

DEFINABLE GROUPS OF AUTOMORPHISMS

MOSHE KAMENSKY

1. MOTIVATION

1.1. Differential Galois theory. A linear differential equation over a differential field K is an equation of the form $D\bar{x} = A\bar{x}$, where A is a matrix over K . The set $Q(L)$ of solutions in a differential field extension L of K is a vector space over the field $C(L)$ of constants of L , of dimension at most n , the length of x .

20 minutes
4 minutes

A *Picard-Vessiot extension* of K (for the given equation) is a differential field extension L with $C(L) = C(K)$, $Q(L)$ of dimension n over $C(L)$, and which is minimal with these properties. This extension plays the same role as Galois extensions in usual Galois theory. When $C(K)$ is algebraically closed, there exists a unique (up to isomorphism) Picard-Vessiot extension for any linear equation. In this case the *Galois group* G of Q is defined to be $Aut_D(L/K)$ (differential field automorphisms.) It turns out that G can be identified with the $C(L)$ points of an algebraic group over $C(L)$.

7 minutes

1.2. A model theoretic point of view. We view the situation within the theory DCF_K of differentially closed fields with parameters for K . The differential equation Q and the field of constants C are definable sets in this theory. Q has the structure of a definable vector space over C . The axioms of DCF imply that C is algebraically closed, and that Q has dimension n over C .

For definable sets Q and C in an arbitrary theory, Q is *internal* to C if there is a finite tuple b such that any element of Q is definable over b and C . The typical example is: C a definable field, Q a definable vector space over C of finite dimension, and b any basis for Q over C . This applies in particular to linear differential equations.

Given a saturated model M of T , and two definable sets Q and C , we may define the automorphism group $Aut(Q(M)/C(M))$ as $Aut(M/C(M))/Aut(M/Q(M))$. In the case that Q is internal to C , this turns out to be the group of M -points of a type-definable group G (Zil'ber, Poizat, Hrushovski,...) G itself is then internal to C .

In DCF , G is actually definable, since DCF is ω -stable. Over parameters we get a group inside C , which is a pure ACF . Any such group is algebraic. If N is a prime model of DCF_K , then $C(N) = C(K)^a$, and the Picard-Vessiot extension for Q is the subfield of N generated by a basis of solutions. By quantifier elimination, the group $G(N)$ is the group of automorphisms preserving the algebraic structure, hence is identified with the differential Galois group.

8 minutes

1.3. Difference equations. A *linear difference equation* over a difference field K is an equation of the form $\sigma(x) = Ax$. The fixed field plays the role of C , the field of constants. The Galois theory of difference equations is parallel to that of differential equations, with the following difference: The Picard-Vessiot extension

is not, in general, a field, but a ring, possibly with zero-divisors. For example, if $C(K)$ is algebraically closed, the equation $\sigma(x) = -x$ does not have a solution in any field extension of K that does not extend the fixed field.

On the model theoretic side, the corresponding theory is *ACFA*. The equation Q is again internal to the fixed field C . However, in pursuing the above analogy, we run into the following problems:

- (1) *ACFA* does not eliminate quantifiers, so the model theoretic automorphism group does not coincide with the algebraic one.
- (2) *ACFA* is not ω -stable and so the group need not be definable (in fact, it is not even stable, so it is not even automatically an intersection of definable groups.)
- (3) The fixed field C is not algebraically closed, so the group, even if definable, need not be algebraic.
- (4) The Picard-Vessiot extension may have zero divisors, so may not be embeddable in a model of *ACFA*.

The solution is to study the definable automorphisms group more closely. On the way to resolving the above obstacles, we:

- (1) define a group of “partial automorphism” preserving an (almost) arbitrary set of formulas.
- (2) show that this group is always an intersection of definable groups, and give explicit formulas for these groups
- (3) interpret $G(M)$ for any model (not necessarily saturated.)

