An Introduction to Differential Galois Theory

and the solvability of $\int e^{-x^2} dx$

Jason Baggett

University of Alaska Fairbanks

Dec. 14, 2009

Introduction

- Motivation: $\int e^{-x^2} dx = ?$

Introduction

- Motivation: $\int e^{-x^2}dx = ?$
- This function is fundamental to statistics

Introduction

- Motivation: $\int e^{-x^2} dx = ?$
- This function is fundamental to statistics
- From an analytic viewpoint, we know that the antiderivative exists (over $\mathbb{C}$) since e^{-x^2} is analytic

Introduction

- Motivation: $\int e^{-x^2} dx = ?$
- This function is fundamental to statistics
- From an analytic viewpoint, we know that the antiderivative exists (over $\mathbb{C}$) since e^{-x^2} is analytic
- But can $\int e^{-x^2} dx$ be expressed in terms of elementary functions?

Introduction

- Motivation: $\int e^{-x^2} dx = ?$
- This function is fundamental to statistics
- From an analytic viewpoint, we know that the antiderivative exists (over $\mathbb{C}$) since e^{-x^2} is analytic
- But can $\int e^{-x^2} dx$ be expressed in terms of elementary functions?
- The answer is no and we will soon see why

Elementary Functions

- Elementary functions are compositions of:
  exp
  log
  $\sqrt[n]{}$
  Polynomials
  The usual field operations $+, -, \cdot, \div$

Elementary Functions

- Elementary functions are compositions of:
  exp
  log
  $\sqrt[n]{}$
  Polynomials
  The usual field operations $+, -, \cdot, \div$
- Notice that working over $\mathbb{C}$, we also get the trigonometric functions and their inverses:
  Examples:

$$\cos(z) = \frac{e^{iz} + e^{-iz}}{2}$$

$$\cos^{-1}(z) = -i \log[z + i(1 - z^2)^{1/2}]$$

Differential Fields

- **Def:** For a field K, a **derivation** $D : K \to K$ is a map satisfying:
  (1) $D(x+y) = D(x) + D(y)$ Additive
  (2) $D(xy) = xD(y) + D(x)y$ Product Rule

Differential Fields

- **Def:** For a field K, a **derivation** $D : K \to K$ is a map satisfying:
  (1) $D(x+y) = D(x) + D(y)$ Additive
  (2) $D(xy) = xD(y) + D(x)y$ Product Rule
- A **differential field** is a field K with a derivation D.

Differential Fields

- **Def:** For a field K, a **derivation** $D : K \to K$ is a map satisfying:
  (1) $D(x+y) = D(x) + D(y)$ Additive
  (2) $D(xy) = xD(y) + D(x)y$ Product Rule
- A **differential field** is a field K with a derivation D.
- **Examples**:
  $\mathbb{C}(z)$ with the usual derivation $\frac{d}{dz}$

Differential Fields

- **Def:** For a field K, a **derivation** $D : K \to K$ is a map satisfying:
  (1) $D(x+y) = D(x) + D(y)$ Additive
  (2) $D(xy) = xD(y) + D(x)y$ Product Rule
- A **differential field** is a field K with a derivation D.
- **Examples**:
  $\mathbb{C}(z)$ with the usual derivation $\frac{d}{dz}$
- $\mathbb{F}_p(x)$ with the formal derivative $\frac{d}{dx}$

Differential Fields

- **Def:** For a field K, a **derivation** $D : K \to K$ is a map satisfying:
  (1) $D(x + y) = D(x) + D(y)$ Additive
  (2) $D(xy) = xD(y) + D(x)y$ Product Rule
- A **differential field** is a field K with a derivation D.
- **Examples**:
  $\mathbb{C}(z)$ with the usual derivation $\frac{d}{dz}$
- $\mathbb{F}_p(x)$ with the formal derivative $\frac{d}{dx}$
- Any field K with $D \equiv 0$

Field of Constants

- For a differential field K with derivation D, let

$$\mathrm{Con}(K) = \{c \in K : D(c) = 0\}$$

Field of Constants

- For a differential field K with derivation D, let

$$\mathrm{Con}(K) = \{c \in K : D(c) = 0\}$$

- Then $\mathrm{Con}(K)$ is a differential field. We call $\mathrm{Con}(K)$ the **field of constants**.

Field of Constants

- For a differential field K with derivation D, let

$$\mathrm{Con}(K) = \{c \in K : D(c) = 0\}$$

- Then $\mathrm{Con}(K)$ is a differential field. We call $\mathrm{Con}(K)$ the **field of constants**.
- We will only consider differential fields with field of constants $\mathbb{C}$.

Linear Differential Operators

- Analogous to considering polynomials, we will consider linear differential operators over a differential field K:

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + ... + a_1 y' + a_0 y$$

with the $a_i \in K$ and $y' = D(y)$.

Linear Differential Operators

- Analogous to considering polynomials, we will consider linear differential operators over a differential field K:

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \dots + a_1 y' + a_0 y$$

  with the $a_i \in K$ and $y' = D(y)$.
- We will study field extensions of K by adjoining solutions of $L(y) = 0$.

Analog of the Splitting Field

- **Existence of Solutions**:
  Working over $\mathbb{C}$ will guarantee the existence of solutions to $y^{(n)} + a_{n-1}y^{(n-1)} + \ldots + a_1 y' + a_0 y = 0$ provided the a_i are analytic (only continuous is necessary over $\mathbb{R}$). Notice that elementary functions are analytic (except possibly at isolated singularities and branch cuts).

Analog of the Splitting Field

- **Existence of Solutions**:
  Working over $\mathbb{C}$ will guarantee the existence of solutions to $y^{(n)} + a_{n-1}y^{(n-1)} + ... + a_1 y' + a_0 y = 0$ provided the a_i are analytic (only continuous is necessary over $\mathbb{R}$). Notice that elementary functions are analytic (except possibly at isolated singularities and branch cuts).
- It is easy to show that there is always a field M containing K with a solution y_0 to $L(y) = 0$ with $y_0 \notin K$.

