Algebraic geometry and model theory

The Hitchhiker's Guide to Hrushovski's proof of the geometric Mordell-Lang conjecture

יעקב גוגולוק

Contents

1. A touch of algebraic geometry

Algebraic geometry, at least in its most basic form, studies sets defined by polynomial equations. Such sets are called **algebraic**. We will begin our encounter with algebraic geometry through **affine algebraic geometry** where one studies algebraic subsets of the **affine space** k^n over a field k. In this chapter we will introduce some very basic notion in the language of algebraic geometry a'la Weil.

Let k be a field. Soon we will restrict ourselves to algebraically closed sets, but the basic definitions make sense of arbitrary fields. We also fix a natural number n.

1.1. Affine algebraic sets

Definition 1.1. Let $I \subseteq k[X_1, \dots, X_n]$. The **zero set of** I is the set

$$V(I) = \left\{ a \in k^n | f(a) = 0 \text{ for all } f \in I \right\}.$$

We call sets of this form **affine algebraic sets.**

Note that if I' is the ideal generated by I, then $V(I) = V(I')$. There is therefore no harm in assuming in the above definition that I is an ideal.

Lemma 1.2. *Let $I, J, (I_\alpha)_{\alpha \in A}$ be ideals of $k[X_1, \dots, X_n]$. The following properties hold.*

1. $V(\emptyset) = k^n, V(\{1\}) = \emptyset$,
2. $V(I) \cup V(J) = V(IJ)$,
3. $V\left(\sum_{\alpha \in A} I_\alpha\right) = \bigcap_{\alpha \in A} V(I_\alpha)$.

Proof. See Exercise 1.4. □

Lemma 1.2 implies that affine algebraic sets form the closed sets of a topology on k^n (and thus on any subset of k^n). We call this topology the **Zariski topology** on k^n. From now on this is the default topology on k^n and its subsets.

Definition 1.3. A subset $V \subseteq k^n$ is called a **quasi-affine algebraic set** if it is an open subset of an affine algebraic set.

Recall that a ring R is **noetherian** if any ideal of R is finitely generated or equivalently: any ascending chain of ideals stabilizes. The following is a standard theorem proven in any reasonable algebra course.

Fact 1.4 (Hilbert Basis Theorem). *If R is a noetherian ring then so is the ring $R[X]$.*

Since fields are clearly noetherian rings, a trivial inductive argument yields the following.

Corollary 1.5. *The ring $k[X_1, \dots, X_n]$ is noetherian.*

Corollary 1.5 has a natural geometric intepretation. To state it we need the following definition.

Definition 1.6. A topological space X is called **noetherian** if there is no strictly descending chain $X_0 \supsetneq X_1 \supsetneq \dots \supsetneq X_n \supsetneq \dots$ of closed subsets of X.

Noetherian spaces are quite orthogonal to spaces one typically has in minds (like the reals or manifolds). Nonetheless, they are ubiquitous in algebraic geometry as seen by the following results.

Proposition 1.7. *Any affine algebraic set is a noetherian space.*

Proof. Since any affine algebraic subset of k^n is closed, an chain of closed subsets of in V is also a chain of closed subsets of k^n. It suffices thus to prove that k^n is a noetherian space. Let $X_0 \supseteq X_1 \supseteq \ldots \supseteq k^n$ be an infinite chain of closed subsets of k^n. By the definition of the Zariski topology, for each k there is some ideal $I_k \trianglelefteq k[X_1, \ldots, X_n]$ such that $X_k = V(I_k)$. Since $X_k \supseteq X_{k+1}$ we have

$$X_k = X_0 \cap X_1 \cap \ldots \cap X_k = V(I_0) \cap V(I_1) \cap \ldots \cap V(I_k) = V(I_0 + \ldots I_k)$$

by Lemma 1.2. Therefore by replacing I_k by $I_0 + \ldots + I_k$ we may assume that

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$$

so by Corollary 1.5 we have that $I_N = I_{N+1} = \ldots$ for some N. Thus $X_N = X_{N+1} = \ldots$, which proves that k^n is noetherian. □

1.2. Dimension

Definition 1.8. A topological space X is called **irreducible** if there are no proper closed subsets $X_1, X_2 \subsetneq X$ such that $X = X_1 \cup X_2$. In the case X is an (quasi-)affine algebraic set, we call X an (quasi-)affine variety.

