Elementary Functions and Liouville's Theorem

Definition: Let R be a commutative ring with 1. We call a map $\partial : R \to R$ a **derivation** if $\partial(a+b) = \partial(a) + \partial(b)$ and $\partial(ab) = \partial(a)b + a\partial(b)$ for all $a, b \in R$. A ring equipped with a particular derivation is called a **differential ring**. For convenience, we write $\partial(a) = a'$ (just like in calculus). If R is a differential ring and an integral domain, it is a **differential integral domain**. If R is a differential ring and a field, it is a **differential field**.

Let R be a differential ring.

- $1' = (1 \cdot 1)' = 1' \cdot 1 + 1 \cdot 1'$ so $1' = 1' + 1'$ and so $0 = 1'$. Notice that ∂ is a group homomorphism (consider R as an abelian group under addition), so $\partial(na) = n\partial(a)$ for all $a \in R$ and $n \in \mathbb{Z}$. Therefore, $\partial(n1) = n\partial(1) = n0 = 0$. Thus everything in the prime subring is a **constant** (i.e. has derivative zero).
- Given $a \in R$, notice that $(a^2)' = (a \cdot a)' = a'a + aa' = 2aa'$. In fact, we can prove (using induction), that

  $$(a^n)' = na^{n-1}a' \text{ for any } n \in \mathbb{Z}_{\geq 0} \qquad \text{(The power rule)}$$
- Let $a \in R^\times$ (a is a unit). Then $0 = 1' = (aa^{-1})' = a'a^{-1} + a(a^{-1})'$ so $a(a^{-1})' = -a^{-1}a'$. Dividing by a, we get that $(a^{-1})' = -a^{-2}a'$. Again, using induction, we have that $(a^n)' = na^{n-1}a'$ for all $n \in \mathbb{Z}$ (if a^{-1} exists).
- Let $a \in R$ and $b \in R^\times$. Then $(ab^{-1})' = a'b^{-1} + a(b^{-1})' = a'b^{-1} + a(-b^{-2}b')$. Therefore,

  $$\partial\left(\frac{a}{b}\right) = \frac{a'b - ab'}{b^2} \qquad \text{(The quotient rule)}$$

  This then implies that if $\mathbb{Q} \subseteq R$, every element of $\mathbb{Q}$ is a constant.

  Note: If R is a differential integral domain, then R's field of fractions $\mathbb{F}$ can be turned into a differential field in a unique way. We define $\partial(a/b)$ via the quotient rule. It is a simple exercise to show that this is well defined, extends the definition of ∂ from R to $\mathbb{F}$, and there is no other way to do this.

Definition: A **differential subring** of a differential ring R, is a subring (containing 1) which is closed under differentiation. Thus $S \subseteq R$ is a differential subring if $1 \in S$, $a, b \in S$ implies that $a - b$, ab, and $a' \in S$.

Likewise, a **differential ideal** of R is an ideal that is closed under differentiation. If I is a differential ideal of R, R/I becomes a differential ring if we define $\partial(a + I) = \partial(a) + I$ (it's easy to show that this is well defined).

A **differential homomorphism** between two differential rings R, S is a map $\varphi : R \to S$ which is a ring homomorphism (i.e. $\varphi(a+b) = \varphi(a) + \varphi(b)$, $\varphi(ab) = \varphi(a)\varphi(b)$, and $\varphi(1) = 1$) that preserves differentiation (i.e. $\varphi(a') = \varphi(a)'$). It's easy to show that the kernel of a differential homomorphism, $\ker(\varphi) = \{x \in R \mid \varphi(x) = 0\}$, is a differential ideal of the domain. Also, the image is a differential subring of the codomain and the isomorphism theorems all hold.

Lemma: Let R be a differential ring. The **constants** of R is the differential subring $C = \ker(\partial) = \{x \in R \mid x' = 0\}$. Moreover, if R is a differential field, then C is a differential subfield.

Proof: First, $1 \in C$ since $1' = 0$. Next, suppose $a, b \in C$. Then $(a-b)' = a' - b' = 0 - 0 = 0$ and $(ab)' = a'b + ab' = 0b + a0 = 0$ so $a - b, ab \in C$. Finally, for all $a \in C$, $a' = 0 \in C$. So C is a differential subring. Now in addition, suppose R is a field. Let $a \in C$ such that $a \neq 0$. Then $(a^{-1})' = -a^{-2}a' = -a^{-2}0 = 0$ so $a^{-1} \in C$. Thus C is a field. ∎

Example: Any commutative ring with 1 is a differential ring when given the derivation $\partial = 0$. In particular, $\mathbb{Q}$ is a differential ring with $\partial = 0$ and by some of the above discussion, this is our only choice!

The field of rational functions with real coefficients, $\mathbb{R}(x)$, is a differential field when given $\partial = \dfrac{d}{dx}$ (the usual derivative). Here the field of constants is $\mathbb{R}$ (as we would expect).

It is interesting (and strange) to consider that $\mathbb{Q}(\pi)$ (which is isomorphic to $\mathbb{Q}(x)$) is a differential field when given the derivation $\partial =$ "$d/d\pi$". In other words, $\pi' = 1$ and $(\pi^3)' = 3\pi^2$ etc. This indicates that $\mathbb{R}$ can be turned into a differential field in many *very strange* ways.