Analog of the Splitting Field

- **Existence of Solutions**:
  Working over $\mathbb{C}$ will guarantee the existence of solutions to $y^{(n)} + a_{n-1}y^{(n-1)} + \ldots + a_1 y' + a_0 y = 0$ provided the a_i are analytic (only continuous is necessary over $\mathbb{R}$). Notice that elementary functions are analytic (except possibly at isolated singularities and branch cuts).
- It is easy to show that there is always a field M containing K with a solution y_0 to $L(y) = 0$ with $y_0 \notin K$.

Proof.

Let $R = K[y_0, y_1, \ldots, y_{n-1}]$ and define $D_R(k) = k'$ for $k \in K$. Define $D_R(y_i) = y_{i+1}$ for $i < n-1$ and $D_R(y_{n-1}) = -a_{n-1}y_{n-1} - \ldots - a_1 y_1 - a_0 y_0$. Notice that $y_0 \notin K$ is a solution of $y^{(n)} + a_{n-1}y^{(n-1)} + \ldots + a_1 y' + a_0 y = 0$. But R is an integral domain, so it has a field of fractions, M. Thus, $K \subseteq R \subseteq M$ and M contains a solution y_0 to $L(y) = 0$ with $y_0 \notin K$. $\square$

Analog of the Splitting Field (cont.)

- Notice what this last result implies: There are infinitely many linearly independent solutions to $L(y) = 0$ over K!

Analog of the Splitting Field (cont.)

- Notice what this last result implies: There are infinitely many linearly independent solutions to $L(y) = 0$ over K!
- We would like the analog of the splitting field to have exactly n linearly independent solutions. Why are there more solutions?

Analog of the Splitting Field (cont.)

- Notice what this last result implies: There are infinitely many linearly independent solutions to $L(y) = 0$ over K!
- We would like the analog of the splitting field to have exactly n linearly independent solutions. Why are there more solutions?
- The problem is that in the previous proof, M may have more constants than K

Analog of the Splitting Field (cont.)

- Notice what this last result implies: There are infinitely many linearly independent solutions to $L(y) = 0$ over K!
- We would like the analog of the splitting field to have exactly n linearly independent solutions. Why are there more solutions?
- The problem is that in the previous proof, M may have more constants than K
- **Example**: Consider the following ODE over $\mathbb{R}$

$$y' = y$$

We would like to think that the "splitting field" is $\mathbb{R}(e^x)$. But notice that ie^x is a second solution to the ODE that is linearly independent over $\mathbb{R}$.

Picard-Vessoit Extensions

- **Def:** Let L be a linear differential operator of order n over a differential field K. A differential field extension M of K is the **Picard-Vessoit extension of K for L** if:
  (1) The constants of M are the constants of K
  (2) M contains a full set V of n linearly independent solutions to L
  (3) M is the smallest differential field extension of K containing V

Picard-Vessoit Extensions

- **Def:** Let L be a linear differential operator of order n over a differential field K. A differential field extension M of K is the **Picard-Vessoit extension of K for L** if:
  (1) The constants of M are the constants of K
  (2) M contains a full set V of n linearly independent solutions to L
  (3) M is the smallest differential field extension of K containing V
- Picard-Vessoit extensions are the analog of splitting fields for linear, homogeneous ODEs. Moreover, they have normality and separability built into them.

Picard-Vessoit Extensions

- **Def:** Let L be a linear differential operator of order n over a differential field K. A differential field extension M of K is the **Picard-Vessoit extension of K for L** if:
  (1) The constants of M are the constants of K
  (2) M contains a full set V of n linearly independent solutions to L
  (3) M is the smallest differential field extension of K containing V
- Picard-Vessoit extensions are the analog of splitting fields for linear, homogeneous ODEs. Moreover, they have normality and separability built into them.
- Note: Picard-Vessoit extensions exist and are unique if the field of constants is algebraically closed. The proof of this will be omitted. We need not worry about this in the case of elementary functions.

Differential Galois Group

- For a Picard-Vessoit extension M/K with derivation D, define

$$\mathrm{Gal}_\partial(M/K) = \{\sigma \in \mathrm{Aut}(M) : \sigma \text{ fixes } K \text{ pointwise and } D\sigma = \sigma D\}$$

Differential Galois Group

- For a Picard-Vessoit extension M/K with derivation D, define

$$\mathrm{Gal}_\partial(M/K) = \{\sigma \in \mathrm{Aut}(M) : \sigma \text{ fixes } K \text{ pointwise and } D\sigma = \sigma D\}$$

- $\mathrm{Gal}_\partial(M/K)$ is the **differential Galois group** of M/K.

Differential Galois Group

- For a Picard-Vessoit extension M/K with derivation D, define

$$\mathrm{Gal}_\partial(M/K) = \{\sigma \in \mathrm{Aut}(M) : \sigma \text{ fixes } K \text{ pointwise and } D\sigma = \sigma D\}$$

- $\mathrm{Gal}_\partial(M/K)$ is the **differential Galois group** of M/K.
- $\mathrm{Gal}_\partial(M/K)$ can be thought of as a subgroup of $\mathrm{GL}_n(C)$ where C is the field of constants of K (and M).

Differential Galois Group (cont.)

- If $\sigma \in \mathrm{Gal}_\partial(M/K)$ is applied to $L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \ldots + a_1 y' + a_0 y$, then

$$\begin{aligned}
\sigma L(y) &= \sigma(y^{(n)} + a_{n-1}y^{(n-1)} + \ldots + a_1 y' + a_0 y) \\
&= \sigma(y^{(n)}) + a_{n-1}\sigma(y^{(n-1)}) + \ldots + a_1\sigma(y') + a_0\sigma(y) \\
&= \sigma(y)^{(n)} + a_{n-1}\sigma(y)^{(n-1)} + \ldots + a_1\sigma(y)' + a_0\sigma(y) \\
&= L\sigma(y)
\end{aligned}$$

Differential Galois Group (cont.)

