DIFFERENTIAL GALOIS THEORY: A STUDY OF NONELEMENTARY ANTIDERIVATIVES

AMOL RAMA AND NILAY MISHRA

June 9, 2020

ABSTRACT. Throughout the course of mathematical studies, one can encounter several integrals that are key to solving a problem, but for some reason can never be integrated. Often solving these integrals can lead to huge mathematical breakthroughs; however, some indefinite integrals can never be evaluated. In particular, some classical functions simply do not have any elementary antiderivatives.

1. INTRODUCTION

But what does it mean for any antiderivative, or for any function at all, to truly be elementary? Clearly, based upon our intuition:

$$f(x) = \frac{\log(e^x + x^e + \pi \cdot 5^x)}{\sqrt{x - 2 + \sin x - \cos x} - \sqrt[5]{x^5 - 7x + \tan(3x+2)}}$$

is an elementary function since nothing more complicated that exponentiation, trigonometry, addition, and multiplication is being used. This notion of what makes some functions "elementary" will come useful later and will be explored upon in greater detail in the following section, where we will be examining it in an abstract setting.

Now, let's look at example where one can come across an indefinite integral that cannot be evaluated directly. Consider the prime counting function, denoted as $\pi(x)$ that counts the number of primes $p \leq x$. The famous prime number theorem in number theory states that:

$$\pi(n) \sim \text{Li}(n) = \int_2^n \frac{1}{\ln(x)}\, \mathrm{d}x$$

where $f(n) \sim g(n)$ (denoting asymptotic equivalence) is equivalent to $\lim\limits_{n\to\infty} \frac{f(n)}{g(n)} = 1$. The question therefore arises to compute the indefinite integral.

This, in fact, turns out to be impossible as we prove later. In particular, $\text{Li}(n)$ cannot be written in the elementary way we are accustomed to. This will be made more formal in subsequent sections.

Our next example will relate the idea of probability theory with computing an integral that cannot be evaluated in an elementary fashion. Consider the following theorem.

Theorem (Central Limit Theorem)
Define $Y_n \to Z$ if:

$$\lim_{n\to\infty} P(Y_n \leq x) = P(Y \leq x)$$

for any $x \in \mathbb{R}$ for which $P(Y \leq x)$ is continuous. Now, we must have that:

$$\frac{1}{\sqrt{n}} \sum_{i=1}^{n} X_i \to \int_0^x \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu^2)}{2\sigma^2}}$$

for independent and identically distributed random variables with mean μ and variance σ^2.

In particular, the definite integral can be evaluated as follows:

$$\int_{-\infty}^{\infty} ae^{-\frac{(x-b)^2}{2c^2}}\,\mathrm{d}x = \sqrt{2\pi}a \cdot |c|$$

$$\int_{-\infty}^{\infty} e^{-\frac{x^2}{2}}\,\mathrm{d}x = \sqrt{2\pi} \tag{1}$$

by a series of clever manipulations. Note, however, that when we begin to think about this as an indefinite integral, things break down and the manipulations no longer work. This is because this integral turns out to be *impossible* to evaluate.

Now consider the equation of a Gaussian Bell Curve, given by $y = ke^{-\frac{x^2}{2}}$ for some constant $k \in \mathbb{R}$ with the property that the area under the curve from $-\infty$ to ∞ is equal to 1.