Proposition 1.9. *Let X be a noetherian space. Then there exist irreducible closed subsets $X_1, \ldots, X_n \subseteq X$ such that $X = X_1 \cup \ldots \cup X_n$. Assuming that $X_i \not\subseteq X_j$ for all i, j, the sets $X_1, \ldots, X_n$ are uniquely determined up to permutation.*

Sketch of a proof. If X is irreducible, then there is nothing to do. Otherwise $X = X_1 \cup X_2$ for some proper closed subsets $X_1, X_2 \subsetneq X$. If X_1 is irreducible, leave it be and move to X_2. Otherwise $X_1 = X_{11} \cup X_{12}$ for some proper closed sets $X_{11}, X_{12} \subsetneq X_1$... This process has to terminate as otherwise we would have constructed an infinite chain of closed sets $X_1 \supsetneq X_{11} \supsetneq \ldots$. Uniqueness is left as an exercise (see Exercise 1.1). □

We call the sets $X_1, \ldots, X_n$ from Proposition 1.9 the **irreducible components of** X.

Irreducible sets allow us to define the notion of dimension of a noetherian space X. Let us introduce (only for the sake of the next definition) the following terminology: a strictly ascending of nonempty irreducible closed sets $X_0 \subsetneq \ldots \subsetneq X_n \subseteq X$ is called a **chain of length** n **in** X.

Definition 1.10. Let X be a noetherian space. Let X We define the **dimension of** X as

$$\dim X := \sup \{ n \in \omega | \text{ there exists an chain of length } n \text{ in } X \} \in \mathbb{N} \cup \{\infty\}.$$

It is pretty easy to see that $\dim k^1 = 1$ (as the topology on k^1 is the cofinite topology) but already showing that the plane k^2 has dimension 2 is a nontrivial task! We give a recipe for that in Exercise 1.16.

For future model-theoretic reasons, the following will unassuming fact will be important.

Lemma 1.11. *A Zariski closed set V has dimension $\geq n + 1$ if and only if there disjoint Zariski closed sets $V_1, V_2, \ldots \subseteq V$, each of dimension $\geq n$.*

Proof. See Exercise 2.5. □

1.3. Hilberts Nullstellensatz

Theorem 1.12 (Weak Nullstellensatz). *Assume that k is algebraically closed and let $I \lhd k[X_1, \ldots, X_n]$ be a proper ideal. Then $V(I)$ is nonempty.*

Definition 1.13. Let R be a ring and let $I \trianglelefteq R$ be an ideal. The **radical of** I

$$\sqrt{I} := \left\{ a \in R | \text{ there is some } n \in \mathbb{N} \text{ such that } a^n \in I \right\},$$

An ideal I is called **radical** if $I = \sqrt{I}$.

Definition 1.14. Let $A \subseteq k^n$ be any set. We define the **vanishing ideal** as the set

$$\mathcal{I}_A = \left\{ f \in k[X_1, \ldots, X_n] | f(a) = 0 \text{ for all } a \in A \right\}.$$

Theorem 1.15 (Nullstellensatz). *Assume that k is an algebraically closed field. For any ideal is I we have that $\mathcal{I}_{V(I)} = \sqrt{I}$.*

1.4. The ring of regular functions. Morphisms.

Definition 1.16. Let $V \subseteq k^n$ be an affine algebraic set. A function $f : V \to k$ is called **regular** if there is a polynomial $F \in k[X_1, \ldots, X_n]$ such that $f(a) = F(a)$ for all $a \in V$.

Definition 1.17. Let $V \subseteq k^m, W \subseteq k^n$ be affine algebraic sets. We say that a function $f : V \to W$ is a **morphism** if there are polynomials $f_1, \ldots, f_n \in k[X_1, \ldots, X_m]$ such that

$$f(a) = (f_1(a), \ldots, f_n(a))$$

for all $a \in W$.

Note that $f : U \to V$ as above yields a morphism $f^\sharp : \mathcal{O}(V) \to \mathcal{O}(W)$ given by $f^*(\varphi) = \varphi \circ f$ for $\varphi \in \mathcal{O}(W)$.

Proposition 1.18. *The ring $\mathcal{O}(V)$ is isomorphic (as a k-algebra) to $k[X_1, \ldots, X_n]/\mathcal{I}_V$.*

Exercises

Noetherian spaces

Exercise 1.1. Show that the irreducible components of a noetherian space are uniquely determined.

The Zariski topology

Exercise 1.2. Consider the map $f\colon k \to k^3$ defined by $f(t) = (t, t^2, t^3)$. Show that the image of f is Zariski closed.

Exercise 1.3. *(A continuation of Exercise 1.2)* For $k = \mathbb{C}$ give an example of a morphism $f\colon k^2 \to k$ whose image is not Zariski closed. Note that the image of your f is a sum of sets of the form $X \setminus Y$ where X and Y are Zariski closed. For $k = \mathbb{R}$ give an example of a morphism $f\colon k^2 \to k$ which does not have this property.