- If $\sigma \in \mathrm{Gal}_\partial(M/K)$ is applied to $L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + ... + a_1 y' + a_0 y$, then

$$\begin{aligned} \sigma L(y) &= \sigma(y^{(n)} + a_{n-1}y^{(n-1)} + ... + a_1 y' + a_0 y) \\ &= \sigma(y^{(n)}) + a_{n-1}\sigma(y^{(n-1)}) + ... + a_1\sigma(y') + a_0\sigma(y) \\ &= \sigma(y)^{(n)} + a_{n-1}\sigma(y)^{(n-1)} + ... + a_1\sigma(y)' + a_0\sigma(y) \\ &= L\sigma(y) \end{aligned}$$

- Thus, σ must map a solution of L to another solution of L.

The Galois Correspondence Theorem

- **Theorem**: Let M be a Picard-Vessoit extension of a differential field K for the linear, homogeneous differential equation $L(y) = 0$. Let $G = \text{Gal}_\partial(M/K)$. Consider the two sets:
  $\mathcal{G}$ = the closed (under the Tariski topology) subgroups of G
  $\mathcal{F}$ = the differential subfields of M containing K.
  Define $\alpha : \mathcal{G} \to \mathcal{F}$ by $\alpha(H) = M^H$. Define $\beta : \mathcal{F} \to \mathcal{G}$ by $\beta(E) = \text{Gal}_\partial(M/E)$. Then

The Galois Correspondence Theorem

- **Theorem**: Let M be a Picard-Vessoit extension of a differential field K for the linear, homogeneous differential equation $L(y) = 0$. Let $G = \mathrm{Gal}_\partial(M/K)$. Consider the two sets:
  $\mathcal{G} =$ the closed (under the Tariski topology) subgroups of G
  $\mathcal{F} =$ the differential subfields of M containing K.
  Define $\alpha : \mathcal{G} \to \mathcal{F}$ by $\alpha(H) = M^H$. Define $\beta : \mathcal{F} \to \mathcal{G}$ by $\beta(E) = \mathrm{Gal}_\partial(M/E)$. Then
- (1) The maps α and β are inverses of each other

The Galois Correspondence Theorem

- **Theorem**: Let M be a Picard-Vessoit extension of a differential field K for the linear, homogeneous differential equation $L(y) = 0$. Let $G = \mathrm{Gal}_\partial(M/K)$. Consider the two sets:
  $\mathcal{G}$ = the closed (under the Tariski topology) subgroups of G
  $\mathcal{F}$ = the differential subfields of M containing K.
  Define $\alpha : \mathcal{G} \to \mathcal{F}$ by $\alpha(H) = M^H$. Define $\beta : \mathcal{F} \to \mathcal{G}$ by $\beta(E) = \mathrm{Gal}_\partial(M/E)$. Then
- (1) The maps α and β are inverses of each other
- (2) $H \triangleleft G \Leftrightarrow M^H$ is a Picard-Vessoit field for some linear differential equation over K

Liouville's Theorem

- **Theorem**: Suppose f is an elementary function and K is an elementary field with constants $\mathbb{C}$ containing f. Then $\int f$ is elementary if and only if there exists $c_1, ..., c_n \in \mathbb{C}$, nonzero $g_1, ..., g_n \in K$ and a function $h \in K$ such that

$$f = \sum_{i=1}^{n} c_i \frac{g_i'}{g_i} + h' \tag{1}$$

in which case $\int f = \sum_{i=1}^{n} c_i \log(g_i) + h$.

Liouville's Theorem

- **Theorem**: Suppose f is an elementary function and K is an elementary field with constants $\mathbb{C}$ containing f. Then $\int f$ is elementary if and only if there exists $c_1, \ldots, c_n \in \mathbb{C}$, nonzero $g_1, \ldots, g_n \in K$ and a function $h \in K$ such that

$$f = \sum_{i=1}^{n} c_i \frac{g_i'}{g_i} + h' \tag{1}$$

  in which case $\int f = \sum_{i=1}^{n} c_i \log(g_i) + h$.
- **Proof**:

Liouville's Theorem

- **Theorem**: Suppose f is an elementary function and K is an elementary field with constants $\mathbb{C}$ containing f. Then $\int f$ is elementary if and only if there exists $c_1, ..., c_n \in \mathbb{C}$, nonzero $g_1, ..., g_n \in K$ and a function $h \in K$ such that

$$f = \sum_{i=1}^{n} c_i \frac{g_i'}{g_i} + h' \tag{1}$$

  in which case $\int f = \sum_{i=1}^{n} c_i \log(g_i) + h$.
- **Proof**:
- $\Leftarrow$ Trivial

Liouville's Theorem

- **Theorem**: Suppose f is an elementary function and K is an elementary field with constants $\mathbb{C}$ containing f. Then $\int f$ is elementary if and only if there exists $c_1, \ldots, c_n \in \mathbb{C}$, nonzero $g_1, \ldots, g_n \in K$ and a function $h \in K$ such that

$$f = \sum_{i=1}^{n} c_i \frac{g_i'}{g_i} + h' \tag{1}$$

in which case $\int f = \sum_{i=1}^{n} c_i \log(g_i) + h$.
- **Proof**:
- $\Leftarrow$ Trivial
- $\Rightarrow$ Consider the tower of fields

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_m$$

where $K_i = K_{i-1}(t_i)$ where t_i is either (1) algebraic, (2) logarithmic, or (3) exponential over K_{i-1}.

Liouville's Theorem

- **Theorem**: Suppose f is an elementary function and K is an elementary field with constants $\mathbb{C}$ containing f. Then $\int f$ is elementary if and only if there exists $c_1, \ldots, c_n \in \mathbb{C}$, nonzero $g_1, \ldots, g_n \in K$ and a function $h \in K$ such that

$$f = \sum_{i=1}^{n} c_i \frac{g_i'}{g_i} + h' \tag{1}$$

  in which case $\int f = \sum_{i=1}^{n} c_i \log(g_i) + h$.
- **Proof**:
- $\Leftarrow$ Trivial
- $\Rightarrow$ Consider the tower of fields

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_m$$

  where $K_i = K_{i-1}(t_i)$ where t_i is either (1) algebraic, (2) logarithmic, or (3) exponential over K_{i-1}.
- We will prove this by induction on m, the length of the tower of fields.

