MODEL THEORETIC VERSIONS OF WEIL'S THEOREM ON PREGROUPS

Elisabeth Bouscaren

In 1955, A. Weil published a paper ["On algebraic groups of transformations", Am. J. of Math., vol.77 (1955), p:355–391] where, starting from a variety V over some algebraically closed field K, together with a binary operation on V which has "good" properties (associativity, rationality) on a large piece of V (generic points), he constructs an algebraic group G over K, whose multiplication is an extension of the given one on generic points and which is birationally equivalent to V.

More precisely:

Let K be an algebraically closed field and let V be an irreducible variety over K such that there is a mapping f: VxV → V with the following properties:

(i) if a,b are independent generic points of V over K, then

$$K(a,b) = K(a,c) = K(b,c)$$

(ii) if a,b,c are independent generic points of V over K, then

$$f(f(a,b),c) = f(a,f(b,c)).$$

Then there is an algebraic group G over K which is birationally equivalent to V, such that this birational equivalence takes f(a,b), for a,b independent generics of V, to the product of the images of a and b.

Model–theorists working on stable groups became interested in this theorem in the following context: first, recall that, by a stable (ω–stable) group, we mean a group (G,·) definable in M^n for M a model of a stable (ω–stable) theory or interpretable, i.e. definable on some quotient of M^n by some definable equivalence relation.

Amongst the first natural examples of ω–stable groups are algebraic groups over an algebraically closed field K (they are definable in the theory of K in the language of fields).

Some years ago arose the conjecture that in fact all simple ω–stable groups with finite Morley rank "were" algebraic groups. Now, if one hopes to be able to define a topology and a variety structure on any such abstract group, one should certainly first try to do it (and the construction should hopefully be rather canonical) in the particular case of a group interpretable in some algebraically closed field but which has a priori no variety structure which makes it into an algebraic group.

This question was asked by B. Poizat and a first positive answer was given at the time by L. van den Dries (unpublished notes, characteristic 0 case): in order to simplify, let us say that the idea is to find a good $V \subseteq G$ with a variety structure satisfying the assumptions of Weil's theorem and then, to get the the algebraic group by applying the theorem.

This was unsatisfactory, even in the characteristic 0 case, for two reasons: first, if one does not know the proof of Weil's theorem, then one does not really know much about this structure of algebraic group and the way it relates to the original group; secondly, using the fact that we start with an actual group, there should be a more direct proof, avoiding some of the difficulties encountered when starting with an operation defined only on generic points.

This indeed turned out to be the case: a direct proof was given by E. Hrushovski (1986), in all characteristics.

This is the proof we want to present here.

Theorem 1:

Let K be an algebraically closed field, let $(G,\cdot)$ be interpretable in K, then G is definably isomorphic to an algebraic group over K.

More precisely this is decomposed in two parts:

Theorem 1–A: Let $(G,\cdot, inv)$ (inv denotes the inverse on G) $\subseteq K^n$ be a group definable with parameters in some countable $k_0 < K$, such that for a,b generic independent,

$$a.b \in k_0(a,b)$$
$$inv(a) \in k_0(a).$$

Then there is definably in K a structure of variety on G (over K) which makes $(G,\cdot,inv)$ into an algebraic group.

Theorem 1–B: Let H be interpretable in K, then there is $G \subseteq K^n$ satisfying the assumptions of 1–A, such that H and G are definably isomorphic.

The theorem above certainly qualifies as a model–theoretic version of Weil's theorem, but it does not deal with the part of the theorem which constructs a group from an operation on the generic points. Now, the following result can certainly be considered as the model–theoretic version of this aspect of Weil's theorem. It was in fact proved by E. Hrushovski prior to the other one, and is purely model–theoretic.

Theorem 2: (Hrushovski, Ph.D., Berkeley, 1986):

Let T be an ω–stable theory, let $p \in S(\varnothing)$ be a stationary type and let $*$ be a partial $\varnothing$ – definable operation such that:

(i) for a,b realizing p, independent,

$a*b$ realizes $p_{|a}$ and $p_{|b}$ (where $p_{|a}$ denotes the unique non forking extension of p over a)

(ii) for a,b,c, realizing p, independent,

$(a*b)*c = a*(b*c)$.

Then there is a definable set G, a definable operation $\cdot$ on G and a definable embedding g of p into G, such that

$(G,\cdot)$ is a group

for a,b $\models$ p, independent, $g(a*b) = g(a) . g(b)$

g(p) is the generic of G.