Exercise 1.4. Let $I, J, I_\alpha (\alpha \in A)$ be ideals of $k[X_1, \dots, X_n]$. Show the following:

1. $V(\emptyset) = k^n, V(\{1\}) = \emptyset$,
2. $V(I) \cup V(J) = V(IJ)$,
3. $V\left(\sum_{\alpha \in A} I_\alpha\right) = \bigcap_{\alpha \in A} V(I_\alpha)$.

Exercise 1.5. Let $R = k[X_1, \dots, X_n]$ and let $f \in R$ be a non-constant polynomial.

1. Assume that f is square-free (i. e. not divisible by a square of any irreducible polynomial). Show that the ideal (f) is radical.
2. Describe the ideal (f) for arbitrary f.

Exercise 1.6. Show that an ideal $I \trianglelefteq R$ is radical if and only if the quotient ring R/I is **reduced** i. e. has no nonzero nilpotent elements.

Exercise 1.7. Let $R = k[X_1, \dots, X_n]$ let $I \lhd R$ be a proper ideal. Show that $\sqrt{I}$ is equal to the intersection of all *maximal* ideals $\mathfrak{m} \lhd R$ containing I. *Hint:* think geometrically and use the Nullstellensatz.

Exercise 1.8. Show that the radical of an ideal $I \lhd R$ is equal of the intersection of all *prime* ideals $\mathfrak{p} \lhd R$ containing I. Show that for $R = k[X_1, \dots, X_n]$ finitely many ideals suffice. *Hint:* For the former Zorn's Lemma might be useful. For the latter: think geometrically.

Regular functions and morphisms. Duality of geometry and algebra

Exercise 1.9. Let $V \subseteq k^n$ be an affine algebraic set.

1. Show that $\mathcal{O}(V)$ is isomorphic as a k-algebra to $k[X_1, \dots, X_n]/\mathcal{I}_V$.
2. Assume that k is algebraically closed. How can homomorphisms of k-algebras $\mathcal{O}(V) \to k$ be interpreted geometrically? Is this intepretation still valid if $k = \mathbb{R}$?
3. Assume that k is algebraically closed. Describe how to see at the level of $\mathcal{O}(V)$ the follwoing properties: V is irreducible, V is finite, V is a point?

Exercise 1.10. Let R be a ring and let $I \trianglelefteq R$ be an ideal. Show that the following correspondence is a bijection.

$$\left\{\text{ideals } \widetilde{J} \trianglelefteq R/I\right\} \longleftrightarrow \{\text{ideals } J \trianglelefteq R \text{ such that } J \supseteq I\}$$
$$\widetilde{J} \longmapsto \pi^{-1}\left(\widetilde{J}\right)$$
$$\pi(J) \longleftarrow J$$

Show that under this correspondence prime (resp. maximal, resp. radical) ideals correspond to prime (resp. maximal, resp. radical) ideals. Use this to describe the ideals of $\mathcal{O}(V)$ geometrically.

Exercise 1.11. Show that the definition of f^* makes sense, i. e. that $\varphi \circ f \in \mathcal{O}(V)$ dla $\varphi \in \mathcal{O}(W)$ and that f^* is a homomorphism of k-algebras. Show that under the identification $\mathcal{O}(V) \cong k[X_1, \ldots, X_n]/\mathcal{I}_V$ the homomorphism f^* corresponds to the homomorphism od k-algebras

$$\widetilde{f} \colon k[X_1, \ldots, X_m]/\mathcal{I}_W \to k[X_1, \ldots, X_n]/\mathcal{I}_V$$

given by $\widetilde{f}\,(X_i + \mathcal{I}_W) = f_i + \mathcal{I}_V$ (first show that $\widetilde{f}$ is well-defined).

Exercise 1.12. Let $f \colon V \to W$ be a morphism of affine algebraic sets.

1. Show that f is injective if f^* is surjective and that the converse does not hold.
2. Show that the image of f is dense in W if and only if f^* in injective.

Exercise 1.13. Let V be an affine algebraic set. Make the following statement precise and then prove it: a choice of a finite tuple of generators of the k-algebra $\mathcal{O}(V)$ is the same as embedding V into an affine space.

Exercise 1.14. Let V be an affine algebraic set. Show that $\mathcal{O}(V)$ is reduced (vide: Exercise 1.6) finitely generated k-algebra and that each reduced finitely generated k-algebra is of the form $\mathcal{O}(W)$ for some affine algebraic set W.

Planar curves

Exercise 1.15. Let V be an affine algebraic set. Show that the following conditions are equivalent.