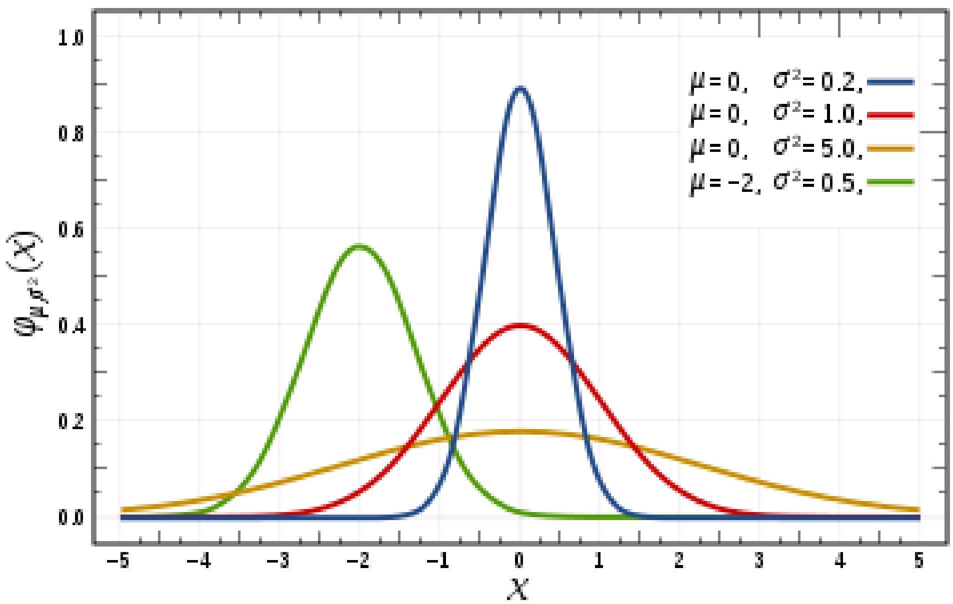

FIGURE 1. A picture of a Gaussian Bell Curve. Credit: Wikimedia Commons

In particular, we must have:

$$k = \frac{1}{\int_{-\infty}^{\infty} e^{-\frac{1}{2}x^2}\,\mathrm{d}x} = \frac{1}{\sqrt{2\pi}}$$

and so we must have $y = \dfrac{1}{2\pi}e^{-\frac{1}{2}x^2}$. In particular, the area until the curve from a to b is:

$$A = \frac{1}{2\pi}\int_a^b e^{-\frac{1}{2}x^2}\,\mathrm{d}x$$

Why is the area under the curve so important? It turns out that the probability of a certain random variable being in a particular range is given by that indefinite integral. In particular:

$$P(a \le X \le b) = A = \frac{1}{\sqrt{2\pi}}\int_a^b e^{-\frac{1}{2}x^2}\,\mathrm{d}x$$

for a random variable X. This turns out to be important in a variety of situation. The question then arises: *Why can't this integral be evaluated?* We will similarly show that the Gaussian error function given by:

$$\mathrm{erf}(z) = \frac{2}{\sqrt{\pi}\int_0^z e^{-x^2}\,\mathrm{d}x}$$

cannot be evaluated in an elementary fashion. This will be shown directly in the last section, but before then, we shall build up some tools.

Now, let's look at one last example: a set of two parametric equations. Let's define them now.

Definition 1 — The Fresnel integrals are two transcendental integrals ($S(x)$ and $C(x)$) given by:

$$S(x) = \int_0^t \sin(t^2)\ \mathrm{d}t \ \text{ and } \ C(x) = \int_0^t \cos(t^2)\ \mathrm{d}t$$

Current physics uses these integrals extensively in calculating both diffraction and the electromagnetic field intensity when light bends around opaque objects. They have also been used in highway, railroad, and roller coaster design, especially in a concept known as the Track Transition Curve. We will also investigate why the function $f(x) = \sin(x^2)$ and $g(x) = \cos(x^2)$ has no elementary antiderivative.

Thus, we shall show the following have no elementary antiderivatives:

- The Logarithmic Integral, which is the integral of $\frac{1}{\ln x}$.
- The Normal Distribution Function, which is the integral of $e^{-\frac{1}{2}x^2}$.
- The Gaussian Integral, which is the integral of e^{-x^2}.
- The Fresnel Integral, which is the integral of $\sin(x^2)$ and $\cos(x^2)$.

2. Basics of Elementary Fields

We're going to now see what an elementary field really is, mathematically speaking. To do, let's review a few definitions.

Definition 2 (Meromorphic Functions) **—** A meromorphic function $f : \mathbb{C} \to \mathbb{C}$ be a function that satisfies:

$$f(z) = \frac{g(z)}{h(z)}$$

where $h \neq 0$, and $g(z), h(z) : \mathbb{C} \to \mathbb{C}$ are *entire* functions i.e. they are analytic at all points $\mathbb{C} \to \mathbb{C}$.