(In fact this theorem with the weaker conclusion that G be infinitely definable is proved for all stable theories).

We will not say more about this aspect, but one should note that, from these two theorems, one recovers the full statement of Weil's theorem: let V be an irreducible variety satisfying the assumptions in Weil's theorem and consider p the generic type of V. Then p satisfies the assumptions in Theorem 2, and by applying first Theorem 2 and then Theorem 1, one gets the algebraic group.

Remark: The same kind of result was also more recently proved in a different (and unstable) setting by A. Pillay ["On groups and fields definable in

O–minimal structures", preprint]. In particular he shows that if a group G is definable in the reals, then G is a Lie group.

Proof of Theorem 1:

We are going to assume that the group G is connected but this is no loss of generality as the general case follows from the connected case.

Theorem 1–A:

Let $(G,\cdot, inv) \subseteq K^n$ be a connected definable group with parameters in $k_0 < K$ such that, for a,b generic independent

$$a.b \in k_0(a,b)$$
$$inv(a) \in k_0(a),$$

then there is definably in K a structure of variety on G which makes $(G,\cdot,inv)$ into an algebraic group.

We are going to need the following easy lemma:

Lemma 0:

a) – Let V be an irreducible variety and let $X \subseteq V$ be a definable set, X containing the generic of V. Then X contains an open subset O of V (and of course O contains the generic).

b) – Let V and V' be two irreducible varieties, and let f be a definable map from V to V' such that, on the generic of V, f is rational. Then there is $O \subseteq V$, open, such that $f|O$ is a morphism.

Proof:

a) – The set X is definable, therefore it is a finite union of sets of the form $O \cap F$, where O is open in V and F is closed in V. Choose one such $O \cap F$ that contains the generic, so F contains the generic, but the complement of F in V is open and, as V is irreducible, must also contain the generic, so $F = V$.

b) – Choose a definable $X \subseteq V$, containg the generic, such that f(a) is a given rational function of a, for all a in X. By a) X contains an open set of V.

Proof of Theorem 1–A:

The group G is definable, so $G = \bigcup_{i<m} (O_i \cap F_i)$, where we can assume the O_i's to be principal open sets in K^n and where the F_i's are closed in K^n. Let V_0 be one of these intersections, containing the generic of G, p. Then on V_0 we have the structure of an irreducible prevariety, with generic p; we also have the usual structure of prevariety on $V_0 \times V_0$, with generic pxp. Let X be a definable subset of $V_0 \times V_0$ containing pxp, such that if $(x,y) \in X$, then $x.y$ is rational over x,y. Let $X' = \{(x,y) \in X ; x.y \in V_0\}$, X' is definable. By the lemma above, there is $M_0 \subseteq X'$, open in $V_0 \times V_0$, such that multiplication, from M_0 in V_0, is a morphism. For the same reasons, there is $V_1 \subseteq V_0$, open such that inv is a morphism from V_1 in V_0.

Now let

$Y = \{x \in V_1 ;$ for all y generic independent from x, $(y,x) \in M_0$ and $(inv(y),y.x) \in M_0\}$.

By definability of the type p, Y is a definable set, and Y contains the generic p. By the lemma again, there is $V_2 \subseteq V \subseteq V_1$, open, and of course, inv is still a morphism from V_2 in V_0. Now let $V = V_2 \cap inv(V_2)$, then V is open, because V is the inverse image (in V_2) by a morphism, of an open set, and $V = inv(V)$. Let $M = \{(x,y) \in M_0 \cap VxV ; x.y \in V\}$, again, because multiplication is a morphism, M is open.

So, by taking smaller and smaller open sets we have come to the following situation: we have V, open in V_0, therefore with the induced variety structure, and M, open in VxV, such that:

(i) multiplication is a morphism from M into V

(ii) inv is a morphism from V into V and $inv(V) = V$

(iii) for all x in V, for all y generic independent from x, (y,x) and $(inv(y),y.x)$ are both in M.

The structure of variety on G is obtained by covering G by translates of V (i.e. of the form $a.V$). As G is an ω–stable group and V contains the generic of G, we know that a finite number of translates of V will be sufficient to of G, we know that a finite number of translates of V will be sufficient to cover G.