1. V is disconnected (as a topological space).
2. There exist some $f, g \in \mathcal{O}(V)$ such that $f^2 = f, g^2 = g, fg = 0, f + g = 1$.

Suggestion: It is good idea to try to understand (geometrically) what f and g should be e.g. by starting with the case when V is a disjoint sum of two lines.

Planar curves

An **affine planar curve** is a closed subset of k^2 all of whose irreducible components have dimension 1.

Exercise 1.16. Show that k^2 is two-dimensional by following the following plan.

1. Show that $\dim k^2 \geq 2$.

2. Prove that if $F, G \in k[X, Y] \setminus k$ are coprime then the set $V(F, G)$ is finite.

3. Show that if $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2$ a chain of prime ideals in $k[X, Y]$ then $\mathfrak{p}_0 = (0)$, $\mathfrak{p}_1$ generated by an irreducible polynomial and $\mathfrak{p}_2$ is maximal.

4. Deduce that $\dim k^2 = 2$.

Exercise 1.17. Deduce from 1.16 that planar curves are precisely the zero-sets of non-constant polynomials $F \in k[X, Y]$. When do two non-constant ideals $F, G \in k[X, Y]$ define the same planar curves? Describe the irreducible components of $V(F)$.

Exercise 1.18. Let $C = V(X^2 - Y^3) \subseteq k^2$ i niech $f\colon k \to k^2$ be the morphism $f(t) = (t^3, t^2)$. Check that the image of f is exactly C. Show that f is a bijective morphism $k \to C$ (even a homeomorphism) but not an isomorphism (i. e. f^{-1} is not a morphism).

2. Algebraically closed fields

Let us cast the very basic geometry developed so far into model-theoric terms. The less model-theoretically inclined reader should consults Appendix A for basic facts and definitions, if needed.

Notation 2.1. We consider the **language of rings** $\mathcal{L}_{\text{rng}}$ consisting of two constant symbols $0, 1$ and three binary function symbols $+, -, \cdot$. Every ring (and thus also every field) is a naturally an $\mathcal{L}_{\text{rng}}$-structure, with $0, 1, +, -, \cdot$ interpreted in the obvious way. The **theory of algebraically closed fields** ACF is the $\mathcal{L}_{\text{rng}}$-theory whose models are precisely algebraically closed fields (considered as $\mathcal{L}_{\text{rng}}$-structures as in the previous sentence). For p being a prime number or zero we can also consider the theory of algebraically closed fields of characteristic p. We denote this $\mathcal{L}_{\text{rng}}$-theory by ACF_p.

2.1. Quantifier elimination and its consequences

Definition 2.2. Let $\mathcal{L}$ be a language and let T be an $\mathcal{L}$-theory. We say that T **eliminates quantifiers** (or that T **admits quantifier elimination**) if for every $\mathcal{L}$ formula $\phi(\overline{x})$ there is a quantifier-free formula $\psi(\overline{x})$ such that $T \vdash \forall \overline{x}(\phi(\overline{x}) \leftrightarrow \psi(\overline{x}))$.

Remark 2.3. In Definition 2.2 it is enough to check $\phi(\overline{x})$ which are **existential** i. e. of the form $\exists \overline{y} \theta(\overline{x}, \overline{y})$ for some quantifier-free formula $\theta(\overline{x}, \overline{y})$.

There is a nice semantic criterion for quantifier elimination.

Fact 2.4. *Assume that $\mathcal{L}$ has at least one constant symbol and let $\phi(\overline{x})$ be an $\mathcal{L}$-formula. Then the following are equivalent.*

1. *There is a quantifier-free formula $\psi(\overline{x})$ such that $T \vdash \forall \overline{x}(\phi(\overline{x}) \leftrightarrow \psi(\overline{x}))$.*
2. *Assume M_1, M_2 are models of T and $N \subseteq M_1, M_2$ is a common $\mathcal{L}$-substructure. Then for any $a \in N$ we have $M_1 \models \psi(\overline{a})$ if and only if $M_2 \models \psi(\overline{a})$.*

Proposition 2.5. *The $\mathcal{L}_{\text{rng}}$-theory ACF_p eliminates quantifiers.*

Proof. We will use Fact 2.4 together with Remark 2.3. □

Corollary 2.6. *The theory ACF_p is model-complete, i. e. whenever $k \subseteq K$ is an extension of models of ACF_p we have $k \prec K$. Explicitely, for every $\mathcal{L}_{\text{rng}}(k)$-formula $\phi(\overline{x})$ and any tuple $\overline{a} \in k$ we have*

$$k \models \phi(\overline{a}) \text{ if and only if } K \models \phi(\overline{a}).$$

Proof. Thanks to Mr Mądrala (who pointed out that this is a future exercise in Ludomir's course) the reader is left to discover a proof by herself/himself (see Exercise 2.1). □

Model-completeness is an extremely useful property. Think about it - if you want to prove something about a tuple $\overline{a} \in k$ relative to your model k you can instead move to some model $K \supseteq k$ as big and fancy as you like (and are able to construct). Or the other way around: if k thinks some law holds in k, then K also adheres to that law. Of course we are limited to thinks expressible in first-order logic, but this is still a powerful property.

