Notes for MA591U, Spring 2001
(Symbolic Computation)

Differential Galois Theory

Let $y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_0 y = f$ where $a_i, f \in k$, a differential field whose constants are algebraically closed. We want to extend the notion of a splitting field, the Galois group, and solvability to these types of equations.

EXAMPLES: Problems where $k = \mathbb{C}(x)$ with $' : k \to k$ such that $(a+b)' = a' + b'$ and $(ab)' = a'b + ab'$.

We will consider the equation

$$0 = L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_0 y,\ a_i \in k.$$

We want

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}' = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-1} \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

and

$$y \mapsto \begin{pmatrix} y \\ y' \\ \vdots \\ y^{(n-1)} \end{pmatrix} = Y.$$

We have $L(y) = 0$ if, and only if, $Y' = AY$, where A is the square matrix above.

FACT: Even the most general system $Y' = AY$ are equivalent, in a certain sense, to $L(y) = 0$.

LEMMA: Let K be a differential field with constants C. Let $A \in M_n(K) \doteq K^{n\times n}$. Let $V = \{y \in K^n | y' = Ay\}$. Then $\dim_C V \leq n$.

PROOF:

Note that any $(n+1)$ vectors of K^n are linearly dependent over K. It suffices to show that if $y_1, \ldots, y_n \in V$ are linearly dependent over K, then they are linearly dependent over C. Let

$$\sum_{i=1}^{t} f_i y_i = 0.$$

Assume (1) $f_1 = 1$ (just divide through if not) and (2) t is the smallest positive integer such that the above equation holds. Apply $y \mapsto y' - Ay$. Then we have

$$\begin{aligned} 0 = \sum_i \left(f_i' y_i + f_i y_i'\right) - \left(\sum_i f_i y_i\right) A &= \sum_i f_i' y_i + \sum_i f_i \left(y_i' - A y_i\right) \\ &= \sum_i f_i' y_i. \end{aligned}$$

But $f_1' = 0$, so by minimality of t it must be that $f_2' = \cdots = f_t' = 0$, which implies that $f_i \in C$. Hence $\{y_i\}$ is dependent over C.

NOTE: This is comparable to saying that a polynomial has at most n roots.

The analog to a *splitting field* in Differential Galois Theory is a *Picard-Vessiot Extension*, which we define as follows:

DEFINITION: Suppose $L(y) = 0$, with coefficients in k, and there exists a differential field K such that

(i) constants of K are the same as the constants of k;
(ii) K contains $y_1, \ldots, y_n$ linearly independent solutions of $L(y_i) = 0$;
(iii) K is the smallest differential field containing k and $y_1, \ldots, y_n$.

Then K is a *Picard-Vessiot Extension* (PVE) and

$$K = k(y_1, y_1', \ldots, y_1^{(n-1)}, \ldots, y_n, y_n', \ldots, y_n^{(n-1)}).$$

Note that $y_i^{(n)} = \sum_{i=0}^{n-1} a_i y^{(i)}$ (where $y^{(0)} = y$).

EXAMPLE: Let $k = \mathbb{C}(x)$ and $L(y) = 0$. Let $x_0 \in \mathbb{C}$ where no denominator of $L(y)$ vanishes. Then there exist $y_1, \ldots, y_n$ linearly independent over $\mathbb{C}$, and differentiable in a neighborhood of x_0 such that $L(y_i) = 0$. (This is the *Analytic Existence Theorem*.)

In general, we can show that this extension exists, but we are not presently able to construct it.

We can now define the Galois Group of an LDE. Let K be a PVE for $L(y) = 0$. We write

$$\mathrm{Gal}\left({}^{\mathrm{K}}/_{\mathrm{k}}\right) \doteq \left\{\sigma : \mathrm{K} \to \mathrm{K} | \sigma \text{ is an automorphism, } \sigma(\mathrm{z}') = (\sigma(\mathrm{z}))', \ \sigma|_{\mathrm{k}} = \iota\right\}.$$

Let $V = \{y \in K | L(y) = 0\}$. Observe that V is a vector space over C. If $y \in V$ and $\sigma \in \mathrm{Gal}\left({}^{\mathrm{K}}/_{\mathrm{k}}\right)$, then $\sigma(0) = \sigma(L(y)) = L(\sigma(y))$, so $\sigma(y) \in V$ as well.