In order to see that this indeed gives G the structure of a variety and in fact of an algebraic group, we need the following lemma:

Lemma:

Let $a,b \in G$, let $H = \{(x,y) \in VxV;\ a.x.b.y \in V\}$. Then

– H is open

– the map f_{ab} from H into V, which takes (x,y) to a.x.b.y is a morphism.

Proof of the Lemma:

Let $(x_o,y_o) \in H$, we want to find H_o, $(x_o,y_o) \in H_o \subseteq H$, open, such that f_{ab} restricted to H_o is a morphism.

We know that $b = c.d$, where c and d both realize the generic p; let e also realize p, independent from $\{a,c,d,x_o,y_o\}$. Let $H_o = \{(x,y) \in VxV;$ $(e.a,x) \in M$, $(e.a.x,c) \in M$, $(e.a.x.c,d) \in M$ $(e.a.x.c.d,y) \in M$, $(inv(e),e.a.x.c.d.y) \in M\}$.

First, by the choice of e, and by applying condition (iii) on V each time, $(x_o,y_o) \in H_o$.

We see that H_o is open in VxV by applying successively the following classical facts: if O is open in VxV, if h is a morphism form O in V, if $z \in V$, then the set

$$\{(x,y);\ (x,z) \in O \text{ and } (h(x,z),y) \in O\}$$

is open, and also,

$$O_z = \{x \in V;\ (z,x) \in O\}$$

is open and h_z, from O_z in V, is a morphism.

Now a.x.b.y = inv(e).e.a.x.c.d.y , so $H_o \subseteq H$, and over H_o, f_{ab} becomes a composition of morphisms because at each step the elements one wants to multiply are in M, and hence it is a morphism.

We can now go back to the proof of the theorem. Choose $a_1,...,a_n$ in G such that $G = a_1 V \cup ... \cup a_n V$ (where aV denotes the set {a.x; $x \in V$}). In order to check that this, together with the left translations f_i from V into a_i V, is a prevariety on G, we need that for all i,j

– $V_{ij} = \{x \in V; a_i.x \in a_j V\} = \{x \in V; inv(a_j).a_i.x \in V\}$ is open

– the map f_{ij} from V_{ij} into V which takes x to $inv(a_j).a_i.x$ is a morphism.

But, it is a direct consequence of the lemma that, for all a in G, the set $V_a = \{x \in V; a.x \in V\}$ is open and the left translation by a is a morphism.

It remains to check that multiplication and inverse are morphisms.

Multiplication:

GxG, as a variety is covered by products of the form aVxbV, which get their variety structure from VxV. To say that multiplication is a morphism means exactly that the set

$A_{abc} = \{(x,y) \in VxV; a.x.b.y \in cV\} = \{(x,y) \in VxV; inv(c).a.x.b.$
$y \in V\}$

is open in VxV and that the map from A into V which takes (x,y) to inv(c).a.x.b.y is a morphism. This is exactly the lemma.

inverse:

It is a morphism if the set

$A_{ab} = \{x \in V; inv(a.x) \in bV\} = \{x \in V; inv(a.x.b) \in V\}$

is open and the map from A_{ab} into V which takes x to inv(a.x.b) is a morphism. But (condition (ii)) inv(V) = V, so $A_{ab} = \{x \in V; a.x.b \in V\}$, and again it is open, as a direct consequence of the lemma, and the map taking x to a.x.b is a morphism. We also have that, on V, inv is a morphism, so inv(a.x.b) is the composition of two morphisms. □

Theorem 1–B:

Let (H,·,inv) be a connected group interpretable in K. Then there is a definable group $(G,*, inv') \subseteq K^n$ and some countable $k_0 \leq K$, k_0 containing the defining parameters of H and G, such that H and G are definably isomorphic and, for a,b generic independent in G, $a*b \in k_0(a,b)$ and inv' (a) $\in k_0(a)$.

Proof:

Note first that, by elimination of imaginaries in algebraically closed fields, any interpretable group is definably isomorphic to some definable group in some K^n, so we can assume that $(H,\cdot, inv) \subseteq K^n$. Without loss of generality, assume K is very staurated.

Now if K has characteristic 0, then there is nothing left to prove, as any definable function is locally rational, so we assume that K has characteristic p>0.

Let $k \subseteq K$ be an uncountable algebraically closed field, containg all the defining parameters of H. There is some $q = 1/p^m$ such that, for all $\bar{a}, \bar{b} \in H$, $\bar{a}.\bar{b} \in k(\bar{a}^q, \bar{b}^q)^n$ and $inv(\bar{a}) \in k(\bar{a}^q)^n$ (where if $\bar{a} = (a_1,...,a_n)$, $k(\bar{a}^q)$ denotes $k(a_1^q,...,a_n^q)$).