Lemma: Let $\mathbb{F}$ be a differential field of characteristic 0 and let $\mathbb{K}/\mathbb{F}$ be an algebraic extension (as regular old fields). The derivation on $\mathbb{F}$ can be extended to a derivative on $\mathbb{K}$ in exactly one way (i.e. $\mathbb{K}$ can be turned into a differential field and this can only be done in one way).

Proof: [Sketch] I'll just show uniqueness. For a complete proof see [Crespo & Hajto] Proposition 5.3.1.

Let $\alpha \in \mathbb{K}$ and let $f(x) \in \mathbb{F}[x]$ be the minimal polynomial for α over $\mathbb{F}$ (every element in an algebraic extension is *by definition* algebraic). Let $Df(x)$ be the formal derivative of our polynomial $f(x)$ (treating the coefficients like constants). Then $f(x)$ and $Df(x)$ are relatively prime ($f(x)$ is irreducible and $Df(x)$ has lower degree and is non-zero since $\mathbb{F}$ has characteristic 0). This means that $Df(\alpha) \neq 0$.

Consider $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Then $(f(x))' = nx^{n-1}x' + (a'_{n-1}x^{n-1} + (n-1)a_{n-1}x^{n-2}x') + \cdots + (a'_1 x + a_1 x') + a'_0$. Therefore, $(f(x))' = Df(x)x' + g(x)$ where $g(x) = a'_{n-1}x^{n-1} + \cdots + a'_1 x + a'_0$. Now α is the root of $f(x)$, so we must have $(f(\alpha))' = 0$. In other words, $0 = Df(\alpha)\alpha' + g(\alpha)$. So the only consistent way to define α' is $\dfrac{g(\alpha)}{Df(\alpha)}$. ■

$\boxed{\text{EXAMPLE:}}$ We know that the only derivation on $\mathbb{Q}$ is zero. Consider $\sqrt{5} \in \mathbb{Q}[\sqrt{5}]$. As in the above proof, we can figure out what the derivative of $\sqrt{5}$ must be from its minimal polynomial. $(\sqrt{5})^2 - 5 = 0$ so $2(\sqrt{5})(\sqrt{5})' - 0 = 0$ and thus $(\sqrt{5})' = 0/(2\sqrt{5}) = 0$ (as we might have guessed).

Even more can be said. Notice in the above proof, if α is algebraic over $\mathbb{F}$'s constants (i.e., $0 = f(\alpha) = a_n\alpha^n + \cdots + a_0$ where $a_n, \ldots, a_0$ are constant), then $g(x) = a'_n x^n + \cdots + a'_0 = 0$. Thus we must have $\alpha' = g(\alpha)/Df(\alpha) = 0$. Therefore, any element that is algebraic over the constants, is itself a constant. In particular, the only possible derivation on the field of algebraic numbers (i.e., $\overline{\mathbb{Q}}$) is $\partial = 0$.

$\boxed{\text{DEFINITION:}}$ Let $\mathbb{F}$ be a differential field. We call $\mathbb{F}(t)/\mathbb{F}$ a **logarithmic** extension if there exists some $s \in \mathbb{F}$ such that $t' = \dfrac{s'}{s}$. Similarly we call $\mathbb{F}(t)/\mathbb{F}$ an **exponential** extension if there exists some $s \in \mathbb{F}$ such that $t' = ts'$.

These definitions mimic the defining properties of the natural logarithm and the exponential function. Suppose that $t' = \dfrac{s'}{s}$ and we could "integrate". Then $t = \int t' = \int \frac{s'}{s} = \ln(s)$. Likewise, solving the "differential equation" $t' = ts'$ would give us $t = e^s$. The above definitions yield formal characterizations of these functions without requiring us to work with actual fields of functions (or dealing with actual real or complex variables).

$\boxed{\text{DEFINITION:}}$ Let $\mathbb{F}$ be a differential field with field of constants C $(= \ker(\partial))$. A differential field extension $\mathbb{E}/\mathbb{F}$ is an **elementary** extension if there exists a tower of differential fields (where all fields have the same constants):

$$\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq \cdots \subseteq \mathbb{F}_\ell = \mathbb{E}$$

such that each extension $\mathbb{F}_{j+1}/\mathbb{F}_j$ is either an algebraic, logarithmic, or exponential extension.

If $\mathbb{F} = \mathbb{C}(x)$ (thought of as actual rational functions in a single complex variable), then $\mathcal{E}$ is defined to be the collection of all complex functions which lie in some elementary extension of $\mathbb{C}(x)$ (we allow these functions to have domains which aren't all of $\mathbb{C}$). $\mathcal{E}$ is the field of elementary functions.

$\boxed{\text{EXAMPLE:}}$ Essentially elementary functions are the functions that can be built from $\mathbb{C}$ and $f(x) = x$ using algebra, exponentiation, and taking logarithms. For example: $f(x) = \sqrt{\dfrac{e^{\sqrt[3]{x^5+1}} - 7}{\ln(x^{15} + \sqrt{x^4 - 1}) + \ln(e^{1/x} - 6)}}$ is elementary.