Furthermore, $\sigma|_V$ is C-linear, so σ restricts to a linear transformation on V. Select a basis $y_1 \ldots, y_n$. Then we can take $\sigma \mapsto (c_{ij}) \in C^{n \times n}$. Hence $\mathrm{Gal}\left({}^{\mathrm{K}}/_{\mathrm{k}}\right) < \mathrm{GL_n(C)}$ (the group of $n \times n$ invertible matrices over C).

DEFINITION: We say that $X \subset C^N$ is *Zariski closed* if it is the common zeroes of some polynomial over C in N variables.

EXAMPLES:
1. Let $N = 1$. Then $\{x|p_1(x) = \cdots = p_N(x) = 0\}$ is finite, or it is all of C.

Conversely, any finite set has $X = \{\alpha_1, \ldots, \alpha_N\} = \{x|(x - \alpha_1) \cdots (x - \alpha_N) = 0\}$. So Zariski closed sets in $C(x)$ are empty, finite, or all of C. Observe that $\mathbb{N} \subset C$ is *not* Zariski closed.
2. Let $N = 2$. The solution sets in this case are finite unions of curves $p(x, y) = 0$, finite sets of points, C, and $\emptyset$.

DEFINITION: A *linear algebraic group* is a Zariski closed subgroup of $\mathrm{GL_n(C)} \subset \mathrm{C^{n^2}}$; that is, it is a subgroup of $\mathrm{GL_n(C)}$ defined by the vanishing of a set of polynomials in the entries of the matrices. All previous examples are these kinds of groups.

An example of those that are not: let

$$\mathrm{GL_1(C)} = \{\mathrm{c}|\mathrm{c} \neq 0\} = \mathrm{C}\backslash\{0\} \doteq (\mathrm{C}^*, \cdot).$$

Zariski closed proper subgroups are finite and cyclic, hence of the form $\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{N}$. So consider $\left\{\left(\sqrt{2}\right)^n | n \in \mathbb{Z}\right\}$. This is not Zariski closed, since it is neither finite, nor is it $\mathrm{GL_1(C)}$.

BASIC FACT: $\mathrm{Gal}\left(\mathrm{K}/\mathrm{k}\right) < \mathrm{GL_n(C)}$ is Zariski closed.

EXAMPLE: Let $y' - ay = 0$ for some $a \in k$.

$\mathrm{Gal} \subseteq \mathrm{GL_1(C)} = \mathrm{C}^*$.

Either $\mathrm{Gal} = \mathrm{GL_1(C)}$ or Gal is finite.

The only finite subsgroups of C^* are the nth roots of unity for some $n \in \mathbb{N}$. So

$$\mathrm{Gal} = \begin{cases} \mathrm{GL_1} \\ \{\zeta : \zeta^n = 1\}\ \exists n \in \mathbb{N} \end{cases}.$$

GENERAL FACT: If $z \in K$ such that $\sigma(z) = z$ for all $\sigma \in K$, then $z \in k$.

To test whether $\mathrm{Gal} = \{\zeta : \zeta^{\mathrm{n}} = 1\}$ for some $n \in \mathbb{N}$, do the following.

Let $y \in K$ be a solution of $y' - ay = 0$. Consider y^n; if $\mathrm{Gal} = \{\zeta : \zeta^{\mathrm{n}} = 1\}$ then

$$\sigma(y^n) = (\sigma(y))^n = (\zeta y)^n = \zeta^n y^n = y^n$$

so $y^n \in k$.

Conversely, if n is the smallest nonzero integer so that $y^n = u \in k$, then $K = k(\sqrt[n]{u})$. So K is an algebraic extension of k. Then $\mathrm{Gal} = \{\zeta | \zeta^{\mathrm{n}} = 1\}$, since $y \mapsto \zeta y$ gives an automorphism.

Observe that $y' - ay = 0$ only if $y'/y = a$. If $y^m = u$,

$$\frac{u'}{u} = \frac{(y_m)'}{y_m} = \frac{my'}{y} = ma.$$

So to test for a Galois group, the group is finite if there is some m such that $u' - mau = 0$ has a rational solution. It equals $\{\zeta | \zeta^m = 1\}$ where m is the smallest such integer. It is, on the other hand, GL_1 if there is no such integer.

To do this, one can modify the algorithm we explored earlier to find rational solutions to LDEs.

EXAMPLE:

$$y' - \frac{1}{3x}y = 0$$

has $m = 3 \in \mathbb{Z}$ giving a rational solution to

$$y' - \frac{m}{3x}y = 0.$$

This is also the smallest such integer.