Let $\bar{a}$ realize the generic of H over k. We define:

$k^*(\bar{a}) = k(\bar{a}^q, inv(\bar{a})^q, \bar{b}_1.\bar{a}.\bar{b}_2, \bar{b}_1.inv(\bar{a}).\bar{b}_2; \bar{b}_1, \bar{b}_2 \in H \cap k^n)$.

We have that $k^*(\bar{a}) \subseteq k(\bar{a}^{q'})$, with $q' = q^2$.

Now $k(\bar{a}^{q'})$ is a finite extension of $k(\bar{a})$ hence so is $k^*(\bar{a})$, so there are $c_1,...,c_k$ in $k(\bar{a}^{q'})$, such that $k^*(\bar{a}) = k(\bar{a},c_1,...,c_k)$, and of course, each c_i is definable over $k \cup \bar{a}$.

Consider f: $H \to k^{n+k}$, definable injection such that for $\bar{a}$ generic,

$f(\bar{a}) = (\bar{a}, c_1, \ldots, c_k)$.

Trivially, $k^*(\bar{a}) = k^*(\mathrm{inv}(\bar{a}))$, so $k(f(\bar{a})) = k(f(\mathrm{inv}(\bar{a})))$, so if G is the image of H by f, with the obvious group law, it is true that, on a generic of G, the inverse is rational.

Now it is also trivial that, if $\bar{b} \in k^n \cap H$, then

$$k^*(\bar{a}.\bar{b}) = k^*(\bar{a}), \text{ so } k(f(\bar{a}.\bar{b})) = k(f(\bar{a}))$$

$$(*)$$

$$k^*(\bar{b}.\bar{a}) = k^*(\bar{a}), \text{ so } k(f(\bar{b}.\bar{a})) = k(f(\bar{a})).$$

We also have that, as f is a definable bijection, for $\bar{a}$, $\bar{b}$ generic, $f(\bar{a}.\bar{b}) \in k(f(\bar{a})^r, f(\bar{b})^r)^{n+k}$ for $r = 1/p^\ell$, for some ℓ.

Let k_0, countable, $k_0 < k$, contain all the necessary parameters.

Let $\bar{b} \in H \cap k^n$ realize the generic of H over k_0, and let $\bar{a}$ realize the generic of H over k. By $(*)$, $f(\bar{a}.\bar{b}) \in k(f(\bar{a}))^{n+k}$, and we also have that

$$f(\bar{a}.\bar{b}) \in k_0(f(\bar{a})^r, f(\bar{b})^r)^{n+k}.$$

But, $k(f(\bar{a})) \cap k_0(f(\bar{a})^r, f(\bar{b})^r) = k_0(f(\bar{a}), f(\bar{b})^r)$: because $f(\bar{a})^r$ remains over $k(f(\bar{a}))$ of the same degree as over $k_0(f(\bar{a}), f(\bar{b})^r)$, since $\bar{a}$ is independent from k, which contains $f(\bar{b})^r)$, over k_0.

Symmetrically, because $\bar{a} \wedge \bar{b}$ and $\bar{b} \wedge \bar{a}$ have the same type over k_0, we have that $f(\bar{a}.\bar{b}) \in (k_0(f(\bar{a}), f(\bar{b})^r) \cap k_0(f(\bar{a})^r, f(\bar{b}))\,)^{n+k}$.

But these two fields are linearly disjoint over $k_0(f(\bar{a}), f(\bar{b}))$: more generally, it is classical algebra that if K_1, K_2 are linearly disjoint over k_0, if $x \in K_1$, $y \in K_2$, then $K_1(y)$ and $K_2(x)$ are linearly disjoint over $k_0(x,y)$. As $\bar{a}$ and $\bar{b}$ are independent over k_0, $k_0(f(\bar{a})^r) = K_1$ and $k_0(f(\bar{b})^r) = K_2$ are linearly disjoint over k_0, then we get the result by letting $f(\bar{a}) = x$ and $f(\bar{b}) = y$. It follows that $f(\bar{a}.\bar{b}) \in k_0(f(\bar{a}), f(\bar{b}))\,)^{n+k}$, that is, that in G, the multiplication of two independent generics is rational. □

UA 753 – CNRS
Université Paris 7.