MODEL THEORY AND DIFFERENTIAL GALOIS THEORY, AN INTRODUCTION

JAVIER MORENO

Abstract. Model theory and differential Galois theory have had a long history of interactions. In this talk we will introduce the basic notions of differential Galois theory and some of the classic model theoretic tools that allows us to use logic to explore differential equations by algebraic means. If time permits, we will briefly discuss some recent applications of model theory that generalise classic results in differential Galois theory to different settings.

Contents

1. Differential algebra: basic definitions

> "The study of polynomial equations leads naturally to the notions of rings and fields. For studying differential equations, the natural analogs are differential rings and fields."
> —van der Put and Singer

Definition 1.1. Let R be an arbitrary (commutative) ring. A **derivation** on R is an additive function $\partial\colon R \to R$ such that $\partial(xy) = x\partial(y) + y\partial(x)$ for any $x, y \in R$. A ring (field) R equipped with a derivation ∂ is what we call a **differential ring (field)**. By **the constants of** R, denoted C_R, we

---

Date: Logic Seminar. University of Waterloo. January 13, 2010.

mean the set of elements in R where ∂ vanish. (If $R = F$, a field, C_F is also a field (Exercise.))

Example 1.2. Some examples of differential fields:

- $C(z)$ with the derivation with respect to z.
- $C((z))$ (formal Laurent series). Same derivation.
- The field of all meromorphic functions on any open connected subset of the complex plane with the natural derivation.

Remark 1.3. Differential algebra studies differential rings and fields from an algebraic perspective. Notions of ideals (prime, maximal), localizations, &c. can be defined and developed. Geometrically, Buium et al. have explored the (algebraic-geometric) notion of a differential scheme. (Recall that differential rings also appear naturally in commutative algebra, e.g. structure theorem for complete local rings (see Matsumura.))

2. Differential Galois theory

2.1. **Motivation.** The goal of Differential Galois Theory is to study differential equations by algebraic means (this is, using the differential algebraic setting we just introduced). We would like to have methods to evaluate if the integral of a given function (or the solution of a differential equation) could be expressed in terms of "elementary functions".

Let's us recall very fast the way (algebraic) Galois theory works. The idea is to associate to a polynomial a group and extract properties about the solution of the polynomial from the structural properties of the group.

Let F a field and let $P(X) \in F[X]$ a polynomial of degree n with no repeated roots. The way we obtain the group goes as follows.

1. Let
$$S = F[X_1, \dots, X_n, \frac{1}{\prod_{i \neq j}(X_i - X_j)}],$$
and let I be the ideal generated by the $P(X_i)$ in S. Let $M > I$ maximal in S.
2. Define the splitting field of P over F as $K = S/M$. And let $G = \mathrm{Aut}(K/F)$.
3. Since S contains $\prod_{i \neq j}(X_i - X_j)$ then the images of X_i in K are distinct roots of P.
4. K is unique up to isomorphism and we have Galois correspondence: to every subgroup of G corresponds an intermediate extension between F and K, etc.
5. This allows us to prove, for instance, that a polynomial P is solvable by radicals if G is a solvable group (i.e. there exists a sequence of

subgroups $1 < G_1 < G_2 \cdots < G_l = G$ such that G_i is normal in G_{i+1} and G_{i+1}/G_i is abelian.)

2.2. **Picard-Vessiot theory.** Let $y' = Ay$ be a linear differential equation of order n $(= \dim(A))$ with coefficients in F, a differential field with C_F algebraically closed. The set V of solutions of this equation in $L > F$ an extension of F is a C_F-vector space of dimension at most n (Exercise). We would like to obtain a corresponding splitting field for this equation (with solution space of full dimension). We proceed as follows:

1. Let
$$S = F[Y_{1,1}, \ldots, Y_{n,n}, \frac{1}{det(Y)}]$$
and define a derivation on S setting $Y' = AY$. Let M be a maximal differential ideal of S.
2. Define the Picard-Vessiot ring of the given equation with respect to F as $R = S/M$. In this case R is not necessarily a field, but it can be proven that it is an integral domain (Exercise). Let $K = Q(R)$. Let $G = \mathrm{Aut}_\partial(K/F)$.
3. From the fact that C_F is algebraically closed we can prove that:
   - (a) P-V ring extensions are unique up to isomorphism.
   - (b) $C_R = C_F$.
   - (c) $K = F(Z)$ for some (fundamental) solution matrix Z and $C_K = C_F$.
4. (New element:) Note that G can be seen as a subgroup of $GL_n(C_F)$: Fix $Z \in GL_n(K)$ a (fundamental) solution matrix (we built K to be able to have that). Let $\sigma \in G$. Consider $\sigma(Z)$; this is again a fundamental solution matrix and it can be proven that $(Z^{-1}\sigma(Z))' = 0$. Thus, $\sigma(Z) = ZM_\sigma$, with $M_\sigma \in GL_n(C_F)$. The injection goes $\sigma \mapsto M_\sigma$. If we take another Z, the corresponding injection is a conjugate.
5. Moreover, $G \subset GL_n(C_F)$ is a linear algebraic group (i.e. a zero set in $GL_n(C_F)$ of a system of polynomials over C_F in n^2 variables)!!! (Exercise)
6. Galois Correspondence (the algebraic structure matters!): There is a correspondence b/w Zariski-closed subgroups $H \subset G$ and intermediate differential subfields b/w F and K.
7. This allows us to prove statements as: If G is solvable then the corresponding equation can be solved by a finite sequence of field extensions $F = F_0 < F_1 \cdots < F_l = K$ such that $F_{i+1} = F_i(t_i)$ where either (i) $t_i' \in F_i$ (integral) or (ii) $t_i'/t_i \in K_i$ (exponencial).

Summarizing: Given F a differential field with C_F algebraically closed and $Y' = AY$, a linear differential equation of order n over F, a P-V extension of F is a differential field K such that:

1. There is $Z \in GL_n$, a fundamental matrix of solutions of the equation such that $K = F(Z)$, and,
2. $C_K = C_F$.

2.3. **Kolchin's (non-linear) differential Galois theory.** Kolchin tried to generalise the P-V extensions a little bit more. For this he forgot about the equation and defined the following:

Definition 2.1. Let F be a differential field with C_F algebraically closed. An strongly normal extension of F is a differential field $K > F$ such that:

1. $K = F(a)$ for some finite $a \in K$,
2. $C_K = C_F$, and,
3. For any $U > F$ and $\sigma \colon K \to U$ over F injective, $\sigma(K) \subseteq K\langle C_U \rangle$.

From this definition, Kolchin managed to prove the following:

Theorem 2.2. *Let K/F an strongly normal extension of differential fields, then:*

1. *$Gal(K/F) = Aut_\partial(K/F)$ is isomorphic to the C_F rational points of an algebraic group over C_F.*
2. *Galois correspondence, etc.*

Remark 2.3. An algebraic condition in F allows us to bring out equations out of this apparently equation-less context. There is also a geometric presentation of this theory, using so-called logarithmic differential equations on algebraic groups.

3. Internality and definable automorphism groups

3.1. **Internality: definition and one consequence.** Question: How is model theory involved in this subject?

Answer: Think Definable Automorphism Groups.

More specifically: Hrushovksi and Zilber isolated conditions to guarantee that certain automorphism groups were definable (which, in essence, makes them visible to model theory).

Here is the key definition:

Definition 3.1. Let T a stable theory. Consider p and q possibly partial types over A. We say that p is **q-internal (over A)** (or **internal to q**) if there is a set B containing A such that, for every realization a of p, there is a tuple b of realizations of q such that $a \in \mathrm{dcl}(Bb)$.

Definition 3.2. Given p q-internal, we say that a tuple a of realizations of p is a **fundamental system of solutions of p relative to q** if there exists $u(\cdot,\cdot)$, an A-definable function, such that for any b realizing p, we have that $b = u(a, c)$ for some tuple c of realisations of q.

Theorem 3.3. *Let T be a stable theory and $\mathcal{U}$ a big saturated model. Suppose that p and q are over A and p is q-internal. Suppose also that there is a fundamental system of solutions of p relative to q. Then the group of automorphisms of $\mathcal{U}$ that fixes $q(\mathcal{U})$ and A pointwise induces a type-definable group of automorphisms on $p(\mathcal{U})$*

Remark 3.4. Two comments:

1. General conditions for the existence of f.s.s.? (1) q is a formula; (2) p is stationary; or, more generally (3) p has finite multiplicity.
2. Stability is not really necessary: Hrushovski (2001) managed to prove these results in a way more general context.