Liouville's Theorem

- **Theorem**: Suppose f is an elementary function and K is an elementary field with constants $\mathbb{C}$ containing f. Then $\int f$ is elementary if and only if there exists $c_1, \ldots, c_n \in \mathbb{C}$, nonzero $g_1, \ldots, g_n \in K$ and a function $h \in K$ such that

$$f = \sum_{i=1}^{n} c_i \frac{g_i'}{g_i} + h' \tag{1}$$

  in which case $\int f = \sum_{i=1}^{n} c_i \log(g_i) + h$.
- **Proof**:
- $\Leftarrow$ Trivial
- $\Rightarrow$ Consider the tower of fields

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_m$$

  where $K_i = K_{i-1}(t_i)$ where t_i is either (1) algebraic, (2) logarithmic, or (3) exponential over K_{i-1}.
- We will prove this by induction on m, the length of the tower of fields.
- If $m = 0$, then take $c_i = g_i = 1$ and $h = \int f$.

Liouville's Theorem (cont.)

- Suppose that the result holds for $m-1$. We have that $f \in K_1 = K(t)$, so by the induction hypothesis

$$f = \sum_{i=1}^{n} c_i \frac{g_i'}{g_i} + h'$$

for $c_i \in \mathbb{C}$, $g_i \in K_1$, and $h \in K_1$.

Liouville's Theorem (cont.)

- Suppose that the result holds for $m-1$. We have that $f \in K_1 = K(t)$, so by the induction hypothesis

$$f = \sum_{i=1}^{n} c_i \frac{g_i'}{g_i} + h'$$

for $c_i \in \mathbb{C}$, $g_i \in K_1$, and $h \in K_1$.

- We have that $g_i = g_i(t)$ and $h = h(t)$ are rational functions in t with coefficients from K.

Liouville's Theorem (cont.)

- Suppose that the result holds for $m-1$. We have that $f \in K_1 = K(t)$, so by the induction hypothesis

$$f = \sum_{i=1}^{n} c_i \frac{g_i'}{g_i} + h'$$

  for $c_i \in \mathbb{C}$, $g_i \in K_1$, and $h \in K_1$.
- We have that $g_i = g_i(t)$ and $h = h(t)$ are rational functions in t with coefficients from K.
- **Case 1**: Suppose t is algebraic over K.

Liouville's Theorem (cont.)

- Suppose that the result holds for $m-1$. We have that $f \in K_1 = K(t)$, so by the induction hypothesis

$$f = \sum_{i=1}^{n} c_i \frac{g_i'}{g_i} + h'$$

for $c_i \in \mathbb{C}$, $g_i \in K_1$, and $h \in K_1$.

- We have that $g_i = g_i(t)$ and $h = h(t)$ are rational functions in t with coefficients from K.
- **Case 1**: Suppose t is algebraic over K.
- Then t has a minimal polynomial $p(x) \in K[x]$ with roots $t = \alpha_1, ..., \alpha_k$ and splitting field M.

Liouville's Theorem (cont.)

- Suppose that the result holds for $m-1$. We have that $f \in K_1 = K(t)$, so by the induction hypothesis

$$f = \sum_{i=1}^{n} c_i \frac{g_i'}{g_i} + h'$$

  for $c_i \in \mathbb{C}$, $g_i \in K_1$, and $h \in K_1$.
- We have that $g_i = g_i(t)$ and $h = h(t)$ are rational functions in t with coefficients from K.
- **Case 1**: Suppose t is algebraic over K.
- Then t has a minimal polynomial $p(x) \in K[x]$ with roots $t = \alpha_1, \ldots, \alpha_k$ and splitting field M.
- Let $\sigma_j : t \to \alpha_j$. Then $\sigma_j \in \mathrm{Gal}_\partial(M/K)$.

Liouville's Theorem (cont.)

- Then

$$f = \sigma_j(f) = \sigma_j\left(\sum_{i=1}^{n} c_i \frac{g_i(t)'}{g_i(t)} + h(t)'\right)$$
$$= \sum_{i=1}^{n} c_i \frac{g_i(\alpha_j)'}{g_i(\alpha_j)} + h(\alpha_j)'$$

Liouville's Theorem (cont.)

- Then

$$f = \sigma_j(f) = \sigma_j\left(\sum_{i=1}^{n} c_i \frac{g_i(t)'}{g_i(t)} + h(t)'\right)$$
$$= \sum_{i=1}^{n} c_i \frac{g_i(\alpha_j)'}{g_i(\alpha_j)} + h(\alpha_j)'$$

- Therefore,

$$f = \frac{1}{k}\left[\sum_{j=1}^{k}\sum_{i=1}^{n} c_i \frac{g_i(\alpha_j)'}{g_i(\alpha_j)} + \sum_{j=1}^{k} h(\alpha_j)'\right]$$
$$= \sum_{i=1}^{n} \frac{c_i}{k}\left[\sum_{j=1}^{k} \frac{g_i(\alpha_j)'}{g_i(\alpha_j)}\right] + \frac{1}{k}\left[\sum_{j=1}^{k} h(\alpha_j)'\right]$$

Liouville's Theorem (cont.)

- Now

$$\frac{\left[\prod_{j=1}^{k} g_i(\alpha_j)\right]'}{\prod_{j=1}^{k} g_i(\alpha_j)} = \frac{g_i(\alpha_1)' g_i(\alpha_2) \ldots g_i(\alpha_k) + \ldots + g_i(\alpha_1) g_i(\alpha_2) \ldots g_i(\alpha_k)'}{g_i(\alpha_1) g_i(\alpha_2) \ldots g_i(\alpha_k)}$$
$$= \frac{g_i(\alpha_1)'}{g_i(\alpha_1)} + \frac{g_i(\alpha_2)'}{g_i(\alpha_2)} + \ldots + \frac{g_i(\alpha_k)'}{g_i(\alpha_k)}$$
$$= \sum_{j=1}^{k} \frac{g_i(\alpha_j)'}{g_i(\alpha_j)}$$

Liouville's Theorem (cont.)