As an example we will use the above strategy to prove Hilbert's Nullstellensatz, as promised in the previous chapter.

Theorem 2.7 (Hilbert's Nullstellensatz). *Let k be an algebraically closed field and let $I \trianglelefteq k[X_1, \ldots, X_n]$ be an ideal. Then $\mathcal{I}_{V(I)} = \sqrt{I}$.*

Proof. It is easy to check that $\mathcal{I}_{V(I)} \supseteq \sqrt{I}$ so let us prove the reverse inclusion. Take $f \in \mathcal{I}_{V(I)}$. By Exercise 1.8 we know that $\sqrt{I}$ is the intersection of all prime ideals $\mathfrak{p}$ containing I, so let us fix a prime ideal $\mathfrak{p} \supseteq I$ and let us show that $f \in \mathfrak{p}$. Since $\mathfrak{p}$ is a prime ideal, the quotient ring $R = k[X_1, \ldots, X_n]/\mathfrak{p}$ is a domain, so we can form its field of fractions R_0, which in turn has an algebraic closure $K \supseteq R_0$. Note that $k \subseteq R \subseteq K$. Fix a set of generators $g_1, \ldots, g_m$ of $I \trianglelefteq k[X_1, \ldots, X_n]$. Unwinding the meaning of "$f \in \mathcal{I}_{V(I)}$"[1] we can translate it into the following statement:

$$k \models (\forall \overline{x}) \left(g_1(\overline{x}) = \ldots = g_m(\overline{x}) = 0 \implies f(\overline{x}) = 0\right).$$

Since $k \subseteq K$ we have by 2.6 that K has to think the same about $g_1, \ldots, g_m, f$! That is

$$K \models (\forall \overline{x}) \left(g_1(\overline{x}) = \ldots = g_m(\overline{x}) = 0 \implies f(\overline{x}) = 0\right). \qquad (\heartsuit)$$

Let us apply the above for $\overline{x}$ set to $\overline{a} = (X_1 + \mathfrak{p}, \ldots, X_n + \mathfrak{p}) \in K^n$. Using intensive staring we see that quite tautologically we have

$$h(\overline{a}) = h + \mathfrak{p}$$

for any $h \in k[X_1, \ldots, X_n]$, in particular we get for $i = 1, \ldots, n$

$$g_i(\overline{a}) = g_i + \mathfrak{p} = 0_K$$

because $g_i \in I \subseteq \mathfrak{p}$. By $(\heartsuit)$ we have that $f(\overline{a}) = 0$, so again by starring we have

$$f + \mathfrak{p} = f(\overline{a}) = 0_K$$

hence $f \in \mathfrak{p}$ as desired. □

Recall that an $\mathcal{L}$-theory T is **complete** if for any $\mathcal{L}$-sentence θ we have that $T \models \theta$ or $T \models \neg\theta$. This is equivalent to saying that all models of T have the same opinion abut θ, i.e. *either* for all $M \models T$ we have $M \models \theta$ *or* for all $M \models T$ we have $M \models \neg\theta$.

Corollary 2.8. *The theory* ACF_p *is complete.*

Proof. Let $\mathbb{F}$ be the prime field of characteristic p (i. e. the field $\mathbb{F}_p$ with p elements if $p > 0$ and $\mathbb{Q}$ if $p = 0$). Let $K_1, K_2 \models \mathrm{ACF}_p$. Let θ be any $\mathcal{L}_{\mathrm{rng}}$-sentence. By Fact 2.4 for

$$M_1 = K_1, M_2 = K_2, N = \mathbb{F}$$

we get that $M_1 \models \theta$ if and only if $M_2 \models \theta$. This means that any model of ACF_p has the same opinion about θ, thus ACF_p is complete. □

Quantifier elimination of ACF_p has a natural geometric intepretation. For this we need to introduce the following terminology.

Definition 2.9. Let X be a noetherian space and let $Y \subset X$. We say that Y is **constructible** if it is a boolean combination of closed subsets of X.

Remark 2.10. Note that in the case $X = k^n$ constructible sets are precisely the quantifier-free definable subsets of k^n (see also Exercise 2.4). Proposition 2.5 can be thus stated as: the definable sets in ACF are precisely the constructible sets.

