

Math 250a: Higher Algebra
Differential algebra and differential Galois theory

Differential algebra. Differential Galois theory is an analogue of classical Galois theory that describes the structure of certain differential equations. Just as Galois theory presumes algebra, we need to say a bit about differential algebra before we can do differential Galois theory.

A *differential field* (k, ∂) is a field k of characteristic zero together with a derivation

$\partial : k \rightarrow k$ satisfying the Leibniz rule $\partial(xy) = y'\partial x + x\partial y$ and $\partial 1 = 0$.

The kernel k_0 of ∂ is a field, called the “constants” of (k, ∂) , and ∂ is k_0 -linear. The trivial example of a differential field is $k_0, \partial = 0$. The canonical example is $k_0(t)$ with the usual definition for ∂ , and by $\partial t = 1$. Further examples are obtained from algebraic extensions of a differential field (k, ∂) , to which ∂ extends uniquely (by “implicit differentiation”). One can also specify transcendental extensions of (k, ∂) by adjoining a solution of a differential equation. Prototypical examples are the extension of $\mathbf{C}(t)$ by e^t and $\log t$. Other examples are solutions of the differential equations $y' = y$ and $y' = 1/t$. Further examples are obtained by adjoining a solution of one of the differential equations

$$y' = ay, \quad y' = b, \quad y'' + y/t + y = 0$$

(where $a, b \in k$). The first two of these can be “solved by quadratures”: $y = \exp \int a$, $y = bt$. The last is the differential equation for the Bessel function

$$J_0(t) = \sum_{k=0}^{\infty} \frac{(-1)^k (t/2)^{2k}}{k!^2}.$$

One consequence of differential Galois (Gal_{∂}) theory is that this equation cannot be solved by quadratures.

The algebra of linear differential operators. Gal_{∂} theory is specifically concerned with “homogeneous linear ODE’s”, that is, differential equations of the form

$$0 = Ty = \sum_{i=0}^n a_i \partial^{n-i} y.$$

We may assume that $a_0 \neq 0$, and then scale to obtain an equivalent “monic” T , one with $a_0 = 1$. The solutions of this equation constitute the kernel of the “ n -th order differential operator” T on k . Many other differential equations that are not of this form can be converted into or subsumed under linear ones. For instance, the differential

equation for $\log t$ is not of this form, but $\log t$, and more generally $\int b$ for $b \in k^*$, is in the kernel of the second-order differential operator $(\partial - (b'/b))\partial = \partial^2 - (b'/b)\partial$.

Now recall some basic facts about ordinary polynomial algebra: given an n -element subset S of a field k , we may form a unique monic polynomial P_S of degree n vanishing on S , namely $P_S(x) = \prod_{y \in S} (x - y)$. Moreover, if S, S' are finite subsets of k then $S \subseteq S'$ if and only if $P_S | P_{S'}$. There is a similar construction in differential algebra. Let $V \subset k$ be a vector space of dimension n over k_0 . Then there is a unique monic differential operator T_V of order n vanishing on V . Moreover, if V, V' are finite-dimensional subspaces of k then $V \subseteq V'$ if and only if $T_{V'}$ factors as $T \circ T_V$ for some other monic operator T .

We may construct T_V using the *Wronskian determinant*. For each m we have an alternating k_0 -multilinear map $W_m : k^m \rightarrow k$ defined by

$$W_m(y_1, \dots, y_m) := \det(\partial^{i-1} y_j)_{i,j=1}^m.$$

Its key property is that $W_m(y_1, \dots, y_m) = 0$ if and only if y_1, \dots, y_m are linear dependent over k_0 . If y_1, \dots, y_n is any basis for V then

$$T_V(x) = \frac{W_{n+1}(x, y_1, \dots, y_n)}{W_n(y_1, \dots, y_n)}.$$

This is independent of the choice of basis: a different choice only multiplies both numerator and denominator by the determinant. If $n = 1$ then the denominator is just a generator for V , and thus satisfies $y' = a_1 y$. More generally, for any $n > 0$ it is well-known that the Wronskian of any basis for V is a nonzero solution of the first-order ODE $y' = a_1 y$.

The Wronskian determinant should remind you of the van der Monde determinant

$$V_m(y_1, \dots, y_m) := \det(y_j^{i-1})_{i,j=1}^m = \prod_{1 \leq j < j' \leq m} (y_j - y_{j'}),$$

which vanishes if and only if the y_j are distinct. Indeed we could use V_m to define P_S as

$$P_S(x) = \frac{V_{n+1}(x, y_1, \dots, y_n)}{V_n(y_1, \dots, y_n)}$$

where y_1, \dots, y_n is any enumeration of S .

Digression: the formal adjoint. The key difference between polynomial and differential algebra is that compositions of linear operators, unlike polynomial products, do not commute in general. The k_0 -algebra of differential operators on k is generated by k and ∂ , with the commutation relation $\partial b = b\partial + b'$. This algebra does, however, have an anti-involution, the *formal adjoint*. This a k_0 -linear map satisfying the

identity $(T_1 \circ T_2)^* = T_2^* T_1^*$ for any differential operators T_1, T_2 , and determined by that

identity together with $a^* = a$ ($a \in k$) and $\partial^* = -\partial$. Classically (Lagrange?) this adjoint arose via the identity

$$xT^*y - yTx = -\partial\langle x, y \rangle_T$$

where $\langle x, y \rangle_T$ is the “bilinear concomitant” associated to T ; for instance, $\langle x, y \rangle_\partial = xy$. It can be shown that $T_V^* = T_{V^*}$ where V^* is the n -dimensional space consisting of $W_{n-1}(y_1, \dots, y_{n-1})/W$ for any $y_j \in V$, where W is the Wronskian of an arbitrary basis for V . As suggested by the notation, V, V^* are canonically dual; indeed $\langle \cdot, \cdot \rangle_T$ gives the perfect pairing!