- Now

$$\frac{\left[\prod_{j=1}^{k} g_i(\alpha_j)\right]'}{\prod_{j=1}^{k} g_i(\alpha_j)} = \frac{g_i(\alpha_1)' g_i(\alpha_2)...g_i(\alpha_k) + ... + g_i(\alpha_1)g_i(\alpha_2)...g_i(\alpha_k)'}{g_i(\alpha_1)g_i(\alpha_2)...g_i(\alpha_k)}$$

$$= \frac{g_i(\alpha_1)'}{g_i(\alpha_1)} + \frac{g_i(\alpha_2)'}{g_i(\alpha_2)} + ... + \frac{g_i(\alpha_k)'}{g_i(\alpha_k)}$$

$$= \sum_{j=1}^{k} \frac{g_i(\alpha_j)'}{g_i(\alpha_j)}$$

- Therefore,

$$f = \sum_{i=1}^{n} \frac{c_i}{k} \left[\sum_{j=1}^{k} \frac{g_i(\alpha_j)'}{g_i(\alpha_j)}\right] + \frac{1}{k}\left[\sum_{j=1}^{k} h(\alpha_j)'\right]$$

$$= \sum_{i=1}^{n} \frac{c_i}{k} \frac{\left[\prod_{j=1}^{k} g_i(\alpha_j)\right]'}{\prod_{j=1}^{k} g_i(\alpha_j)} + \left[\frac{1}{k}\sum_{j=1}^{k} h(\alpha_j)\right]'.$$

Liouville's Theorem (cont.)

- Notice that $\prod_{j=1}^{k} g_i(\alpha_j) \in M^{<\sigma_j \mid 1 \leq j \leq k>} = K$, and similarly $\frac{1}{k}\sum_{j=1}^{k} h(\alpha_j) \in K$.

- Notice that $\prod_{j=1}^{k} g_i(\alpha_j) \in M^{<\sigma_j \mid 1 \leq j \leq k>} = K$, and similarly $\frac{1}{k}\sum_{j=1}^{k} h(\alpha_j) \in K$.
- Thus, f has the desired form of (1).

Liouville's Theorem (cont.)

- Notice that $\prod_{j=1}^{k} g_i(\alpha_j) \in M^{<\sigma_j \mid 1 \leq j \leq k>} = K$, and similarly $\frac{1}{k}\sum_{j=1}^{k} h(\alpha_j) \in K$.
- Thus, f has the desired form of (1).
- **Case 2**: Now suppose that t is logarithmic over K, i.e. $t' = \frac{k'}{k}$ for some $k \in K$.

Liouville's Theorem (cont.)

- Notice that $\prod_{j=1}^{k} g_i(\alpha_j) \in M^{<\sigma_j \mid 1 \leq j \leq k>} = K$, and similarly $\frac{1}{k}\sum_{j=1}^{k} h(\alpha_j) \in K$.
- Thus, f has the desired form of (1).
- **Case 2**: Now suppose that t is logarithmic over K, i.e. $t' = \frac{k'}{k}$ for some $k \in K$.
- We may assume that the g_i are distinct, irreducible, monic polynomials in $K[t]$ (consider $\int f$ and break up the log's). Taking derivatives, we see that $\deg(g_i') < \deg(g_i)$ since

$$(t^m + ... + a_1 t + a_0)' = m\frac{k'}{k}t^{m-1} + ... + (a_1\frac{k'}{k} + a_0')$$

Thus, g_i' is not divisible by g_i.

Liouville's Theorem (cont.)

- Furthermore, we may assume h is decomposed into partial fractions, so h is a polynomial plus a sum of fractions of the form $\frac{a(t)}{b(t)^{\ell}}$ where $b(t)$ is irreducible and $\deg(a) < \deg(b)$. Moreover, we may assume that the b are distinct from the g_i and each other.

Liouville's Theorem (cont.)

- Furthermore, we may assume h is decomposed into partial fractions, so h is a polynomial plus a sum of fractions of the form $\frac{a(t)}{b(t)^\ell}$ where $b(t)$ is irreducible and $\deg(a) < \deg(b)$. Moreover, we may assume that the b are distinct from the g_i and each other.
- Then h' is a polynomial plus a sum of the form $\frac{-\ell ab'}{b^{\ell+1}} + \frac{a'}{b^\ell}$. In particular, $b^{\ell+1}$ does not divide ab'.

Liouville's Theorem (cont.)

- Furthermore, we may assume h is decomposed into partial fractions, so h is a polynomial plus a sum of fractions of the form $\frac{a(t)}{b(t)^\ell}$ where $b(t)$ is irreducible and $\deg(a) < \deg(b)$. Moreover, we may assume that the b are distinct from the g_i and each other.
- Then h' is a polynomial plus a sum of the form $\frac{-\ell a b'}{b^{\ell+1}} + \frac{a'}{b^\ell}$. In particular, $b^{\ell+1}$ does not divide ab'.
- But no $\frac{g_i'}{g_i}$ terms cancels with $\frac{-\ell a b'}{b^{\ell+1}}$ since the b and g_i are distinct and irreducible. Since the sum of these fractions is $f \in K$, the fractions of the form $\frac{a(t)}{b(t)^\ell}$ in h must be in K. But $\deg(a) < \deg(b)$ implies that $\frac{a(t)}{b(t)^\ell} = 0$. Thus, h is a polynomial in t with coefficients from K.

Liouville's Theorem (cont.)