3.2. **An example: Strongly Normal Theory.** What does model theory tell us about differential fields?

- (Robinson, 1950's!) There is a model companion of the theory of differential fields (ch. 0): Differential Closed Fields.
- DCF_0 is stable (it is actually ω-stable (Blum)). It has elimination of imaginaries and QE (??). Also, $\mathrm{dcl}(A) = \langle A \rangle$.
- Additionally, the constants are pure: Let $\mathcal{C} = C_{\mathcal{U}}$. If $Z \subset \mathcal{U}^m$ is definable in $\mathcal{U}^m$ over A, then $Z \cap \mathcal{C}^m$ is definable in $(\mathcal{C}, +, \cdot\ )$ over $\mathrm{dcl}(A) \cap \mathcal{C}$ (A consecuence of stability, if you like).

Remark 3.5. Observe the following:

1. Condition (3) in the definition of s.n.e. basically says: $p = tp(a/F)$ is C-internal in a very special way: for every $b \models p$, we have that $b \in dcl(aFC_{\mathcal{U}})$.
2. C is a formula, thus there is a fundamental system of solutions (actually a, in this case!!).

Proof of theorem 2.2(1). Let's see how internality works:

1. Let $u(\cdot,\cdot)$ a definable function over F such that for every $b \models p$ there is $c \in \mathcal{C}$ such that $b = u(a, c)$.
2. Let $Y = Z/E$ where $Z = \{c \in \mathcal{C} : u(a, c) \in p(\mathcal{U})\}$ and E is an equivalence relation on Z defined by the formula $u(a, x_1) = u(a, x_2)$. Because of elimination of imaginaries of the theory of algebraically closed fields and the pureness of $\mathcal{C}$, Y is a type-definable set in $\mathcal{C}$ over $\mathrm{dcl}(a) \cap \mathcal{C} \subset C_F$.

(3) For $b \in \mathcal{X}$ and $d \in Y$, define $f(b,d) = u(b,c)$ with $c \in Z$ such that $c/E = d$, and note that for any b_1 and $b_2 \in \mathcal{X}$, there is a unique $d \in Y$ such that $f(b_1,d) = b_2$. Let $h\colon\ : \mathcal{X} \times \mathcal{X} \to Y$ a definable function that witnesses this uniqueness.

(4) Consider the function $\mu\colon \mathrm{Gal}(K/F) \to Y\colon \sigma \mapsto h(a,\sigma(a))$. Key point: μ is a bijection. Now endow Y with the group operation induced by μ. That is, let us define $d \cdot d' = \mu(\mu^{-1}(d) \cdot \mu^{-1}(d'))$. Note that this group operation is definable (Exercise).

(5) Finally, the fact that $\mathcal{C}$ is totally transcendental gives us that $(Y,\cdot)$ is actually definable. But wasn't it an algebraic group!? Well, the Weil-Van den Dries-Hrushovski theorem (motivated precisely by this question) tells us that $(Y,\cdot)$ is definably isomorphic to the set of $\mathcal{C}$-rational points of an algebraic group G defined over C_F. Identify $G(\mathcal{C})$ and Y.

□

4. Applications

(1) Generalised strongly normal theory: What if we substitute the constants by an arbitrary formula? (Explored by Pillay, Marker, Süer, etc.) The Galois group is finite-dimensional definable.

(2) Difference Galois theory: Automorphisms instead of derivatives? (Kameski ("partial automorphism" (preserving an almost arbitrary set of formulas), Singer, Chatzidakis, etc.)

(3) Positive characteristic: An analog for positive characteristic? Iterative derivations! (Okugawa, van der Put, Matzat, M.) Beyond: "Generalised" version.

(4) Difference-differential Galois theory (?) (Singer has possed the problem. In model theory we have the work of Bustamante, who has explored the theory of differentially closed fields with a generic automorphism. In positive characteristic, separably closed fields with a generic automorphism: Delon, Chatzidakis...)

Institut Camille Jordan, Université Claude Bernard Lyon 1, 43 boulevard du 11 novembre 1918, 69622 Villeurbanne Cedex, France
E-mail address: `moreno@math.univ-lyon1.fr`
URL: `http://math.univ-lyon1.fr/~moreno/`