Keep in mind that elementary functions also include some functions which may be unfamiliar to us. For example: The Bring radical is $\mathrm{BR}(a)$ is the unique real root of the polynomial $x^5 + x + a$ (then extend $\mathrm{BR}(a)$ analytically to a function of a complex variable). Because $Y = \mathrm{BR}(x)$ is a root of the equation $Y^5 + Y + x = 0$, we have that $\mathbb{C}(x)(\mathrm{BR}(x))$ is an elementary extension of $\mathbb{C}(x)$ and so $\mathrm{BR}(x)$ is an elementary function. By the way, for $Y = \mathrm{BR}(x)$, $0 = (Y^5 + Y + x)' = 5Y^4Y' + Y' + 1$ so $Y' = -\dfrac{1}{5Y^4 + 1}$. Thus $\mathrm{BR}'(x) = -\dfrac{1}{5 \cdot \mathrm{BR}(x)^4 + 1}$.

$\boxed{\text{EXAMPLE:}}$ What about trigonometric functions? The trig functions can be built from log's and exponential's. For example: $\sin(x) = \dfrac{e^{ix} - e^{-ix}}{2i}$ and $\cos(x) = \dfrac{e^{ix} + e^{-ix}}{2}$. Then $\tan(x)$, $\sec(x)$, $\csc(x)$, and $\cot(x)$ can be built from sine and cosine. Inverse trig functions? For example: $\arcsin(x) = -i\ln(ix + \sqrt{1 - x^2})$, $\arccos(x) = -i\ln(x + \sqrt{x^2 - 1})$, and $\arctan(x) = \dfrac{i}{2}\left(\ln(1 - ix) - \ln(1 + ix)\right)$. The other inverse functions have similar looking formulas.

This means that functions like $f(x) = e^{\tan(\sqrt{x})}\ln(\sin(x) + \sec^5(e^{\sqrt{x}}))$ are elementary.

We should be careful. By definition, elementary functions include all algebraic functions. They are closed under algebraic operations (for example: addition, multiplication, taking roots). They are also closed under function composition. However, they are not closed under function inverses. For example, $f(x) = xe^x$ under proper restrictions of domain can be inverted. One such branch of $f^{-1}(x)$ is called the Lambert W-function $W(x)$. Even though xe^x is elementary, $W(x)$ is not. See [Ritt2] for a characterization of when an inverse of an elementary function is still elementary.

Now let's prove Liouville's theorem which characterizes which functions live in an elementary extension. We will follow the proof as presented in [Rosenlicht].

$\boxed{\text{LEMMA:}}$ Let $\mathbb{F}$ be a differential field with differential field extension $\mathbb{F}(t)$. Suppose that $\mathbb{F}(t)$ and $\mathbb{F}$ have the same constants (i.e. the kernels of the derivations match) and that t is transcendental over $\mathbb{F}$.

1. Let $t' \in \mathbb{F}$ and $f(t) \in \mathbb{F}[t]$ with $\deg(f(t)) > 0$. Then $(f(t))' \in \mathbb{F}[t]$ and $\deg(f(t)) = \deg((f(t))')$ iff the leading coefficient of $f(t)$ is non-constant. If the leading coefficient of $f(t)$ is constant, then $\deg((f(t))') = \deg(f(t)) - 1$.

2. Let $t'/t \in \mathbb{F}$. Then for all $a \in \mathbb{F}^\times$, $n \in \mathbb{Z}_{\neq 0}$, $(at^n)' = ht^n$ for some $h \in \mathbb{F}^\times$. Moreover, if $f(t) \in \mathbb{F}[t]$ with $\deg(f(t)) > 0$, then $\deg(f(t)) = \deg((f(t))')$. Also, $(f(t))' = cf(t)$ for some $c \in \mathbb{F}$ iff $f(t)$ is a monomial.

Proof: Let $f(t) = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in \mathbb{F}[t]$ with $a_n \neq 0$ so that $\deg(f(t)) = n > 0$.

For item 1, $(f(t))' = a_n' t^n + (na_n t' + a_{n-1}')t^{n-1} + ((n-1)a_{n-1}t' + a_{n-2}')t^{n-2} + \cdots + (a_1 t' + a_0')$. Notice that the coefficients all lie in $\mathbb{F}$ since we have assumed $t' \in \mathbb{F}$ (if $a_j \in \mathbb{F}$, then $a_j' \in \mathbb{F}$ because $\mathbb{F}$ is a differential field).

Recall that a_n is non-constant iff $a_n' \neq 0$ (by definition). Thus the degree does not drop iff the leading coefficient is not constant. In the case that it is, we have $a_n' = 0$. Suppose that $(na_n t' + a_{n-1}') = 0$ (i.e. the coefficient of t^{n-1} is zero). This implies that $(na_n t + a_{n-1})' = na_n' t + na_n t' + a_{n-1}' = na_n t' + a_{n-1}' = 0$ (we are assuming $a_n' = 0$). Therefore, $na_n t + a_{n-1} = c$ for some constant $c \in \mathbb{F}$. Since $na_n \neq 0$ and $na_n, a_{n-1} \in \mathbb{F}$, we have t is algebraic over $\mathbb{F}$ (contradicting our hypothesis that t is transcendental over $\mathbb{F}$). Thus $(na_n t' + a_{n-1}') \neq 0$ and so the degree of $(f(t))'$ is $n-1$.