These turn out to be quite important for both subsequent definitions and proofs, and in complex analysis in general. Now, we take a look at a differential field, which takes the idea of a derivative into a far more abstract setting, and looks at how $\mathbb{R}$ can be visualized as a field with an operator, δ, such that $\delta(f) = \frac{df}{\mathrm{d}x}$ for all functions $f(x) : \mathbb{R} \to \mathbb{R}$. We can define it so that the derivative is a linear map that satisfies the multiplication rule, and the other properties follow easily.

Definition 3 (Differential Fields) **—** A differential field is a field $\mathscr{F}$ together with a derivation $\delta : \mathscr{F} \to \mathscr{F}$, i.e. a $\mathscr{F}$-linear map satisfying the Leibniz rule

$$\delta(fg) = f\delta(g) + \delta(f)g$$

Let $\mathscr{F}$ be a differential field with derivation δ. The constant field of $\mathscr{F}$, denoted Con $\mathscr{F}$, is

$$\text{Con } \mathscr{F} = \{x \in \mathscr{F} \mid \delta(x) = 0\}$$

Note that these must form a subfield of $\mathscr{F}$.

Now, we take the idea of a splitting field, and extend it to the notion of a differential field. Let $\mathfrak{M}(S)$ denote all the metamorphic functions $f : S \to S$.

Definition 4 (Splitting Fields) **—** Let $\mathscr{L}$ be a differential operator on $\mathscr{F}$. The (differential) splitting field for $\mathscr{L}$, denoted $E_{\mathscr{L}}$, is the smallest subfield of $\mathfrak{M}(U_{\mathscr{L}})$ containing $\mathscr{F}$ and the solutions of $\mathscr{L}$.

We are now ready to take a look at what elementary fields are. This definition will be extremely important when we are trying to figure out which functions have elementary antiderivatives and which ones do not.

Definition 5 (Elementary Fields) — If $f_1, \ldots, f_n$ are meromorphic functions then $\mathscr{C}(f_1, \cdots, f_n)$ denotes the set of meromorphic functions h of the form

$$h = \frac{p(f_1, \cdots, f_n)}{q(f_1, \cdots, f_n)} = \frac{\sum a_{e_1, \cdots, e_n} f_1^{e_1} \cdots f_n^{e_n}}{\sum b_{j_1, \cdots, j_n} f_1^{j_1} \cdots f_n^{j_n}}$$

for n-variable polynomials:

$$p(X_1, \cdots, X_n) = \sum a_{e_1, \cdots, e_n} X_1^{e_1} \cdots X_n^{e_n}$$
$$q(X_1, \cdots, X_n) = \sum b_{j_1, \cdots, j_n} X_1^{j_1} \cdots X_n^{j_n}$$

in $\mathscr{C}[X_1, \cdots, X_n]$ with $q(f_1, \cdots, f_n) \neq 0$. A field K of meromorphic functions is an elementary field if $K = \mathscr{C}(x, f_1, \cdots, f_n)$ with each f_j either an exponential or logarithm of an element of $K_{j-1} = \mathscr{C}(x, f_1, \ldots, f_{j-1})$ or else algebraic over K_{j-1} in the sense that $P(f_j) = 0$ for some

$$P(T) = T^m + a_{m-1}T^{m-1} + \cdots + a_0 \in K_{j-1}[T]$$

with all $a_k \in K_{j-1}$. A meromorphic function f is an elementary function if it lies in an elementary field of meromorphic functions.

In this abstract setting, it is difficult to understand why the functions we think are elementary truly are. Let's do a quick example to understand this better.

Consider the function:

$$f(x) = \frac{\pi x^2 - 3x \log x}{\sqrt{e^x - \sin(x/(x^3 - 7))}}$$

There is an elementary field K where $f \in K$, in particular:

$$K = \mathscr{C}\left(x, \log(x), e^x, e^{\frac{ix}{x^3-7}}, \sqrt{e^x - \sin(x/(x^3 - 7))}\right)$$

is elementary. In particular, this definition simply formalizes what is elementary and what is not. Now, we put it to use and state and prove some important results in the field of differential Galois theory, proposed by Joseph Liouville.

3. A Theorem and Corollary of Liouville

The following theorem of Louiville will prove to be very useful. We state it here without proof.