2. GROUPS OF PARTIAL AUTOMORPHISMS

We consider an arbitrary theory T with definable sets $Q = X_0$ and C as before, as well as additional definable sets X_i . We consider a collection Δ of definable subsets of products of the X_i , and C . If M is any model of T , a Δ -*automorphism* of $X_i(M)$ over $C(M)$ is a bijection $\phi_i : X_i(M) \rightarrow X_i(M)$ for each i , which preserve all the formulas in Δ . We let $Aut_\Delta(X_i/C)(M)$ be the group of all such automorphisms.

If Q is internal to C , then, by definition, there is a b -definable function g_b from some subset of C onto Q . Let X be a definable set where b lies, such that g_x is a function onto Q , and such that $g_x \neq g_y$ for $x \neq y$. We call this function an *internality datum*.

We now have the following result: Let X_i , C and Δ be as before. Assume that the X_i are internal to C , and that Δ contains the internality data. Then there is a collection G_j of definable groups and group actions on the X_i that identify the intersection of the G_j with $Aut_\Delta(X_i/C)$. The groups and group actions are described explicitly in term of Δ .

2.1. Construction of G_0 . We start with the following remark: The classical definition of internality says that Q is internal to C is there is an x -definable surjective function $g_x : C_x \rightarrow Q$ for some x -definable $C_x \subseteq C^n$. It follows that there is a definable set X , a definable set D in C^{eq} , a definable map $\pi : X \rightarrow D$, a definable subset \tilde{C} of $C^n \times D$, and a definable map $g : \tilde{C} \times_D X \rightarrow Q$ such that $g_x : \tilde{C}_{\pi(x)} \rightarrow Q$ is surjective, and all g_x are distinct. Furthermore, since we are considering automorphisms fixing C , we may divide by the kernel (family) of g and get g_x to be injective. In this form, we may equivalently describe the internality datum as a function $f : Q \times X \rightarrow C$ over maps $\pi_X : X \rightarrow D$ and $\pi_C : C \rightarrow D$, where D is

in C^{eq} , such that the induced map $(f, p_2) : Q \times X \rightarrow C \times_D X$ is a bijection. The function g is then the inverse of this map, followed by the projection on Q . We assume from now on that the internality is given in this form. We note that D can be viewed as the set types of elements in X with respect to π_X .

Let H be the set of compositions $f_x \circ f_y^{-1}$. This is a quotient of $X \times X$. There are two maps from H to D , corresponding to the domain and range. Since H is a family of functions from C to itself, defined in terms of f , any automorphism that fixes C and preserves f will fix H (pointwise.) Given elements $x \in X$ and $h \in H$, we may consider the map $h \circ f_x$. This is a map from Q to C , and we may ask if it is represented by some element $y \in Y$. Let $\phi(x, h)$ be the formula $h \circ x \in X$.

Proposition. *$x, y \in X$ are conjugate under the automorphism group G_0 if and only if they have the same $\{\pi_X, \phi\}$ type*

Proof. If x and y are conjugate, then they have the same image. Let $y = \tau(x)$, and assume that for some $h \in H$, $h \circ x = z \in X$. Then $h \circ y = \tau(z) \in X$. Conversely, assume that x and y have the same type, and define a map τ as follows: $\tau_Q(q) = y^{-1} \circ x(q)$, $\tau_X(z) = z \circ x^{-1} \circ y$. τ_X is well defined because, taking $h = z \circ x^{-1}$, we have $h \circ x \in X$, hence so is $\tau_X(z)$. \square

Since G_0 acts freely on X , we get a definable family of G_0 -torsors. G_0 is then a quotient of a subset of $X \times_D X$, with the group operation defined by composition of functions, and the action on Q is defined via evaluation of functions.

There is an associated groupoid action, defined as follows: Let E be the set of canonical parameters for the subsets $\phi(x, -)$ of H . E can be identified with the set of types of elements of X over C with respect to ϕ (and π_X .) By replacing H with a subset of $H \times E$, we may assume that the data is given by $d : H \rightarrow E$. We also have a map $t : X \rightarrow E$ ($x \mapsto \text{tp}_0(x/C)$), and a composition map $\mu : H \times_E X \rightarrow X$. Using it we get a second map $c : H \rightarrow E$, given by $c(h) = t(h \circ x)$ for some $x \in X_{d(h)}$ (this does not depend on x .) The groupoid is now given as follows: The set of objects is E , the set of morphisms is H , the domain and codomain maps are d and c , respectively. The composition is given by composition of functions (from C to C .) There is a groupoid action on C given by evaluation of functions. Note that all the structure is in C^{eq} . The groupoid can be extended to an addition object $*$, with $\underline{Hom}(*, e) = X_e$ and $\underline{Hom}(*, *) = G_0$, and all composition are again as functions. The action is extended by adding Q .