[1] "If $\overline{a} \in k^n$ is a zero of every element of I, the $\overline{a}$ is also a zero of f".

Corollary 2.11 (Chevalley's Theorem). *Let $f: V \to W$ be a morphism of affine algebraic sets. Then for any constructible set $U \subseteq V$ its image $f(U)$ is a constructible subset of W.*

Remark 2.12. It turns out that algebraically closed fields are the only field which eliminate quantifiers in the language $\mathcal{L}_{\text{rng}}$ (see Exercise 2.4). One might ask whether there are interesting examples of fields which eliminate quantifiers after naming some specific definable sets. There is a construction called the morleyization of a theory which achieves this almost tautologically for any theory, but in our context it is hardly interesting. A more natural example is the theory of $(\mathbb{R}, +, -, \cdot, 0, 1, \geq)$. The ordering relation $x \leq y$ on $\mathbb{R}$ is definable in the field-language via the formula $(\exists z)\,(y - x = z^2)$. This means that adding $\leq$ to the language adds no new definable sets, but it turns out that it yields quantifier elimination. One may say that $(\exists z)\,(y - x = z^2)$ is essentially the only non-eliminable existential formula.

2.2. Fields of definition

For convenience **we assume in this section that k is an algebraically closed of characteristic zero.** The positive characteristic case is not much different, but the slight additional inconviniences might disturb the presentation. Some examples of positive characteristic quirks are discussed in the exercises.

Definition 2.13. Let $k_0 \subseteq k$ be a subfield, not neccesarily algebraically closed. We say that an affine algebraic set $V \subseteq k^n$ is **defined over** k_0 if the $\mathcal{I}_V$ can be generated by polynomials $f_1, \dots f_n$ with coefficients in k_0. In this situation we may also say that V is k_0**-closed.** We say that V is k_0**-irreducible** (or a k_0**-variety**).

Example 2.14 (Somewhat stupid, but it delivers a point)**.** Let us work with $k = \mathbb{C}$. The variety $V = V(\pi X - \pi Y)$ is defined over $\mathbb{R}$ and $\mathbb{Q}(\pi)$ but also over $\mathbb{Q}$. A fortiori $\mathbb{Q}$ is the smallest field over which V is defined. The variety $W = V(X - \sqrt{2}Y)$ is defined over $\mathbb{C}$, $\mathbb{R}$ and $\mathbb{Q}[\sqrt{2}]$, but not over $\mathbb{Q}(\sqrt[3]{17})$. In fact in can be checked that $\mathbb{Q}[\sqrt{2}]$ is the smallest field over which W is defined.

In the above example V and W both admit smallest field over which they are defined. It is not particulary suprising as these are varieties defined by very simple equations. One might suspect that for more complicated algebraic sets V there are maybe several minimal fields k_0 over which V is defined, or that maybe therea are no minimal ones at all. The following result of Weil proves doubters wrong: there is always a smallest field k_V over which V is defined. This is stricking! It implies in particular that if you can defined V using polynomials over a field k_1 and a field k_2, then you can define V using polynomials over $k_1 \cap k_2$.

Definition 2.15. Let V be an affine algebraic set. We call a field $k_V \subseteq k$ the **field of definition** of V if k_V is the smallest field over which V is defined.

It is absolutely unclear that fields of definitions exists, but we will prove that they do. Before doing so, let us note the following property.

Lemma 2.16. *Let V be an affine algebraic set. If the field of definitions k_V of V exists, then it is finitely generated (as a field over $\mathbb{Q}$).*

Proof. See Exercise 2.15. □

Lemma 2.16 will also follow directly from our construction of k_V (see Theorem 2.20), but it is good to notice that it is true by general reasons.

Now time for an auxilliary lemma, for which we need a piece of notation.

Notation 2.17. Let σ Aut(k) be any field automorphism. Such σ naturally induces a bijection on k^n, which we also denote by σ. Moreover σ induces an automorphism of $k[X_1, \dots, X_n]$ by acting on k by σ and fixing $X_1, \dots, X_n$, and by abuse of notation we denote it also by σ.

Remark 2.18. It is easy to see that for an affine algebraic set V and an automorphism σ Aut(k) we have that $\sigma(V)$ is also an affine algebraic set. Moreover $\mathcal{I}_{\sigma(V)} = \sigma(\mathcal{I}_V)$. In particular $\sigma(V) = V$ if and only if $\sigma(\mathcal{I}_V) = \mathcal{I}_V$.