- Furthermore, we may assume h is decomposed into partial fractions, so h is a polynomial plus a sum of fractions of the form $\frac{a(t)}{b(t)^\ell}$ where $b(t)$ is irreducible and $\deg(a) < \deg(b)$. Moreover, we may assume that the b are distinct from the g_i and each other.
- Then h' is a polynomial plus a sum of the form $\frac{-\ell ab'}{b^{\ell+1}} + \frac{a'}{b^\ell}$. In particular, $b^{\ell+1}$ does not divide ab'.
- But no $\frac{g_i'}{g_i}$ terms cancels with $\frac{-\ell ab'}{b^{\ell+1}}$ since the b and g_i are distinct and irreducible. Since the sum of these fractions is $f \in K$, the fractions of the form $\frac{a(t)}{b(t)^\ell}$ in h must be in K. But $\deg(a) < \deg(b)$ implies that $\frac{a(t)}{b(t)^\ell} = 0$. Thus, h is a polynomial in t with coefficients from K.
- Similarly, the $\frac{g_i'}{g_i}$ must be in K since nothing can cancel with them. But $\deg(g_i') < \deg(g_i)$ implies $g_i \in K$.

Liouville's Theorem (cont.)

- Therefore, $h' = f - \sum_{i=1}^{n} c_i \frac{g_i'}{g_i}$ is in K.

Liouville's Theorem (cont.)

- Therefore, $h' = f - \sum_{i=1}^{n} c_i \frac{g_i'}{g_i}$ is in K.
- Since h is a polynomial in t, the only way this can be is if $h = at + b$ where $a \in \mathbb{C}$ and $b \in K$.

Liouville's Theorem (cont.)

- Therefore, $h' = f - \sum_{i=1}^{n} c_i \frac{g_i'}{g_i}$ is in K.
- Since h is a polynomial in t, the only way this can be is if $h = at + b$ where $a \in \mathbb{C}$ and $b \in K$.
- Then

$$f = \sum_{i=1}^{n} c_i \frac{g_i'}{g_i} + a\frac{k'}{k} + b'$$

  is of the desired form (1).

Liouville's Theorem (cont.)

- **Case 3**: Now suppose t is exponential over K, i.e. $\frac{t'}{t} = s'$ for some $s \in K$. We proceed similarly as in Case 2. In this case, $\deg(g_i') = \deg(g_i)$ since

$$(t^m + ... + a_1 t + a_0)' = mst^m + ... + a_1 st + a_0'$$

However, g_i still does not divide g_i', unless $g_i = t$. In any case, we have $\frac{g_i'}{g_i}$ must be in K as before.

Liouville's Theorem (cont.)

- **Case 3**: Now suppose t is exponential over K, i.e. $\frac{t'}{t} = s'$ for some $s \in K$. We proceed similarly as in Case 2. In this case, $\deg(g_i') = \deg(g_i)$ since

$$(t^m + \ldots + a_1 t + a_0)' = mst^m + \ldots + a_1 st + a_0'$$

  However, g_i still does not divide g_i', unless $g_i = t$. In any case, we have $\frac{g_i'}{g_i}$ must be in K as before.
- If $g_i \neq t$, then this implies $g_i \in K$.

Liouville's Theorem (cont.)

- **Case 3**: Now suppose t is exponential over K, i.e. $\frac{t'}{t} = s'$ for some $s \in K$. We proceed similarly as in Case 2. In this case, $\deg(g_i') = \deg(g_i)$ since

$$(t^m + ... + a_1 t + a_0)' = mst^m + ... + a_1 st + a_0'$$

  However, g_i still does not divide g_i', unless $g_i = t$. In any case, we have $\frac{g_i'}{g_i}$ must be in K as before.
- If $g_i \neq t$, then this implies $g_i \in K$.
- Also as before, we must have that $h \in K[t]$ and $h' \in K$.

Liouville's Theorem (cont.)

- **Case 3**: Now suppose t is exponential over K, i.e. $\frac{t'}{t} = s'$ for some $s \in K$. We proceed similarly as in Case 2. In this case, $\deg(g_i') = \deg(g_i)$ since

$$(t^m + ... + a_1 t + a_0)' = mst^m + ... + a_1 st + a_0'$$

  However, g_i still does not divide g_i', unless $g_i = t$. In any case, we have $\frac{g_i'}{g_i}$ must be in K as before.
- If $g_i \neq t$, then this implies $g_i \in K$.
- Also as before, we must have that $h \in K[t]$ and $h' \in K$.
- This implies that $h \in K$ since $\deg(h') = \deg(h)$.

Liouville's Theorem (cont.)

- If all of the $g_i \neq t$, then all the $g_i \in K$ and

$$f = \sum_{i=1}^{n} c_i \frac{g_i'}{g_i} + h'$$

is of the desired form (1).

Liouville's Theorem (cont.)

- If all of the $g_i \neq t$, then all the $g_i \in K$ and

$$f = \sum_{i=1}^{n} c_i \frac{g_i'}{g_i} + h'$$

  is of the desired form (1).
- Otherwise, a single $g_i = t$. Without loss of generality, suppose $g_n = t$. Then $\frac{g_n'}{g_n} = s'$, so

$$f = \sum_{i=1}^{n-1} c_i \frac{g_i'}{g_i} + (c_n s + h)'$$

  is of the desired form (1). This completes the proof.

A Useful Corollary

- **Corollary:** Let K be an elementary differential field with field of constants $\mathbb{C}$, and let $f, g \in K$. Suppose e^g is transcendental over K. Then $\int fe^g$ is elementary if and only if there exists $r \in K$ such that $f = r' + rg'$.

A Useful Corollary

- **Corollary:** Let K be an elementary differential field with field of constants $\mathbb{C}$, and let $f, g \in K$. Suppose e^g is transcendental over K. Then $\int fe^g$ is elementary if and only if there exists $r \in K$ such that $f = r' + rg'$.
- **Proof:** $\Leftarrow$ Suppose $f = r' + rg'$ for some $r \in K$. Then $fe^g = r'e^g + rg'e^g = (re^g)'$. Thus, $\int fe^g = re^g$, which is elementary.

A Useful Corollary

- **Corollary:** Let K be an elementary differential field with field of constants $\mathbb{C}$, and let $f, g \in K$. Suppose e^g is transcendental over K. Then $\int fe^g$ is elementary if and only if there exists $r \in K$ such that $f = r' + rg'$.
- **Proof:** $\Leftarrow$ Suppose $f = r' + rg'$ for some $r \in K$. Then $fe^g = r'e^g + rg'e^g = (re^g)'$. Thus, $\int fe^g = re^g$, which is elementary.
- $\Rightarrow$ Suppose $\int fe^g$ is elementary. By Liouville's Theorem,

$$fe^g = \sum_{i=1}^{n} c_i \frac{g_i'}{g_i} + h'$$

for some $c_i \in \mathbb{C}$ and $g_i, h \in K(e^g)$.