EXAMPLE: One can homogenize $y' = f$ (which has solution $y = \int f$) as $y'' - (f'/f)y' = 0$ (which has solutions $y \in \left\{\int f, 1\right\}$). Since the latter is homogeneous, the PVE is $K = k(1, \int f)$. Let $\sigma \in \mathrm{Gal}$. We know that $\sigma(1) = 1$ and $[\sigma(\int f)]' = \sigma((\int f)') = \sigma(f) = f$. So $\sigma(\int f)$ and $\int f$ differ by a constant. Hence $\sigma(\int f) = \int f + c_\sigma$ for some $c_\sigma \in C$. In the basis $\left\{1, \int f\right\}$ of the solution space,

$$\sigma = \left\{ \begin{array}{cc} 1 & c_\sigma \\ 0 & 1 \end{array} \right\}.$$

So

$$\mathrm{Gal} < \left\{ \left(\begin{array}{cc} 1 & c \\ 0 & 1 \end{array} \right) | \mathrm{c} \in \mathrm{C} \right\}.$$

Hence the only algebraic subgroups are $\{I\}$ and $\left\{ \left(\begin{array}{cc} 1 & c \\ 0 & 1 \end{array} \right) | c \in C \right\}$ itself. We have $\mathrm{Gal} = \{\mathrm{I}\}$ if, and only if, $\int f \in k$. We need to see if $y'' - (f'/f)y' = 0$ has a two-dimensional solution space in k. If $k = \mathbb{Q}(x)$, we can do this.

MAIN THEOREM OF GALOIS THEORY:

Let K be a PVE of k associated with $L(y) = 0$. There is a bijective correspondence between algebraic subgroups H of $\mathrm{Gal}\left({}^{\mathrm{K}}/_{\mathrm{k}}\right)$ and differential subfields $\mathbb{F}$, with $K \supset \mathbb{F} \supset k$:

$$\begin{array}{rcl} \{\text{algebraic subgroups}\} & \leftrightarrow & \{\text{subfields}\} \\ H & \leftrightarrow & K^H = \{y \in K | \sigma(y) = y \, \forall \sigma \in H\} \\ \mathrm{Gal}\left({}^{\mathrm{K}}/_{\mathbb{F}}\right) = \{\sigma | \sigma(\mathrm{y}) = \mathrm{y} \, \forall \mathrm{y} \in \mathbb{F}\} & \leftrightarrow & \mathbb{F} \end{array}$$

Furthermore, $H \lhd \mathrm{Gal}\left({}^{\mathrm{K}}/_{\mathrm{k}}\right)$ if, and only if, K^H is a PVE.

EXAMPLE: Again let $y' - ay = 0$ and assume $\mathrm{Gal} = \mathrm{GL}_1$. We have

$$\begin{array}{ccc} K = K(y) & \leftrightarrow & \{1\} \\ \cup & & \cap \\ k(y^m) & \leftrightarrow & \{\zeta | \zeta^m = 1\} \\ \cup & & \cap \\ k & \leftrightarrow & C^* \end{array}$$

where $(y^m)' - may^m = 0$.

We now turn to the issue of *solvability*.

DEFINITION: Let $F \supset k$ be differential fields. We call L a *Liouvillian Extension of* k if there is a tower

$$F = F_m \supset \cdots \supset F_0 = k$$

such that $F_i = F_{i-1}(t_i)$ where either t_i is algebraic over F_{i-1}, $t_i' \in F_{i-1}$ (which implies that $t_i = \int u_i$ for some $u_i \in F_{i-1}$), or $t_i'/t_i \in F_{i-1}$ (which implies that $t_i = e^{\int u_i}$ for some $u_i \in F_{i-1}$).

A differential equation is said to be Liouvillian if its PVE lies in a Liouvillian extension of k.

THEOREM: Suppose K is the PVE of k corresponding to $L(y) = 0$. Let $G = \mathrm{Gal}\left({}^{\mathrm{K}}/_{\mathrm{k}}\right)$. It turns out that $L(y) = 0$ is Liouvillian if, and only if, there is some normal subgroup H of G with $[G : H] < \infty$, and H solvable.

For $k = \overline{\mathbb{Q}}(x)$, this is decidable! For $n = 2$, Kovacic determined this in 1978. For $n \geq 2$, Singer published a result in the American Journal of Mathematics, in 1980.

REFERENCES:

"Direct and Inverse Problems in Differential Galois Theory"; see Singer's homepage (currently `www.math.ncsu.edu/~singer`).

"Symbolic Analysis of D.E." in *Some Tapas of Computer Algbebra* by Cohen, Cuypers, and Steck (editors), published by Springer-Verlag.