Let now $\psi(\bar{q}, \bar{x}, \bar{c})$ be some formula. Let $\psi^*(y, \bar{d}, \bar{h}, \bar{c})$ be the formula $\psi(y(\bar{d}), \bar{h} \circ y, \bar{c})$. Let $G = G_{\{\psi\}}$ be the subgroup of G_0 preserving ψ . Then we get, similarly to the proposition above that $x, y \in X$ are conjugate under G if and only if they have the same type over ψ^* and the previous formulas. Thus G is definable in the same way as before. On the level of groupoids, the set of objects is again the type space (types with the additional ψ^*), and the set of morphisms is the same. We also get a definable functor from this groupoid to the original one, surjective on the level of objects. For an arbitrary collection of formulae, we get a projective system of such groupoids.

Example. Let T be the theory with two sorts Q and C , where C is a field, and Q is a vector space over C of dimension d . We may take X to be the set of bases of Q over C . In this case, H will be the set $Gl_d(C)$, the formula ϕ will be $hx \in X$ (which always holds.) The group $Gl(Q)$ of automorphisms of Q over C has X as a definable torsor and is reconstructed as $X \times X/Gl_d(C)$.

If, in addition, we are given a bilinear form $b : Q \times Q \rightarrow C$, the construction will produce the condition $b(x(d_1), x(d_2)) = b(y(d_1), y(d_2))$ (all d_i) for the pair (x, y) to give an automorphism of b . Applying this to the standard basis, we get the condition $A_x = A_y$, where A_x is the matrix $(b(x_i, x_j))$. We note that this condition is uniform in b . The set of objects of the corresponding groupoid is then a subset of $Mat_n(C)$. If x and y are two bases with $A_x = A_y$, and $h \in Gl_n(C)$, then $A_{hx} = A_{hy}$. Therefore the action of $Gl_n(C)$ descends to the A_x . In fact, $Hom(A_x, A_y)$ is the set of matrices h such that $hA_xh^T = A_y$.

6 minutes

2.2. Galois theory. The existence of a torsor X for the automorphism group gives rise to Galois theory, as follows: let $a \in X$ be an element, and let $A = dcl(a)$ (in T^{eq}). If $H_1 < H_2 < G$ are A -definable subgroups, such that $A^{H_1} = A^{H_2}$, then $H_1 = H_2$. Indeed, H_1 fixes the a -orbit under itself, hence so does H_2 .

This allows us to connect our construction with the one defined in the introduction. Recall that a definable set C is *stably embedded* if it satisfies the following equivalent conditions:

- (1) any parametrically definable subset of C^n is definable with parameters from C .
- (2) If $x \in M$, where M is a saturated model, is fixed by any automorphism fixing $C(M)$ pointwise, then x is definable over $C(M)$.

Let Q be internal to C , and let M be a saturated model. Let G be the automorphism group in our sense (where Δ is the collection of all definable sets), and let H be the automorphism group defined in the introduction. Clearly, $H \subseteq G$. Now assume that C is stably embedded. We claim that $H = G$. By Galois theory, it is enough to prove that any elements of A (as above) fixed by H is also fixed by G . Since C is stably embedded, any such element is definable over C , hence is fixed by H .

3. STABLE THEORIES WITH AN AUTOMORPHISM

12 minutes

The main example we would like to consider is when $T = ACFA$, and Δ is the collection of quantifier free formulas. In this case, we get an intersection of definable groups, but the definition of the groups themselves need not be quantifier free.