A Useful Corollary

- **Corollary:** Let K be an elementary differential field with field of constants $\mathbb{C}$, and let $f, g \in K$. Suppose e^g is transcendental over K. Then $\int fe^g$ is elementary if and only if there exists $r \in K$ such that $f = r' + rg'$.
- **Proof:** $\Leftarrow$ Suppose $f = r' + rg'$ for some $r \in K$. Then $fe^g = r'e^g + rg'e^g = (re^g)'$. Thus, $\int fe^g = re^g$, which is elementary.
- $\Rightarrow$ Suppose $\int fe^g$ is elementary. By Liouville's Theorem,

$$fe^g = \sum_{i=1}^{n} c_i \frac{g_i'}{g_i} + h'$$

  for some $c_i \in \mathbb{C}$ and $g_i, h \in K(e^g)$.
- The g_i and h can be viewed as rational functions of e^g with coefficients from K.

A Useful Corollary

- **Corollary:** Let K be an elementary differential field with field of constants $\mathbb{C}$, and let $f, g \in K$. Suppose e^g is transcendental over K. Then $\int fe^g$ is elementary if and only if there exists $r \in K$ such that $f = r' + rg'$.
- **Proof:** $\Leftarrow$ Suppose $f = r' + rg'$ for some $r \in K$. Then $fe^g = r'e^g + rg'e^g = (re^g)'$. Thus, $\int fe^g = re^g$, which is elementary.
- $\Rightarrow$ Suppose $\int fe^g$ is elementary. By Liouville's Theorem,

$$fe^g = \sum_{i=1}^{n} c_i \frac{g_i'}{g_i} + h'$$

for some $c_i \in \mathbb{C}$ and $g_i, h \in K(e^g)$.

- The g_i and h can be viewed as rational functions of e^g with coefficients from K.
- Moreover, just as before, we can assume that the g_i are irreducible, monic polynomials.

A Useful Corollary (cont.)

- Just as in Case 3 of the proof of Liouville's Theorem, $\deg(g_i') = \deg(g_i)$, and g_i does not divide g_i' unless $g_i = e^g$.

A Useful Corollary (cont.)

- Just as in Case 3 of the proof of Liouville's Theorem, $\deg(g_i') = \deg(g_i)$, and g_i does not divide g_i' unless $g_i = e^g$.
- Suppose $g_i \neq e^g$. Then there is nothing to cancel with $\frac{g_i'}{g_i}$ in the sum to acquire fe^g. So $\frac{g_i'}{g_i}$ must be 0, or otherwise we would have a leftover fraction in the sum and not fe^g.

A Useful Corollary (cont.)

- Just as in Case 3 of the proof of Liouville's Theorem, $\deg(g_i') = \deg(g_i)$, and g_i does not divide g_i' unless $g_i = e^g$.
- Suppose $g_i \neq e^g$. Then there is nothing to cancel with $\frac{g_i'}{g_i}$ in the sum to acquire fe^g. So $\frac{g_i'}{g_i}$ must be 0, or otherwise we would have a leftover fraction in the sum and not fe^g.
- If $g_i = e^g$, then $\frac{g_i'}{g_i} = g'$. Without loss of generality, suppose $g_n = e^g$.

A Useful Corollary (cont.)

- Just as in Case 3 of the proof of Liouville's Theorem, $\deg(g_i') = \deg(g_i)$, and g_i does not divide g_i' unless $g_i = e^g$.
- Suppose $g_i \neq e^g$. Then there is nothing to cancel with $\frac{g_i'}{g_i}$ in the sum to acquire fe^g. So $\frac{g_i'}{g_i}$ must be 0, or otherwise we would have a leftover fraction in the sum and not fe^g.
- If $g_i = e^g$, then $\frac{g_i'}{g_i} = g'$. Without loss of generality, suppose $g_n = e^g$.
- Then

$$fe^g = c_n g' + h'$$

A Useful Corollary (cont.)

- Just as in Case 3 of the proof of Liouville's Theorem, $\deg(g_i') = \deg(g_i)$, and g_i does not divide g_i' unless $g_i = e^g$.
- Suppose $g_i \neq e^g$. Then there is nothing to cancel with $\frac{g_i'}{g_i}$ in the sum to acquire fe^g. So $\frac{g_i'}{g_i}$ must be 0, or otherwise we would have a leftover fraction in the sum and not fe^g.
- If $g_i = e^g$, then $\frac{g_i'}{g_i} = g'$. Without loss of generality, suppose $g_n = e^g$.
- Then
$$fe^g = c_n g' + h'$$
- Arguing as in Cases 2 and 3 of the proof of Liouville's Theorem, h must be a polynomial in e^g with coefficients from K.

A Useful Corollary (cont.)

- Moreover, $\deg(h) = \deg(h') = \deg(h' + c_n g') = \deg(fe^g) = 1$, and e^g divides $c_n g' + h'$.

A Useful Corollary (cont.)

- Moreover, $\deg(h) = \deg(h') = \deg(h' + c_n g') = \deg(fe^g) = 1$, and e^g divides $c_n g' + h'$.
- Therefore, $h = re^g - c_n g$ for some $r \in K$.

A Useful Corollary (cont.)

- Moreover, $\deg(h) = \deg(h') = \deg(h' + c_n g') = \deg(fe^g) = 1$, and e^g divides $c_n g' + h'$.
- Therefore, $h = re^g - c_n g$ for some $r \in K$.
- Therefore,

$$\begin{aligned} fe^g &= c_n g' + r'e^g + rg'e^g - c_n g' \\ &= r'e^g + rg'e^g \end{aligned}$$

A Useful Corollary (cont.)