For item 2, let $t'/t = b \in \mathbb{F}$. Let $a \in \mathbb{F}^\times$. Then $(at^n)' = a't^n + nat^{n-1}t' = (a' + nab)t^n$ since $t' = bt$. If $a' + nab = 0$, then at^n would be constant. So t would satisfy the polynomial $aX^n + c$ for the constant $c = -at^n$. Since $a \neq 0$ and $a, c \in \mathbb{F}$, this would mean that t is algebraic over $\mathbb{F}$ (again, a contradiction). Therefore, $a' + nab \neq 0$ (i.e. $(at^n)' = ht^n$ where $h = a' + nab \in \mathbb{F}^\times$).

Notice that our calculation above shows that each non-zero term of $f(t)$ yields a non-zero term (of the same degree) in $(f(t))'$. Thus $\deg(f(t)) = \deg((f(t))')$. Also, if $f(t)$ is a non-zero monomial, say $f(t) = at^n$, the above calculation says that $(at^n)' = ht^n$ so $(f(t))' = cf(t)$ where $c = h/a \in \mathbb{F}^\times$.

Conversely, suppose that $(f(t))' = cf(t)$ for some $c \in \mathbb{F}$. Then the above calculations say that $c = h/a_j = (a_j' + ja_j b)/a_j$ for all $a_j \neq 0$. Suppose that $a_m, a_\ell \neq 0$ (where $m \neq \ell$). Then $\dfrac{a_m' + ma_m b}{a_m} = \dfrac{a_\ell' + \ell a_\ell b}{a_\ell}$. That means $(a_\ell' + \ell a_\ell b)a_m = (a_m' + ma_m b)a_\ell$. Therefore, $\left(\dfrac{a_m t^m}{a_\ell t^\ell}\right)' = \dfrac{(a_m' + ma_m b)a_\ell t^{m+\ell} - (a_\ell' + \ell a_\ell b)a_m t^{m+\ell}}{a_\ell^2 t^{2\ell}} = 0$. Thus $\dfrac{a_m t^m}{a_\ell t^\ell} = z$ for some constant $z \in \mathbb{F}$. Therefore, $a_m t^m - za_\ell t^\ell = 0$ (t satisfies a non-zero polynomial over $\mathbb{F}$). Thus t is algebraic over $\mathbb{F}$ (again, a contradiction). Therefore, at most one coefficient is non-zero (i.e. $f(t)$ is a monomial). ■

We can now give Liouville's theorem which characterizes which "functions" in $\mathbb{F}$ can be "integrated" in terms of elementary functions.

$\boxed{\text{THEOREM:}}$ (Liouville) Let $\mathbb{F}$ be a differential field of characteristic 0. Let $\alpha \in \mathbb{F}$. If $y' = \alpha$ has a solution y in an elementary extension of $\mathbb{F}$ (with the same constants), then there exists constants $c_1, \ldots, c_n$ and elements $u_1, \ldots, u_n, v \in \mathbb{F}$ such that

$$\alpha = v' + c_1 \frac{u_1'}{u_1} + c_2 \frac{u_2'}{u_2} + \cdots + c_n \frac{u_n'}{u_n}$$

Proof: Suppose that $y = \int \alpha$, a solution of $y' = \alpha$ is elementary over $\mathbb{F}$. This implies that there exists a tower of differential fields:

$$\mathbb{F} \subseteq \mathbb{F}(t_1) \subseteq \mathbb{F}(t_1, t_2) \subseteq \cdots \mathbb{F}(t_1, t_2, \ldots, t_N)$$

such that all of these fields have the same constants, $y \in \mathbb{F}(t_1, \ldots, t_N)$, and each t_i is either algebraic, logarithmic, or exponential over $\mathbb{F}(t_1, \ldots, t_{i-1})$.

Use proof by induction. If $N = 0$, $y \in \mathbb{F}$ and thus $\alpha = y' \in \mathbb{F}$ so we're done. Suppose the result is true for any tower of height $N-1$. Notice that the tower with $\mathbb{F}$ deleted is $N-1$ steps tall. Therefore, by induction, there exists constants $c_1, \ldots, c_n$ and elements $u_1, \ldots, u_n, v \in \mathbb{F}(t_1)$ such that $\alpha = v' + \sum\limits_{i=1}^{n} c_i \dfrac{u_i'}{u_i}$. We need to get elements in $\mathbb{F}$ (not $\mathbb{F}(t_1)$). To do this we consider several cases: t_1 is algebraic or transcendental (then when t_1 is transcendental it must be either logarithmic, or exponential).

