 t + \cdots + a_n t^n$, then

$$q' = a_0' + (a_1' t + a_1 t') + \cdots + (a_n' t^n + n a_n t' t^{n-1}).$$

We make take q to be monic (move the leading coefficient into p), so that $a_n' = 1' = 0$, then because $t' \in F$ for this logarithmic extension, $\deg(q') < \deg(q)$ so q cannot divide q'.

Now, because $f \in F$ and $\frac{pq'}{q^{k+1}}$ cannot be simplified further, one of the h_i must have denominator q^{k+1}, where k is the largest power of q in the partial fraction decomposition. But the h_i are irreducible, so they cannot have denominator with exponent more than 1, so $k = 0$. In other words, the partial fraction decomposition of g did not have any fractions all along, in other words, only the quotient part remains, so $g \in F[t]$. Now the only fractions remaining are the h_i, therefore we must have $h_i \in F$ for all i.

Lastly, it remains to deal with g. Since $f \in F$ and $h_i \in F$, we know that $g' \in F$. Thus, $g = at + b$ for some $b \in F$ and $a \in \mathrm{const}(F)$. So we get that $g' = at' + b' = a\frac{s'}{s} + b'$, where $t' = \frac{s'}{s}$. So we have a new $c_{n+1} = a$, $h_{n+1} = s$, and the new "g" is just b. □

Great! Now, we just have to deal with the exponential case, which will be extremely similar to the corollary and even use the same lemma.

Claim 3.5. *When $F(t)$ is exponential, $f \in F$, and*

$$f = g' + c_1 \frac{h_1'}{h_1} + \cdots + c_n \frac{h_n'}{h_n}$$

for some $g, h_1, \ldots, h_n \in F(t)$, then an equation of this form is true with polynomials in F. ⌟

Proof. Again we look at whether or not $\frac{pq'}{q^{k+1}}$ can be simplified further. If there exists such a term that cannot be simplified, then it must appear as the denominator for some h_i, but this implies that $k = 0$ and we can argue identically to the previous claim to get $g \in F[t]$ and $h_i \in F$. To get $g \in F$, simply recall that in an exponential extension $\deg(g) = \deg(g')$, and $g' \in F$, so g must be in F.

The other case is that q divide pq' for all terms in the partial fraction decomposition. Then q must divide q'. By Lemma 2.7, then $q = t$. Then all of the denominators of are powers of t. Comparing denominators with the h_i, which are all irreducible, we see that they must be in F or exactly t. But because we are in an exponential extension, if $h = t$, then $\frac{h'}{h} = s'$ for some $s \in F$. So, this s can go with the g term, and the only h_i remaining belong to F. Now, g must be a polynomial because there are no more denominators involving t, so we can argue identically to before. □

Congratulations! We're done!