Lemma 2.19. *Let V be an affine algebraic set and let k_0 be a field over which V is defined. Assume that for any $\sigma \in \mathrm{Aut}(k)$ we have $\sigma|_{k_0} = \mathrm{id}_{k_0}$ if and only if $\sigma(V) = V$. Then k_0 is the field of definition of V.*

Proof. We have to check that whenever $k_1 \subseteq k$ is a field over V is defined then $k_0 \subseteq k_1$. By Galois theory in order to show $k_0 \subseteq k_1$ it is enough to show that any $\sigma \in \mathrm{Aut}(k)$ which fixes k_1 pointwise fixes also k_0.[2] So take $\sigma \in \mathrm{Aut}(k)$ which fixes k_1 pointwise. Since V is defined over k_1 we have $\sigma(V) = V$ so by assumption $\sigma|_{k_0} = \mathrm{id}_{k_0}$ as desired. □

Theorem 2.20. *Every affine algebraic set V admits a field of definition k_V.*

Proof. Denote by $I = \mathcal{I}_V$ the vanishing ideal of V. The ring $R := k[X_1, \dots, X_n]$ is a k-vector space and the set of all monomials (in variables $X_1, \dots, X_n$) is a basis of R over k. Let $(m_i \colon i < \omega)$ be an enumeration of all monomials. The quotient R/I is also a k-vector space and the elements $m_0 + I, m_1 + I, \dots$ span R/I, so we may choose a subsequence $(b_j \colon j < \omega)$ of $(m_i \colon i < \omega)$ such that $b_0 + I, b_1 + I, \dots$ is a basis of R/I. For every $i < \omega$ let $\alpha_i^0, \alpha_i^1, \dots \in k$ be the coordinates of $m_i + I$ relative to this basis, i.e. for big enough $j < \omega$ we have $\alpha_i^j = 0$ and

$$m_i + I = \sum_{j<\omega} \alpha_i^j b_j + I.$$

Let k_V be the field generated by all the coefficients α_i^j for $i, j < \omega$. We will prove that k_V satisfies the assumptions of Lemma 2.19 from which it will follows that k_V is the field of definition of V. Define $f_i := m_i - \sum_{j<\omega} \alpha_i^j b_j \in I$.

Claim 1. V is defined over k_V. More precisely, $\mathcal{I}_V$ is generated by $f_0, f_1, \dots$.

$\vdash$ Take first any $f \in R$ and write $f = \sum_{i<\omega} \beta^i m_i$ (here upper i is a superscript, not exponentiation). We have

$$f + I = \sum_{i<\omega} \beta^i \sum_{j<\omega} \alpha_i^j b_j + I = \sum_{j<\omega} \left(\sum_{i<\omega} \beta^i \alpha_i^j \right) b_j$$

thus $f \in I$ exactly when $\sum_{i<\omega} \beta^i \alpha_i^j$ for all $j < \omega$. But then

$$\sum_{i<\omega} \beta^i f_i = \sum_{i<\omega} \beta^i \left(m_i - \sum_{j<\omega} \alpha_i^j b_j \right) = \dots = \sum_{i<\omega} \beta^i m_i = f,$$

as desired. $\dashv$

Claim 2. For any $\sigma \in \mathrm{Aut}(k)$ we have $\sigma|_{k_V} = \mathrm{id}_{k_V}$ if and only if $\sigma(V) = V$.

$\vdash$ The "only if" part holds simply because V is defined over k_V by Claim 1. For the "if" part, assume $\sigma \in \mathrm{Aut}(k)$ fixes V setwise. We want to show $\sigma|_{k_V} = \mathrm{id}_{k_V}$, i.e. that $\sigma\left(\alpha_i^j\right) = \alpha_i^j$ for all $i, j < \omega$. Since $\sigma(V) = V$ we have $\sigma(I) = I$... $\dashv$

Claim 1 and Claim 2 mean that k_V satisfy the assumptions of Lemma 2.19, hence by this lemma we have that k_V is the field of definition of V. □

[2]Here we use our assumption that k has characteristic zero - otherwise we would need to care about separability.

Corollary 2.21. *For any affine algebraic set V there is a finite tuple $\bar{c} \in k$ such that an automorphism $\sigma \in \mathrm{Aut}(k)$ fixes V setwise if and only if σ fixes $\bar{c}$ pointwise.*

Proof. Let k_V be the field of definition of V, which exists by Theorem 2.20. By Lemma 2.16 there is some finite tuple $\bar{c}$ such that $k_V = \mathbb{Q}(\bar{c})$. Clearly $\sigma \in \mathrm{Aut}(k)$ fixes k_V pointwise if and only if it fixes $\bar{c}$, so Lemma 2.19 the proof is finished. □

Remark 2.22. Essentially the same proof as in Theorem 2.20 and Corollary 2.21 gives the following: every ideal of the ring $R = k[X_1, \ldots, X_n, \ldots]$ of polynomials in infinitely many variables admits a field of definition. We leave it to the reader to make this statement precise and supply a proof.