Theorem (Liouville's Theorem)

Let $\mathscr{F}, \mathscr{G}$ be differential fields, let $a \in \mathscr{F}$, let $y \in \mathscr{G}$, and suppose $y' = a$ and $\mathscr{G}$ is an elementary differential extension field of $\mathscr{F}$, and Con $\mathscr{F} =$ Con $\mathscr{G}$. Then there exist $c_1, \ldots, c_n \in$ Con $\mathscr{F}$, $u_1, \ldots, u_n, v \in \mathscr{F}$ such that

$$a = v' + \sum_{j=1}^{n} c_j \frac{u_j'}{u_j}$$

In addition, the converse also holds. Let $a \in \mathscr{F}$ be an elementary function of the above form for some elementary field $\mathscr{F}$. Then, we can find an elementary antiderivative in some elementary extension of $\mathscr{F}$, denoted $\mathscr{F}'$, such that Con $\mathscr{F}' =$ Con $\mathscr{F}$.

Using this theorem, we can actually prove the following corollary which will enable us to prove that some classical function do not have any elementary antiderivatives.

Corollary (Liouville)

Consider functions $f(x), g(x)$, which are rational functions in $\mathbb{C}$ with $f(x), g'(x) \neq 0$. Then, the function $f(x)e^{g(x)}$ has an elementary integral if and only if there exists a rational function $R(x)$ satisfying

$$R'(x) + g'(x)R(x) = f(x)$$

Proof of Corollary. Define $t := e^g$. Then, we have that $t' = g't$. Thus, as g is nonconstant, we must have that $\frac{1}{g}$ has a root - this is essentially a pole of g. Note $h(x) = e^{\frac{1}{x}}$ has an essential singularity $x = 0$, where an essential singularity is a point a such that

$$\lim_{z\to a} h(z) \quad \text{and} \quad \lim_{z\to a} \frac{1}{h(z)}$$

are both not well-defined. Thus, t must have an essential singularity at the said pole. As all meromorphic functions have no essential singularities (as the only such points could be the roots of the denominator, but these turn out to be poles instead), t must be irreducible over $\mathbb{C}(z)$. Define $\mathscr{F} := \mathbb{C}(z)(t)$, the set of meromorphic functions in t over $\mathbb{C}$, and let $\mathscr{G}$ be the smallest elementary field extension of $\mathscr{F}$ containing t. Note that obviously the constants of $\mathscr{F}$ and $\mathscr{G}$ are the constant meromorphic functions, so thus we can apply Liouville's Theorem. Thus, we must have

$$f \cdot e^g = f \cdot t = v' + \sum_{j=1}^{n} c_j \frac{u_j'}{u_j}$$

Now, we can rewrite the product and quotient rules as (for functions $u(x), v(x)$)

$$\frac{(uv)'}{uv} = \frac{u'}{u} + \frac{v'}{v}$$

$$\frac{(u/v)'}{u/v} = \frac{u'}{u} - \frac{v'}{v}$$

To verify this, just multiply by the denominator of the left hand side. Now, this means that we can assume that each u_j is irreducible over $\mathbb{C}(z)$ (otherwise we can use the product/quotient rule). Now, note

$$\frac{\mathrm{d}}{\mathrm{d}z}(t^n) = \frac{\mathrm{d}}{\mathrm{d}z}(e^{ng}) = ng'e^{ng} = ng't^n$$

so differentiation (with respect to z) actually keeps the same degree in t.

Now, we can write

$$f \cdot e^g = f \cdot t = v' + \sum_{j=1}^{n} c_j \frac{u_j'}{u_j} = \Omega' + \sum_{j=1}^{n} c_j \frac{w_j}{u_j}$$

where $\Omega, w_j \in C(z)$ and $\deg_t(w_j) < \deg_t(u_j)$ (use polynomial division). Consider the partial fraction decomposition of Ω. Now, by the Uniqueness of Partial Fraction Decompositions, we must have that any non-multiple of t in the said partial fraction decomposition of $f \cdot t$ must be 0. In addition, note that the maximum degree is 1, as otherwise we would have terms such as t^2 (and $t \notin \mathscr{F}$). Thus, we can write

$$f \cdot t = (h \cdot t)'$$

for some $h \in C(z)$. Now, this means that

$$f \cdot e^g = f \cdot t = (h \cdot t)' = ht' + h't = he^g + g'he^g$$

so dividing by e^g finishes the proof.