Case 1: Suppose $t_1 = t$ is algebraic over $\mathbb{F}$. There exists some non-zero polynomials in $\mathbb{F}[t]$ such that $u_i = U_i(t)$ and $v = V(t)$. Consider the distinct conjugates of t in some algebraic closure of $\mathbb{F}(t)$ [or some splitting field over $\mathbb{F}(t)$] say $t = \tau_1, \tau_2, \ldots, \tau_s$. Now $\mathbb{E} = \mathbb{F}(\tau_1, \ldots, \tau_s)$ is an algebraic extension of $\mathbb{F}$ so it extends uniquely as a differential field. There is an automorphism of $\mathbb{E}$ fixing $\mathbb{F}$ such that $t = \tau_1$ maps to τ_j (this is the very definition of a "conjugate"), call this map

σ_j, then we have $\alpha = \sigma_j(\alpha) = \sigma_j\left(V(t)' + \sum_{i=1}^n c_i \frac{U_i'(t)}{U_i(t)}\right) = V(\tau_j)' + \sum_{i=1}^n c_i \frac{U_i'(\tau_j)}{U_i(\tau_j)}$ (because α and all of the coefficients in the polynomials U_i and V lie in $\mathbb{F}$ and so are fixed by σ).

Now we "symmetrize"! Add up all of these conjugate expressions and divide by s (note that s^{-1} exists because we are working in characteristic 0). First, note that by "logarithmic differentiation" we have:

$$\frac{(A_1 \cdots A_s)'}{A_1 \cdots A_s} = \frac{A_1'(A_2 \cdots A_s) + (A_1)A_2'(A_3 \cdots A_s) + \cdots + (A_1 \cdots A_{s-1})A_s'}{A_1 \cdots A_s} = \frac{A_1'}{A_1} + \cdots + \frac{A_s'}{A_s}$$

Therefore, symmetrizing yields:

$$\alpha = \frac{1}{s}\sum_{j=1}^s \alpha = \frac{1}{s}\sum_{j=1}^s \sigma_j(\alpha) = \frac{1}{s}\sum_{j=1}^s \left(V(\tau_j)' + \sum_{i=1}^n c_i \frac{U_i'(\tau_j)}{U_i(\tau_j)}\right) = \frac{1}{s}\sum_{j=1}^s V(\tau_j)' + \sum_{i=1}^n \frac{c_i}{s} \frac{(U_i(\tau_1)\cdots U_i(\tau_s))'}{U_i(\tau_1)\cdots U_i(\tau_s)}$$

Notice both $\frac{1}{s}(V(\tau_1)' + \cdots + V(\tau_s)')$ and $\frac{(U_i(\tau_1)\cdots U_i(\tau_s))'}{U_i(\tau_1)\cdots U_i(\tau_s)}$ are fixed by all automorphisms because they are symmetric. Hence, each of these lies in the ground field $\mathbb{F}$. Letting $v = \dfrac{1}{s}(V(\tau_1) + \cdots + V(\tau_s))$ and $u_i = U_i(\tau_1)\cdots U_i(\tau_s)$ we're done.

Case 2: Suppose that $t_1 = t$ is transcendental $\mathbb{F}$. Again we have $v, u_1, \ldots, u_n \in \mathbb{F}(t_1) = \mathbb{F}(t)$. But now, since t is transcendental, we need to consider rational polynomials in t with coefficients in $\mathbb{F}$. Such polynomials can be factored and for any $w = u_i$ we can get $w = a_1(t)^{k_1} \cdots a_\ell(t)^{k_\ell} \cdot b$ where $a_i(t) \in \mathbb{F}[t]$ is monic and irreducible, $k_j \in \mathbb{Z}_{\neq 0}$ (positive and negative powers), and $b \in \mathbb{F}^\times$. Again, using logarithmic differentiation we have

$$\frac{w'}{w} = \frac{(ba_1(t)^{k_1} \cdots a_\ell(t)^{k_\ell})'}{ba_1(t)^{k_1} \cdots a_\ell(t)^{k_\ell}} = \frac{b'}{b} + k_1 \frac{a_1'(t)}{a_1(t)} + \cdots + k_\ell \frac{a_\ell'(t)}{a_\ell(t)}$$

So without loss of generality we can assume each u_i is either a monic irreducible $a(t) \in \mathbb{F}[t]$ or an element of $\mathbb{F}$. As for v, decompose it into its partial fraction decomposition. After possibly a polynomial term, each term in the fractional part of this decomposition is of the form $\dfrac{g(t)}{f(t)^r}$ for some monic irreducible $f(t) \in \mathbb{F}[t]$ and some $g(t) \in \mathbb{F}[t]$ where $\deg(g(t)) < \deg(f(t))$.