Picard-Vessiot extensions. We are now ready to describe Gal_∂ theory. Recall that in the classical Galois theory, we associate to a separable monic polynomial $P \in k[X]$ a splitting field K , which is the minimal field in which $P = P_S$ for some $S \subseteq K$. We then define the Galois group $\text{Gal}(K/k) = \text{Aut}_k K$, and show that this is a finite group of order $[K : k] = \dim_k K$, and that k is the subfield of K fixed by the action of $\text{Gal}(K/k)$. Moreover, intermediate field extensions F correspond bijectively with subgroups $\text{Gal}(K/F)$ of $\text{Gal}(K/k)$; such an extension is itself Galois over k if and only if $\text{Gal}(K/F)$ is normal in $\text{Gal}(K/k)$, in which case the quotient group is canonically identified with $\text{Gal}(F/k)$; and a polynomial is solvable by radicals if and only if its splitting field has a solvable Galois group. These results all have differential analogues.

A “differential splitting field” of a monic differential operator T on (k, ∂) is a differential extension K of k generated as a differential field by k and a finite-dimensional k_0 -subspace $V \subset K$ such that $T = T_V$. Such K/k is said to be a Picard-Vessiot extension of (k, ∂) . It contains a differential splitting field for any monic differential operator over k whose kernel in K is nonempty. Its *differential Galois group* $\text{Gal}_\partial(K/k)$ is the group of differential automorphisms of K that fix k . This is an algebraic subgroup of $\text{GL}(V)$. For example, $\text{Gal}_\partial((\mathbf{C}(t))(e^t)/\mathbf{C}(t))$ is the multiplicative group \mathbf{G}_m ; more generally, if k_0 is algebraically closed then the Gal_∂ group of any first-order operator $\partial - a$ is \mathbf{G}_m unless $a = y'/ny$ for some $y \in k^*$ and $n \in \mathbf{Z}$, in which case the Gal_∂ group is the μ_n for the minimal n . Also, $\text{Gal}_\partial((\mathbf{C}(t))(\log t)/\mathbf{C}(t)) = \mathbf{G}_a$; this is the Gal_∂ group of any operator $\partial^2 - (b'/b)\partial$, unless $b \in \partial k$ in which case the Gal_∂ group is trivial. The Gal_∂ of the Bessel differential operator is necessarily contained in $\text{SL}_2(\mathbf{C})$; it can be shown by monodromy considerations that it actually equals $\text{SL}_2(\mathbf{C})$.

In general, the dimension of $\text{Gal}_\partial(K/k)$ the *transcendence degree* of K over k , that is, the size of a maximal subset of K that is algebraically independent over k . As in the classical case, k is the subfield fixed by $\text{Gal}_\partial(K/k)$; intermediate differential extensions correspond bijectively to algebraic subgroups of $\text{Gal}_\partial(K/k)$; and such an extension F is itself Picard-Vessiot if and only if $\text{Gal}_\partial(K/F)$ is normal in $\text{Gal}_\partial(K/k)$, in which case $\text{Gal}_\partial(F/k) = \text{Gal}_\partial(K/k)/\text{Gal}_\partial(K/F)$.

What of solvability? There is indeed a characterization of Picard-Vessiot extensions with solvable Gal_∂ groups: they are precisely the ones that can be obtained by repeated

quadratures! So for instance J_0 cannot be reduced to indefinite integrals because its Gal_∂ group SL_2 is not solvable.

Further examples and connections. A monic operator and its formal adjoint generate isomorphic Picard-Vessiot extensions; their kernels are contragredient representations of the same Gal_∂ group.

If a monic operator is self-adjoint or anti-self-adjoint, its kernel has a canonical nondegenerate pairing, which the differential Galois group must respect. Necessarily if $T^* = T$ then n is even, and if $T^* = -T$ then n is odd. By writing down the bilinear concomitant, one may check that the pairing is alternating in the former case, symmetric in the latter. It is a classical fact if T is any second-order differential operator then one can find (by integrating a first-order ODE) some a such that $a^{-1}Ta$ is self-adjoint; this is “explained” by $\text{Sp}_2 = \text{SL}_2$. Further example: the general anti-self-adjoint monic differential operator of order 3 is $\partial^3 + 2a\partial + a'$; its kernel consists of the homogeneous quadratic polynomials in the kernel of $\partial^2 + a/2$.

The inverse Gal_∂ problem for connected linear subgroups of GL_n is easier than the Noether problem, but not trivial, especially if we want explicit formulas. Example: if $T = \partial^7 + \sum_{i=0}^5 c_m \partial^m = -T^*$ and $a_3 = (a_5/2)^2 + 3a_5''$ then Gal_∂ is generically G_2 ! [NDE 1996; Katz obtained the family $\partial^7 + 2c\partial + c'$, which is the special case $a_3 = a_5 = 0$.]

Other connections: close analogies with p -polynomials; Drinfeld-Beilinson “Opers”; D-modules; monodromy of exponential sums [the Katz connection].