The source of the problem is that the definition of the group is given in terms of formulas of the form $E_\phi = \forall \bar{c} \in C(\phi(x, \bar{c}) \iff \phi(y, \bar{c}))$. As an example, let $Q = X$ be the set $\sigma(x) = -x$. Then one of the formulas ϕ will be $x^2 = c$. However, in this case, E_ϕ is equivalent to $x^2 = y^2$, a quantifier free formula.

This is an example of a general fact that holds for the following class of theories. Let T be a theory with EQ. A σ -structure for T is a definably closed subset of a model B of T , together with an automorphism $\sigma : B \mapsto B$. The theory T_σ of T with a generic automorphism is a theory with language extended with a symbol σ , which is the model companion of the theory of T with an automorphism. In other words, it is model complete, contains the universal part of T , and any σ -structure extends to a model of T_σ . T_σ need not exist, but it is unique. Any model of T_σ is a model of T together with an automorphism, and definable sets in T can be identified with definable sets in T_σ obtained by restricting the language.

Let T be a stable theory with EQ and EI, and assume that T_σ exists and eliminates imaginaries. Let C be the definable set $\sigma(x) = x$, and let Q be internal to C , with internality data X given within a T definable set by the formula $\sigma(x) = A(x)$, with A a T definable function. We also let Δ be the set of quantifier free sets, and

assume that $\pi : X \rightarrow D$, $g : X \times_D C \rightarrow Q$ and $\mu : H \times_E X \rightarrow X$ are given by function symbols in T_σ (it follows that Δ^* is also the set of quantifier free sets.)

Example. Let $T = ACF$. Then T_σ is $ACFA$. EI was proved in [CH99]. Since the internality datum is given by function symbols, all assumptions are satisfied.

Remark. The condition that $\sigma(x)$ is definable over x can be replaced with $\sigma^n(x)$ definable over $\sigma^i(x)$ for $i < n$. It is satisfied in each of the following cases:

- (1) Let $\tau : X \times_D X \rightarrow G_0$ be the map $(x, y) \mapsto x^{-1} \circ y$ (taking the pair to the automorphism it defines.) Let $m : G_0 \times X \rightarrow X$ be the action. By definition, for any $x, y \in X$, $m(\tau(x, y), x) = y$. In particular, $m(\tau(x, \sigma(x)), x) = \sigma(x)$. If $y \in X$ is another element, then $y = h \circ x$ for $h = y \circ x^{-1} \in H$. Therefore, if the composition $(h, x) \mapsto h \circ x$ is defined over the constants, then $\tau(y, \sigma(y)) = \tau(h \circ x, h \circ \sigma(x)) = \tau(x, \sigma(x))$, and we get that $\tau(x, \sigma(x))$ does not depend on x , and so corresponds to some constant A . Hence $m(A, x) = \sigma(x)$ for all x . Thus if m is T -definable, and the composition is over the constants, the condition holds.
- (2) Assume that T has the property that a substructure of a finitely generated structure is finitely generated (over any set of parameters.) Let $x \in X$ be an element, and consider the σ -structure B_x generated by x . If y is another element, the $y = h \circ x$ for some $h \in H$. Therefore, the σ -structure A_y generated by y is contained in the T -structure generated by h over A_x . Therefore, A_y is finitely generated over A_x . In particular, for some n , $\sigma^n(y)$ is definable from $\{\sigma^i(y) | i < n\}$ and A_x . When y varies, n is bounded (by compactness.) Since x and y were arbitrary, we may pick x and y independent. Therefore, A_x is not really used in the definition.

This Noetherian assumption holds when T is ω -stable, by a rank computation (of a generator for the big set over a substructure.)

We note that the formulas E_ϕ above assert that $tp_\Delta(x/C) = tp_\Delta(y/C)$. A T definable function that maps X into C will be called σ -invariant. If h is such a function, the formula $h(x) = c$ will appear in $tp_\Delta(x/C)$ for some $c \in C$. Restricting to this kind of formulas, the equality of types is given by $h(x) = h(y)$. We show that (under the above assumptions) these equations give the full definition: The relation $tp_\Delta(x/C) = tp_\Delta(y/C)$ is given by the set of equations $h(x) = h(y)$, where h is a T -definable invariant function. In particular, in $ACFA$ it is given by polynomial equations.

