A TALK ON 'SMALL' MULTIPLICATIVE SUBGROUPS

AYHAN GÜNAYDIN

1. A very brief introduction to Model Theory

Here I'll summarize -in very vague terms- quite a small part of model theory that will be necessary for some parts of the rest of the talk. I'll refer to this part of model theory as 'definability theory'. The basic objects of 'definability theory' are 'definable' sets. These are like varieties in algebraic geometry or analytic sets in complex analysis.

Fix a *language* L, this just means a set whose elements fall into two categories: *relations* and *functions*; and each of them come with *arity*. For the moment they are just abstract objects, but in a bit we will interpret them as honest relations and functions and the arities will mean what they are supposed to mean. Then we have *L-terms* and *L-formulas*: terms are like polynomials or linear forms and formulas are polynomial equalities or polynomial inequalities and so on. I won't get into the details of these, but I want to emphasize that formulas have *quantifiers* and this is really the subtle part. These things still don't have meaning, but when we give them meanings we will be allowed to quantify only over elements of our 'structure'. On this note, let me say what a structure is: an *L-structure* $\mathcal{M}$ is a set, say M and interpretations in M of the symbols in L; this is to say that if $R \in L$ is a relation symbol of arity k, then the interpretation $R^{\mathcal{M}}$ of R in $\mathcal{M}$ is just a subset of M^k.

So given a structure $\mathcal{M}$, there is a correspondence between formulas and definable sets; but note that a definable set could be defined by many different formulas; like in the field $\mathbb{C}$, the singleton $\{0\}$ is defined by $2x = x$ or $3x = x$ or $\forall y(x \cdot y = x)$ and so on... But then we can take care of this problem by taking formulas up to *equivalence in* $\mathcal{M}$.

Also when we have a chain of structures $\mathcal{M} \subseteq \mathcal{N}$, the definable set defined by a formula often gets bigger. It might be a good idea to introduce a special kind of extension of structures. We say that $\mathcal{N}$ is an *elementary extension* of $\mathcal{M}$ if for every formula $\phi(\vec{x})$ and $\vec{m} \in M$, the sentence $\phi(\vec{m})$ holds in $\mathcal{N}$ if and only if it holds in $\mathcal{M}$. The good thing is that we can always find nice elementary extension where 'anything that can be true is true'. These 'big' structures are called *saturated*.

Date: May 5, 2011.

The point is that we want to understand the structure of definable sets; many mathematical topics could be covered this way. For instance all the basic algebraic geometry could be coded as the study of the definable sets and functions in the structure $(\mathbb{C}, +, -, \cdot, 0, 1)$. It is worth noting that this is actually a very special structure as the only definable sets here are the (Zariski) constructible sets. In general this is a very desirable result: representing the definable sets in a natural and simple form.

A good source for learning model theory is [6] and the first part of the article [7] is very helpful introduction.

2. Solving equations in finitely generated groups

One vein of number theory is the study of zeros of polynomials in finitely generated groups; or rather it was until a good answer was given in 90's.

Now let me start to be more precise. Let's fix a big algebraically closed field Ω of characteristic 0 (for most purposes $\mathbb{C}$ is enough). Let $\mathbb{A}$ be a semi-abelian variety over Ω; that is an extension of an abelian variety by some copies of the algebraic group $\mathbb{G}_m$. Also let Γ be a subgroup of $\mathbb{A}$ of finite rank; this is to say that it has a finitely generated subgroup Γ^* such that Γ/Γ^* is torsion or that the $\mathbb{Q}$-dimension of $\Gamma \otimes_{\mathbb{Z}} \mathbb{Q}$ is finite.

Now the *Mordell-Lang Conjecture* states that for every subvariety $V \subseteq \mathbb{A}$, the trace $V \cap \Gamma$ is a finite union of cosets of algebraic subgroups of Γ; here by 'algebraic subgroup of Γ', I mean a subgroup of Γ of the form $T \cap \Gamma^n$, where T is an algebraic subgroup of $\mathbb{A}$.