Case 2A: Suppose that (in addition to being transcendental) t is logarithmic over $\mathbb{F}$. This means that there exists some $a \in \mathbb{F}^\times$ such that $t' = \dfrac{a'}{a}$. Thus $t' = a'/a \in \mathbb{F}$. By our lemma, if $f(t) \in \mathbb{F}[t]$, then $(f(t))' \in \mathbb{F}[t]$ and $(f(t))'$ has degree 1 less than that of $f(t)$. Since $f(t)$ is irreducible (and the $\mathbb{F}$ is separable since it has characteristic 0), $(f(t))'$ and $f(t)$ must be relatively prime. Notice that

$$\left(\frac{g(t)}{f(t)^r}\right)' = \frac{(g(t))'(f(t))^r - g(t)r(f(t))^{r-1}(f(t))'}{(f(t))^{2r}} = \frac{(g(t))'}{(f(t))^r} - \frac{rg(t)(f(t))'}{(f(t))^{r+1}}$$

Now $\deg(g(t))$ and $\deg((f(t))')$ are both less than $\deg(f(t))$. This along with the fact that $f(t)$ is irreducible implies that $f(t)$ does not divide $g(t)$ or $(f(t))'$. Therefore, the partial fraction decomposition of v' involves a term with the denominator $(f(t))^{r+1}$. Thus this appears in α's partial fraction decomposition. But $\alpha \in \mathbb{F}$ so it has no fractional part to its decomposition (it's already its own decomposition). Thus such terms cannot appear in v's decomposition. Likewise, they cannot appear in the u_i's either. Therefore, $u_1, \ldots, u_n \in \mathbb{F}$ and $v = V(t) \in \mathbb{F}[t]$ (a polynomial in t – that is – v has no fractional part).

At this point we have, $\alpha = (V(t))' - \sum_{i=1}^n c_i \frac{u_i'}{u_i}$ where c_i, u_i, u_i', and α all lie in $\mathbb{F}$. Therefore, $(V(t))' \in \mathbb{F}$. Hence $v = V(t) = ct + d$ for some $c, d \in \mathbb{F}$. But v' has degree 0, so c must be a constant. Therefore, $(V(t))' = c\dfrac{a'}{a} + d'$ where $a, d \in \mathbb{F}$ and c is a constant. We then have

$$\alpha = d' + c\frac{a'}{a} + \sum_{i=1}^n c_i \frac{u_i'}{u_i}$$

just as we wanted.

Case 2B: Suppose that (in addition to being transcendental) t is exponential over $\mathbb{F}$. This means $\dfrac{t'}{t} = b'$ for some $b \in \mathbb{F}$. Recall that our lemma says, $\deg(f(t)) = \deg((f(t))')$ and $f(t)$ divides $(f(t))'$ only if $f(t)$ is a monomial. So if $f(t)$ is monic irreducible and $f(t) \neq t$, then $f(t)$ is not a monomial and so $f(t)$ does not divide $(f(t))'$. As before, if $f(t) \neq t$, then $\dfrac{(f(t))'}{f(t)}$ can be written as a polynomial in t plus a proper fraction with denominator $f(t)$. We are led to the same contradiction since if $\dfrac{g(t)}{(f(t))^r}$ appears in the partial fraction decomposition of v, then v' will have a term in it's decomposition with denominator $(f(t))^{r+1}$, so this appears in the decomposition of $\alpha \in \mathbb{F}$ (which has no fractional part). The same applies to the u_i's. Therefore, the only fractional parts that can appear must have denominators $f(t)^m = t^m$. This implies that $v = V(t) = \sum a_j t^j$ for some $a_j \in \mathbb{F}$ where the sum ranges over a finite set of integers (some powers can be negative). Likewise, all $u_i \in \mathbb{F}$ with a possible exception of some $u_i = t$, without loss of generality, say $u_1 = t$. Then $\sum_{i=1}^n c_i \frac{u_i'}{u_i} = c_1 \frac{t'}{t} + \sum_{i=2}^n c_i \frac{u_i'}{u_i}$. But $\frac{t'}{t} = b' \in \mathbb{F}$. Therefore, again $(V(t))' = \alpha - c_1 b' - \sum_{i=2}^n c_i \frac{u_i'}{u_i} \in \mathbb{F}$. Recall that $(at^n)' = ht^n$ for some $h \in \mathbb{F}^\times$. But $(V(t))'$ has no t terms (it belongs to $\mathbb{F}$), thus $V(t) = at^0 = a \in \mathbb{F}^\times$. Therefore, $\alpha = c_1 \frac{t'}{t} + \sum_{i=2}^n c_i \frac{u_i'}{u_i} + v' = (c_1 b + v)' + \sum_{i=2}^n c_i \frac{u_i'}{u_i}$ as desired. ■

Now with Liouville's theorem in hand, we can show that various functions are not elementary functions. This means that we "cannot integrate" them (well, we can't integrate them and get a formula for the antiderivative written in terms of elementary functions).