The stability is used in the proof in the following two ways: first, if A is a σ -structure which is algebraically closed in the sense of T , then it is algebraically closed in the sense of T_σ . Sketch of proof: Let A be an acl set, B and C σ closed sets. Then we may form $B \otimes_A C$, and this is again a σ -structure. Therefore we may embed it in a model M of T_σ . Now take $B = C = acl_\sigma(A)$. Then any element of B will have two copies in M unless it is already in A . But the number of algebraic elements in a class is fixed between models. Hence $B = A$.

The second use of stability is canonical bases: Let T be a stable theory with EI, a, b two elements, and C a definably closed set. Let E_a (E_b) be the set of elements fixed by all automorphisms fixing a (b) pointwise, and let D be a set containing both $E_a \cap C$ and $E_b \cap C$. If $tp(a/D) = tp(b/D)$ then $tp(a/C) = tp(b/C)$.

Given that, the proof goes as follows: Let x and y be two solutions to the equation, which agree on all invariant functions. This means that $dcl(x) \cap C =$

$dcl(y) \cap C = E$, and $tp(x/E) = tp(y/E)$. We show that this holds with E replaced by $D = acl(x) \cap C$. If $b \in D$, let $[b]$ be the set of conjugates of b over x . Then $[b] \in C$, since $\sigma(x) \in dcl(x)$, and $[b] \in dcl(x)$, hence $[b] \in E$. Since $tp(x/E) = tp(y/E)$, we get that $[b] \in dcl(y)$, and so b is algebraic over y . We now note that $acl(x) = acl_\sigma(x)$ and the same for y . However, $dcl_\sigma(x) \cap C \subseteq acl_\sigma(x) \cap C$ contains the canonical base of x .

As another application we prove the following result: Let G be the quantifier free automorphism group discussed above, and let G_0 be the subgroup of full automorphisms. Then G/G_0 is pro-finite. Since G_0 is already given as an intersection of groups G_ϕ , where ϕ is some definable (with quantifiers) subset of X , it is enough to prove that each such ϕ has a finite number of conjugates under G . Let p be the type of an element of X over C , and fix an element $x \in p$. Then $x\phi$ is a subset C_x of $H = C$. Let $t(x) \in C$ be the code of C_x . The function $x \mapsto t(x)$ is (σ) -definable. Therefore $t(x)$ is T -algebraic over C , so taking the code, we get a T -definable function $x \mapsto [t(x)]$. This function is in fact constant on p , and so t takes finitely many values on p . Hence the number of sets C_x is finite. These sets are identified with the conjugates of ϕ under G .

4. LINEAR DIFFERENCE EQUATIONS

Assume now that Q is given by the difference equation $\sigma(x) = Ax$. Following through the construction, we see that the group G_0 of automorphisms of the internality data is the subgroup of Gl_n given by $\sigma(X) = AXA^{-1}$. The group of automorphisms is the subgroup of this group preserving all values $h(x)$, where h is a rational invariant function. This group will, in general, be larger than the model-theoretic automorphisms group (eg, $\sigma(x) = 4x$.)

The condition $\forall x \in X(h(x) = h(gx))$ does not yet appear to be algebraic. However, it follows from the axioms of *ACFA* that X is dense in the set of all bases for K^n . It follows that the above condition can be replaced by $\forall x(h(x) = h(gx))$, which is just in the language of fields. From this it follows that the Galois group is in fact given by an algebraic group.

REFERENCES

- [CH99] Zoé Chatzidakis and Ehud Hrushovski, *Model theory of difference fields*, Trans. Amer. Math. Soc. **351** (1999), no. 8, 2997–3071. MR MR1652269 (2000f:03109) 3

DEPARTMENT OF PURE MATH, UNIVERSITY OF WATERLOO, WATERLOO, ONTARIO, CANADA

E-mail address: <mailto:mkamensky@math.uwaterloo.ca>

URL: <http://mkamensky.notlong.com>