One might ask why this is number theory. Consider a smooth projective curve $C \subseteq \mathbb{P}^2(\mathbb{C})$ over $\mathbb{Q}$ and the rational points $C(\mathbb{Q})$ on it (this is certainly number theory). If the genus of C is 0, then it is parametrized by rational functions in one variable; this is there are polynomials $p, q, r \in \mathbb{Q}[T]$ such that $(x, y) \in C$ if and only if there is $t \in \mathbb{C}$ such that $x = \frac{p(t)}{r(t)}$ and $y = \frac{q(t)}{r(t)}$. Then it is easy to calculate all the rational points. If the genus is 1, then C is an elliptic curve and the Mordell-Weil theorem says that $C(\mathbb{Q})$ is a finitely generated subgroup of C. If the genus is greater than or equal to 2, then the Mordell conjecture claimed that $C(\mathbb{Q})$ is finite (this is proven by Faltings among much stronger things). Another way to see this last case is by embedding C into its jacobian $\mathbb{A} = J(C)$, which happens to be an abelian variety. Then we know that the rational points of C embeds into the rational points of $\mathbb{A}$ and again by Mordell-Weil we know that $\mathbb{A}(\mathbb{Q})$ is finitely generated. Now we want to understand $C(\mathbb{Q}) = C \cap \mathbb{A}(\mathbb{Q})$ and now MLC says that it is a finite union of algebraic subgroups. But C being one dimensional and of genus ≥ 2, cannot be a translate of an elliptic curve itself. So the only possible abelian subvarieties of $\mathbb{A}$ that could appear in that union is 1. Hence the Mordell conjecture is proven.

The finite rank case is included in MLC in order to cover the so called Manin-Mumford conjecture on the torsion points of abelian varieties. I am not going to get into that today.

In the positive characteristic case the question was still open for a while, until Hrushovski found a model theoretic proof that works uniformly in every characteristic. His proof is very involved and uses very sophisticated model theory. However, allow me to state a very crucial ingredient.

Proposition 2.1. *Let $\mathbb{A}$ be a commutative algebraic group over Ω (not necessarily an abelian variety) and $\Gamma \leq \mathbb{A}$ (not necessarily of finite rank). Then Γ satisfies the conclusion of MLC if and only if the structure $(\Omega, +, \cdot, 0, 1, \Gamma)$ is 'stable' and the structure induced on Γ is 'one-based'.*

The definition of one-based is a very involved matter and I don't know a way to explain it in algebraic terms, but 'stable' means that 'we cannot define an infinite ordered set'. I just wanted to illustrate that these seemingly unrelated model theoretic notions becomes very important in this proof. (In this case, one based means something like 'for any tuple $\vec{g}$ from Γ, the field of definition of the locus of $\vec{g}$ over any finite set is contained in $\mathbb{Q}(\vec{g})^{alg}$'.)

My interest is in very special kind of semi-abelian varieties, namely $\mathbb{G}_m^n$. In this case MLC was solved by Laurent in 80's(?) In this case, we know exactly what the algebraic subgroups are: they are *tori*; subgroups given by $x_1^{k_1} \cdots x_n^{k_n} = 1$ for a fixed integer tuple $(k_1, \ldots, k_n)$. Then MLC is to say that in the group Γ

$$\text{ALGEBRAIC DEPENDENCE} = \text{LINEAR DEPENDENCE}.$$

A good source for these topics is [5] and one could read [1] for the model theory connections.

3. Solving linear equations in multiplicative groups

Inspired by a paper of Zilber handling $(\mathbb{C}, \mathbb{U})$, I've started to work on the solutions of 'linear' equations in multiplicative groups. We keep the notation from the beginning of the previous section with $\mathbb{A} = \mathbb{G}_m$. We say that Γ has the *Mann property* if for every $q_1, \ldots, q_n \in \mathbb{Q}^\times$, there are only finitely many $(g_1, \ldots, g_n) \in \Gamma^n$ such that

$$q_1 g_1 + \cdots + q_n g_n = 1 \text{ and } \sum_{i \in I} q_i g_i \neq 0,$$

for every nonempty proper subset I of $\{1, \ldots, n\}$. (We call such solutions *nondegenerate*.)

This turns out to be the same as the *Mordell-Lang property*. This way we get a lot of model theoretic information on the structure (Ω, Γ). For instance, it is *near model complete*, which is to say that the subsets of Ω^n definable in the pair (Ω, Γ) are boolean combinations of existentially definable subsets. We also get that it is ω-stable when Γ is divisible, hence we have a notion

of dimension, called *Morley rank*, different than the usual dimension; for instance the group Γ has Morley rank 1 and Ω has Morley rank ω. Morley rank somehow gives a finer information than the one given by the usual dimension.