- Moreover, $\deg(h) = \deg(h') = \deg(h' + c_n g') = \deg(fe^g) = 1$, and e^g divides $c_n g' + h'$.
- Therefore, $h = re^g - c_n g$ for some $r \in K$.
- Therefore,

$$\begin{aligned} fe^g &= c_n g' + r' e^g + rg' e^g - c_n g' \\ &= r' e^g + rg' e^g \end{aligned}$$

- Dividing through by e^g, we obtain

$$f = r' + rg'.$$

This completes the proof.

$\int e^{-x^2} dx$ is not elementary

- **Prop:** $\int e^{-x^2} dx$ is not solvable by elementary functions.

$\int e^{-x^2} dx$ is not elementary

- **Prop:** $\int e^{-x^2} dx$ is not solvable by elementary functions.
- **Proof:** Suppose $\int e^{-x^2} dx$ is elementary. Let $K = \mathbb{C}(x)$, $f = 1$, and $g = -x^2$ and apply the previous corollary. Thus, there exists $r \in \mathbb{C}(x)$ such that
$$1 = r' - 2xr.$$

$\int e^{-x^2} dx$ is not elementary

- **Prop:** $\int e^{-x^2} dx$ is not solvable by elementary functions.
- **Proof:** Suppose $\int e^{-x^2} dx$ is elementary. Let $K = \mathbb{C}(x)$, $f = 1$, and $g = -x^2$ and apply the previous corollary. Thus, there exists $r \in \mathbb{C}(x)$ such that
$$1 = r' - 2xr.$$
- Solving for r, we find that
$$r = e^{x^2} \int e^{-x^2} dx$$

$\int e^{-x^2} dx$ is not elementary

- **Prop:** $\int e^{-x^2} dx$ is not solvable by elementary functions.
- **Proof:** Suppose $\int e^{-x^2} dx$ is elementary. Let $K = \mathbb{C}(x)$, $f = 1$, and $g = -x^2$ and apply the previous corollary. Thus, there exists $r \in \mathbb{C}(x)$ such that
$$1 = r' - 2xr.$$
- Solving for r, we find that
$$r = e^{x^2} \int e^{-x^2} dx$$
- But $e^{x^2} \int e^{-x^2} dx$ is an entire function, so r must be a nonconstant polynomial.

$\int e^{-x^2} dx$ is not elementary

- **Prop:** $\int e^{-x^2} dx$ is not solvable by elementary functions.
- **Proof:** Suppose $\int e^{-x^2} dx$ is elementary. Let $K = \mathbb{C}(x)$, $f = 1$, and $g = -x^2$ and apply the previous corollary. Thus, there exists $r \in \mathbb{C}(x)$ such that
$$1 = r' - 2xr.$$
- Solving for r, we find that
$$r = e^{x^2} \int e^{-x^2} dx$$
- But $e^{x^2} \int e^{-x^2} dx$ is an entire function, so r must be a nonconstant polynomial.
- But $\deg(r') < \deg(2xr)$ and so $\deg(r' - 2xr) = \deg(2xr) > 1$.

$\int e^{-x^2} dx$ is not elementary

- **Prop:** $\int e^{-x^2} dx$ is not solvable by elementary functions.
- **Proof:** Suppose $\int e^{-x^2} dx$ is elementary. Let $K = \mathbb{C}(x)$, $f = 1$, and $g = -x^2$ and apply the previous corollary. Thus, there exists $r \in \mathbb{C}(x)$ such that
$$1 = r' - 2xr.$$
- Solving for r, we find that
$$r = e^{x^2} \int e^{-x^2} dx$$
- But $e^{x^2} \int e^{-x^2} dx$ is an entire function, so r must be a nonconstant polynomial.
- But $\deg(r') < \deg(2xr)$ and so $\deg(r' - 2xr) = \deg(2xr) > 1$.
- Therefore, $r' - 2xr \neq 1$, which is a contradiction.

But wait, there's more...

- Using that same corollary, we can show that

$$\mathrm{Ei}(x) = \int \frac{e^x}{x} dx$$

is not elementary.

But wait, there's more...

- Using that same corollary, we can show that

$$\mathrm{Ei}(x) = \int \frac{e^x}{x}\,dx$$

  is not elementary.
- This immediately gives us that three other important antiderivatives are not elementary:

$$\mathrm{Li}(x) = \int \frac{1}{\ln x}\,dx,$$

$$\mathrm{Si}(x) = \int \frac{\sin x}{x}\,dx,$$

$$\mathrm{Ci}(x) = \int \frac{\cos x}{x}\,dx.$$

But wait, there's more...

- Using that same corollary, we can show that

$$\mathrm{Ei}(x) = \int \frac{e^x}{x}\,dx$$

  is not elementary.

- This immediately gives us that three other important antiderivatives are not elementary:

$$\mathrm{Li}(x) = \int \frac{1}{\ln x}\,dx,$$

$$\mathrm{Si}(x) = \int \frac{\sin x}{x}\,dx,$$

$$\mathrm{Ci}(x) = \int \frac{\cos x}{x}\,dx.$$

- The details are left to the audience.

References

[1] Marius van der Put and Michael F. Singer, *Galois Theory of Linear Differential Equations*, Springer-Verlag, Berlin Heidelberg New York, 2003.

[2] R.C. Churchill, *Liouville's Theorem on Integration in Terms of Elementary Functions* (September 2006). http://www.sci.ccny.cuny.edu/∼ksda/PostedPapers/liouv06.pdf.

[3] Matthew P. Wiener, *Functions without elementary antiderivatives*, University of Pennsylvania, November 30, 1997.
http://www.math.niu.edu/∼rusin/known-math/97/nonelem_integr2.

[4] Andy R. Magid, *Differential Galois Theory*, Notices of the AMS **46** (October 1999), no. 9, 1041-1049.

[5] Moshe Kamensky, *Differential Galois Theory*.
http://www.nd.edu/ mkamensk/lectures/diffgalois.pdf.

[6] T. Dyckerhoff, *Tutorial on Differential Galois Theory I*, University of Pennsylvania.
http://www.math.upenn.edu/ tdyckerh/lecture1.pdf.