4. Proving the Motivating Examples

Let's start by proving that the integrals stated in the introduction do not have elementary antiderivatives:

Motivating Example 1

$\frac{1}{\ln(x)}$ (the Logarithmic Integral) and $\frac{e^x}{x}$ do not have any elementary anti-derivative.

Proof. Suppose that there exists an elementary function g for which $g' = \frac{1}{\ln(x)}$, and so $g(e^x)' = \frac{e^x}{x}$ would also have an elementary antiderivative. We will therefore show that $h(x) = e^x/x$ has no elementary antiderivative.

By the corollary, there must exist $R(x) \in \mathbb{C}(x)$ such that:

$$R(x) + R'(x) = \frac{1}{x}$$

Now, suppose $R(x)$ was constant or a polynomial. Then $R(x)+R'(x)=\frac{1}{x}$ would be too, a contradiction. Since $R(x)$ is rational, write:

$$R(x)=\frac{p(x)}{q(x)}$$
$$R'(x)=\frac{p'(x)q(x)-p(x)q'(x)}{q(x)^2}$$
$$p(x)q(x)+p'(x)q(x)-p(x)q'(x)=q(x)^2$$

where $p(x)$ and $q(x)$ have no common factor. Now, suppose r is a root of $q(x)$. Then, we must have $p(r)q'(r)=0$. Since $p(r)\neq 0$, $q'(r)=0$, and so r is repeated at least twice. In particular, one denominator of the partial fraction decomposition of $R'(x)$ will be $(x-r)^{k+1}$ so of $R(x)+R'(x)\neq\frac{1}{x}$ as the maximum such power of $(x-r)$ in R(x) is $(x-r)^k$, making it impossible to "cancel" $\frac{1}{(x-r)^{k+1}}$. ■

Motivating Example 2

e^{-x^2} (the Gaussian Error Function) and $e^{-\frac{1}{2}x^2}$ (the Normal Distribution Function) do not have any elementary anti-derivatives.

Proof. We shall show that e^{-ax^2} does not have an elementary antiderivative, which will immediately show that none of the two have elementary antiderivatives. We use the corollary, and see that there must exist rational $R(x)\in\mathbb{C}(x)$ such that:

$$R'(x)-2axR(x)=1$$

As before, $R(x)=\frac{p(x)}{q(x)}$ is clearly not constant or a polynomial (due to degree issues). As before, we must have:

$$R'(x)=\frac{p'(x)q(x)-p(x)q'(x)}{q(x)^2}$$
$$p'(x)q(x)-p(x)q'(x)-2axp(x)q(x)=q(x)^2$$

Plugging in $x=r$ (which is possible because of the continuity of polynomials), we get that $p(r)q'(r)=0$. As we assumed $\gcd(p,q)=1$, we have that $q'(r)=1$, so $q(x)$ has a root r with multiplicity $k\geq 2$. Thus, the denominator of $R'-2axR$ will have a factor of $\frac{1}{(x-r)^k}$. ■

Motivating Example 3

$\sin(x^2)$ and $\cos(x^2)$ (the Fresnel Integrals) do not have any elementary anti-derivative.

Proof. We start by using the converse of Liouville's Theorem. Clearly $\sin(x^2)\in K\left(x,e^{ix^2}\right)$, it is elementary. Now, assume that it has an elementary antiderivative. Then, we can write it in the form of the theorem. From here, we can see that the only irreducible in the partial fraction expansion is e^{ix^2}. Now, note that the e^{ix^2} and e^{-ix^2} terms in the expansion must add up to $\sin(x^2)$ while the rest will cancel out. In particular, we have:

$$a+2ia'=\frac{1}{2i}$$

which has no solutions as in the first example in this section, so we are done with this proof. ■

References

[1] Brian Conrad. http://wstein.org/edu/winter06/20b/Conrad.pdf. Impossibility Theorems in Elementary Integration.
[2] A R Magid LECTURES ON DIFFERENTIAL GALOIS THEORY (AMS, 1994)