Of course, all subgroups of $\Omega^\times$ of finite rank have this property. Another (non-finite rank) example of groups with this property is the group of exponentials of algebraic numbers. We use the following to show that:

Lemma 3.1. *Let K be a field with subfield E, and G and Γ are subgroups of $K^\times$ with $\Gamma \subseteq G$. Suppose Γ is a pure subgroup of G and each root of unity in G lies in Γ. Then the following two conditions are equivalent:*

1. *for any $c_1, ..., c_m \in E^\times$ the equation $c_1x_1 + \cdots + c_mx_m = 1$ has the same nondegenerate solutions in Γ as in G;*
2. *whenever $g_1, ..., g_n \in G$ are multiplicatively independent over Γ, they are algebraically independent over $E(\Gamma)$.*

Now it follows from the Lindemann-Weierstrass theorem that the second property holds with $G = \exp(\mathbb{Q}^{\mathrm{ac}})$, $\Gamma = 1$ and $E = \mathbb{Q}^{\mathrm{ac}}$. As a matter of fact, such a proof shows even more. Namely it proves that for every $n > 0$, there is a finite subset $G(n) = \{(1, \ldots, 1)\}$ of G^n such that for every $k_1, \ldots, k_n \in \mathbb{Q}^\times$, the nondegenerate solutions of $k_1x_1 + \cdots + k_nx_n = 1$ in G^n are in $G(n)$. Moreover we could take $k_1, \ldots, k_n$ from $\mathbb{Q}^{\mathrm{ac}}$. This gives us the following very uniform form of Mann/Mordell-Lang property.

Definition 3.2. Let Ω be an ambient algebraically closed field and let K be a subfield of Ω and G a subgroup of $\Omega^\times$. We say that (K, G) is a *Mann pair* if for every $n > 0$, there is a finite subset $G(n)$ of G^n such that for every $a_1, \ldots, a_n \in K^\times$, the nondegenerate solutions of $a_1x_1 + \cdots + a_nx_n = 1$ in G^n lie in $G(n)$.

In our paper we prove the following.

Theorem 3.3. *Let K be algebraically closed and G is of finite rank with $K^\times \cap G = \{1\}$. Then (K, G) is a Mann pair.*

Allow me to illustrate this in a very simple case. Let K be an algebraically closed field and let G be the subgroup of $K(t)$ generated by $t - 5$ and $t^2 + 2t - 7$. Note that $G \cap K^\times = \{1\}$ and obviously G is finitely generated. Then according to our theorem (K, G) must be a Mann pair. However, in this case we could even tell what the possible solutions are, using the following theorem from [2].

Theorem 3.4. *Let K be of characteristic zero and let F be a function field over K. Also let g be the genus of $F|K$, and let S be a finite subset of $\mathcal{R}(F|K)$ and $n \geq 2$. Suppose $u_1, \ldots, u_n$ are S-units and $(u_1, \ldots, u_n)$ is a non-degenerate solution of $x_1 + \cdots + x_n = 0$. Then*

$$H(u_1, \ldots, u_n) \leq \frac{1}{2}(n-1)(n-2)\{|S| + \max(0, 2\,\mathrm{g} - 2)\}.$$

In our case $F = K(t)$ and hence $H(u_1, \ldots, u_n) = \max\{\deg_t u_1, \ldots, \deg_t u_n\}$ and also the cardinality of S is at most 4. Thus we get that the degrees of the polynomials involved should be less than $2(n-1)(n-2)$.

On the model theory side of the story we have both "near model completeness" and "orthogonality". Namely subsets of Ω^n definable in the structure (Ω, K, G) are given by boolean combinations of sets of defined by

$$\exists y \exists z (y \in K^p \wedge z \in G^q \wedge \phi(x, y, z)),$$

and definable subsets of $K^m \times G^n$ are finite unions of $X \times Y$ where X is definable in the field K and Y is definable in the group G.

Also when K is algebraically closed and G is divisible, the structure (Ω, K, G) becomes ω-stable, which is to say that there is notion of dimension "somehow" refining the usual one. It is called the Morley rank. In this particular case $\mathrm{MR}(K) = \mathrm{MR}(G) = 1$ and $\mathrm{MR}(\Omega) = \aleph_0$.

Everything in this section appears in [3] and [4].

References

[1] Elisabeth Bouscaren, editor. *Model theory and algebraic geometry*, volume 1696 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1998. An introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture.

[2] W.D. Brownawell and D.W. Masser. Vanishing sums in function fields. *Math. Proc. Camb. Phil. Soc.*, 100:427–434, 1986.

[3] Lou van den Dries and Ayhan Günaydın. The fields of real and complex numbers with a small multiplicative group. *Proc. London Math. Soc. (3)*, 93(1):43–81, 2006.

[4] Lou van den Dries and Ayhan Günaydın. Mann pairs. *Trans. Amer. Math. Soc.*, 362(5):2393–2414, 2010.

[5] Serge Lang. *Number theory. III*, volume 60 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 1991. Diophantine geometry.

[6] D. Marker. *Model Theory. An Introduction.* Graduate Texts in Mathematics, 217. Springer-Verlag, New York, 2002.

[7] Rahim Moosa. Model theory and complex geometry. *Notices Amer. Math. Soc.*, 57(2):230–235, 2010.