COROLLARY: Let $f(x), g(x) \in \mathbb{C}(x)$ be nonzero and suppose that $g(x)$ is also non-constant. Then

$$\int f(x) e^{g(x)}\, dx \quad \text{is elementary} \quad \text{if and only if} \quad f(x) = a'(x) + a(x)g'(x) \quad \text{for some } a(x) \in \mathbb{C}(x).$$

Proof: We will suppress the variable x and write $f = f(x)$, $g = g(x)$, etc. Let $\mathbb{F} = \mathbb{C}(x)$ and $t = e^g$ so that we have $t'/t = g'$ (i.e. $\mathbb{F}(t)$ is an exponential extension). Also, since g is non-constant, $\mathbb{F}(t)$ is a pure transcendental extension of $\mathbb{F}$. Suppose that $\int fe^g\, dx = \int ft\, dx$ is elementary, by Liouville's theorem we can write

$$ft = v' + \sum_{i=1}^n c_i \frac{u_i'}{u_i} \quad \text{for some} \quad v, u_1, \ldots, u_n \in \mathbb{F}(t) \quad \text{and} \quad c_1, \ldots, c_n \in \mathbb{C}.$$

As in the proof of Liouville's theorem, we can factor each $u_i \notin \mathbb{F}$ into a power product of irreducible elements of $\mathbb{F}[t]$ and then using logarithmic differentiation, we can guarantee (at the expense of a possibly longer summation) that each of $u_i \notin \mathbb{F}$ is distinct, monic, and irreducible.

Now imagine that v has been expanded in its partial fraction decomposition (with respect to the ring $\mathbb{F}[t]$). If this decomposition of v had some (nonzero) term $\frac{a}{b^k}$ (necessarily with $\deg(a) < \deg(b)$ and $k \in \mathbb{Z}_{>0}$ as this is part of what it takes to be a term in a partial fraction decomposition), then when computing v' we would have a term $\frac{a'b^k - akb^{k-1}b'}{b^{2k}} = \frac{a'}{b^k} - k\frac{ab'}{b^{k+1}}$. Notice that $v' = ft - \sum c_i u_i'/u_i$ where the u_i's of degree > 0 are distinct, monic, and irreducible and only *appear in denominators raised to the first power*. This means that either $a'b^k - akb^{k-1}b' = 0$ (i.e. $(a/b)' = 0$) or $k = 1$ (i.e. only the first power of b can possibly appear in the denominator).

Now if $k = 1$, we have $\frac{a'}{b} - \frac{ab'}{b^2}$ and thus the second term cannot be unreduced (after reducing we can only have the first power of b appearing) so b must divide $-ab'$ (in $\mathbb{F}[t]$). Now b is irreducible so b either divides $-a$ or b'. But $\deg(a) < \deg(b)$, so b must divide b'. However, by our lemma, part 2, $\deg(b) = \deg(b')$, this means that $b' = cb$ for some $c \in \mathbb{F}$. Again by our lemma, b must be a monomial. It's irreducible, monic, and monomial so $b = t$.

On the other hand, $a'b^k - akb^{k-1}b' = 0$ and so $a'b = kab'$. Thus b divides kab' so as in the paragraph above we will be led to conclude that $b = t$. Therefore, the only fractional terms in the partial fraction decomposition of v have denominators $b^k = t^k$. Thus $v = \sum p_j t^j$ for some $p_j \in \mathbb{F}$ (the sum ranging over a finite set of integers).

Now turning back to the u_i's. Notice that $\sum_{i=1}^n c_i u_i'/u_i = ft - v' = ft - \sum p_j t^j$ and u_j is either in $\mathbb{F}$ or monic irreducible. Thus the only possible $u_i \notin \mathbb{F}$ would be $u_i = t$. In this case, $u_i'/u_i = t'/t \in \mathbb{F}$. Thus $\sum_{i=1}^n c_i u_i'/u_i \in \mathbb{F}$.

At this point we have $ft = v' + \sum_{i=1}^n c_i \frac{u_i'}{u_i} = \sum p_j' t^j + \sum p_j j t^{j-1} t' + q$ where $q = \sum_i u_i'/u_i \in \mathbb{F}$. Recall that $t'/t = g' \in \mathbb{F}$ so $ft = \sum p_j' t^j + \sum j p_j g' t^j + q$. Comparing coefficients of t^1, we get $f = p_1' + 1p_1 g'$. Letting $a = p_1$ ($\in \mathbb{F}$), we have $f = a' + ag'$ as desired.

Conversely, suppose that $f = a' + ag'$ for some $a \in \mathbb{F}$. Then $\int fe^g = \int (a' + ag')e^g = ae^g$. ■

EXAMPLE: $\int e^{x^2}\, dx$ is not elementary. In our corollary, this goes with $f(x) = 1$ and $g(x) = x^2$. So if it were elementary, we would have a solution $a(x) \in \mathbb{C}(x)$ for $1 = a'(x) + 2xa(x)$. Consider $a(x) = p(x)/q(x)$ for some $p(x), q(x) \in \mathbb{C}[x]$ and $q(x) \neq 0$. Without loss of generality, assume $p(x)$ and $q(x)$ are relatively prime. Then $1 = \frac{p'(x)q(x) - p(x)q'(x)}{q(x)^2} + 2x\frac{p(x)}{q(x)}$. Clearing denominators we get $q(x)^2 = p'(x)q(x) - p(x)q'(x) + 2xp(x)q(x)$. In other words, $q(x)(q(x)-2xp(x)-p'(x)) = -p(x)q'(x)$. Notice that if $q(x)$ has a root, say r, then $p(r) \neq 0$ (since $p(x)$ and $q(x)$ are relatively prime). But $q(x)(q(x)-2xp(x)-p'(x)) = -p(x)q'(x)$ so if $q(x)$ has a factor $(x-r)^k$ then $q'(x)$ must have the same factor! This is impossible ($q'(x)$ must have one less factor). Thus $q(x)$ cannot have any roots (i.e. $q(x) = c$ is constant). But then we have $a(x) = p(x)/c$ so $a(x)$ must be a polynomial. But then looking at degrees we have $0 = \deg(1) = \deg(a'(x) + 2xa(x)) = \deg(a(x)) + 1$ (contradiction). Hence, no such $a(x)$ exists. Thus our integral is not elementary. This means that the error function: $\mathrm{erf}(x) = (2/\sqrt{\pi}) \int_0^x e^{t^2}\, dt$ isn't elementary.

$\boxed{\text{EXAMPLE:}}$ $\displaystyle\int \frac{e^x}{x}\, dx$ is not elementary. In our corollary, this goes with $f(x) = 1/x$ and $g(x) = x$. So if it were elementary, we would have a solution $a(x) \in \mathbb{C}(x)$ for $1/x = a'(x) + 1a(x)$. In other words, $1 = x(a'(x) + a(x))$. If $a(x) = p(x)/q(x)$ is again written in lowest terms, $a'(x) = (p'(x)q(x) - p(x)q'(x))/q(x)^2$ and so after clearing denominators $q(x)^2 = x[p'(x)q(x) - p(x)q'(x) + p(x)q(x)]$. Suppose that $q(x)$ has some root $r \neq 0$ with multiplicity k, then $xp(x)q'(x) = q(x)[xp'(x) + p(x) - q(x)]$ and again we reach the same kind of contradiction as in the example above. Thus the only root $q(x)$ can have is 0. Since $q(x)^2 = x[p'(x)q(x) - p(x)q'(x) + p(x)q(x)]$, 0 is a root (and must be repeated). Thus $q(x) = cx^k$ for some $k > 1$. Then, $x^k(ckp(x)) = xp(x)kcx^{k-1} = xp(x)q'(x) = q(x)[xp'(x) + p(x) - q(x)] = cx^k[xp'(x) + p(x) - cx^k]$ and so $kp(x) = xp'(x) + p(x) - cx^k$ and thus $(k-1)p(x) = xp'(x) - cx^k$ so that $p(x)$ has 0 as a root. But then $p(x)$ and $q(x)$ aren't relatively prime (contradiction). Thus our integral is not elementary.

This also implies that the real and imaginary parts of this integral are not elementary. Therefore, the sine integral function $\mathrm{Si}(x) = \int_0^t \sin(t)/t\, dt$ isn't elementary.

$\boxed{\text{EXAMPLE:}}$ $\displaystyle\int \frac{1}{\ln(x)}\, dx$ is not elementary. Let $u = \ln(x)$ (so $e^u = x$) then $du = 1/x\, dx$ so that $\displaystyle\int 1/\ln(x)\, dx = \int x/(x\ln(x))\, dx = \int e^u/u\, du$. Thus if the integral of $1/\ln(x)$ were elementary, then $\displaystyle\int e^x/x\, dx$ would be too – which it isn't!

The above proof of Liouville's theorem was drawn from the article [Rosenlicht]. Additional examples of non-elementary integrals as well as some more details about our examples can be found in the article [Mead]. The books [Kaplansky] and [Ritt1] are classical introductions to differential algebra whereas [Magid] and [Crespo & Hajto] give more modern introductions to the subject.

It turns out that there is a complete algorithm for determining when a function can be integrated in terms of elementary functions. This is the so called "Ricsh Algorithm" developed by Robert Risch in the late 60's. For an excellent, very readable, introduction to this as well as more details about results like Liouville's theorem, I highly recommend [Geddes].

References

[Crespo & Hajto] T. Crespo and Z. Hajto, *Algebraic Groups and Differential Galois Theory*, AMS Graduate Studies in Mathematics **Vol. 122** (2011).

[Geddes] K. Geddes, S. Czapor, and G. Labahn, *Algorithms for Computer Algebra*, Kluwer Acad. Pub. (1992).

[Kaplansky] I. Kaplansky, *An Introduction to Differential Algebra*, Pub. of De L'Inst. De Math. De L'Univ. De Nancago (1957). Web: http://mmrc.iss.ac.cn/∼weili/DifferentialAlgebra/References/Kaplansky.pdf

[Magid] A. Magid, *Lectures on Differential Galois Theory*, AMS University Lecture Series **Vol. 7** (1994).

[Mead] D. Mead, *Integration*, Am. Math. Monthly **Vol. 68** No. 2 (Feb. 1961) 152–156.

[Ritt1] J. Ritt, *Differential Algebra*, Dover Publications (1950).

[Ritt2] J. Ritt *Elementary Functions and their Inverses*, Trans. Amer. Math. Soc. **27** (1925), 68–90.
Web: https://www.ams.org/journals/tran/1925-027-01/S0002-9947-1925-1501299-9/S0002-9947-1925-1501299-9.pdf

[Rosenlicht] M. Rosenlicht, *Integration in Finite Terms*, Am. Math. Monthly **Vol. 79** No. 9 (Nov. 1972) 963–972.