Corollary 2.21 motivates the following definition.

Definition 2.23. Let T be an $\mathcal{L}$-theory, let $M \models T$ be a sufficiently saturated model, X a definable set in M and $\bar{c} \in M$ a tuple. We say that $\bar{c}$ is a **canonical parameter for** X (or a **code for** X) if any automorphism $\sigma \in \mathrm{Aut}(k)$ fixes X setwise if and only if σ fixes $\bar{c}$ pointwise.

The name "canonical parameter" is explained by the following result.

Lemma 2.24. *Let T be a $\mathcal{L}$-theory, let M be a sufficiently saturated model of T, let X be a definable set in M and let $\bar{c} \in M$ be a tuple. Then the following conditions are equivalent.*

1. *$\bar{c}$ is a canonical parameter of X*
2. *There exists an $\mathcal{L}$-formula $\phi(x, y)$ such that $X = \phi(M, \bar{c})$ and whenever $\bar{c}' \neq \bar{c}$ we have $X = \phi(M, \bar{c}')$*

Proof. See Exercise 2.14. □

So a *canonical parameter* for X is a tuple $\bar{c}$ which appears as a *parameter* in a formula defining X and in this formula only using $\bar{c}$ as parameters results in X (so in a way tuple $\bar{c}$ is *canonical*).

Corollary 2.25. *Every definable set in* ACF_0 *has a code.*

Proof. We know that two things:

1. Zariski closed sets have codes by Corollary 2.21.
2. The definable sets in ACF_0 are precisely the locally constructible sets (see Remark 2.10), so are boolean combinations of Zariski closed sets.

One can combine these two facts to show that every definable set in ACF_0 has a code (which is the content of Exercise 2.16). □

2.3. Imaginaries and how to eliminate them

Equivalence relations and quotient set are all over the place in mathematics. If X is a definable set in some model M and E is a definable equivalence on X then the quotient set X/E is something that M sees and can touch but it is not directly a definable set. *Elimination of imaginaries* is the ability to treat X/E like a definable set.

Definition 2.26. We say that an a structure M **eliminates imaginaries** (or **admits elimination of imaginaries**) if for every $n < \omega$ and every 0-definable equivalence relation E on M^n there is some $k < \omega$ and a 0-definable map $f_E \colon M^n \to M^k$ such that for $a, b \in M^n$ we have aEb if and only if $f_E(a) = f_E(b)$. We say that a theory T **eliminates imaginaries** (or **admits elimination of imaginaries**) if every model of T eliminates imaginaries.

Intuitively, the function f expresses the quotient set M^n/E as a bona fide definable set $f(X) \subseteq M^k$.

Example 2.27. We work in $k \models \mathrm{ACF}_0$. Let E be the equivalence relation on k^2 defined via the formula

$$(x_1, x_2)\, E\, (y_1, y_2) \iff \{x_1, x_2\} = \{y_1, y_2\}$$

which is easily seen to be definable. Set $f \colon k^2 \to k^2$ as $f(a, b) = (a + b, ab)$. By kindergarten algebra we have that $\{a_1, a_2\} = \{b_1, b_2\}$ if and only if $f(a_1, a_2) = f(b_1, b_2)$.

Remark 2.28. It is easy to see that if T is complete then it is enough to check the conditions from Definition 2.26 for a single model $M \models T$ (see Exercise 2.10).

Lemma 2.29. *Assume that T eliminates imaginaries. Then every definable set has a code.*

Proof. ($\Longleftarrow$) Let $E(x, y)$ be a formula defining an equivalence relation on a definable set X

$$E(x, y)$$

($\Longrightarrow$) Assume that T eliminates imaginaries and let X be a definable set defined by a formula $\phi(x, \overline{a})$, where $\overline{a} \in M^n$. Let $E \subseteq M^n \times M^n$ be the equivalence relation defined via the formula

$$\theta(y_1, y_2) := (\forall x)\, (\phi(x, y_1) \longleftrightarrow \phi(x, y_2))$$

or in other words $\overline{a}_1 E \overline{a}_2$ exactly when $\phi(x, \overline{a}_1)$ and $\phi(x, \overline{a}_2)$ define the same set. Since T eliminates imaginaries there is some $k < \omega$ and a 0- definable function $f_E \colon \to Y$ such that

$$\overline{a}_1 E \overline{a}_2 \text{ if and only if } f(\overline{a}_1) = f(\overline{a}_2)$$

for all $\overline{a}_1, \overline{a}_2 \in \mathcal{U}$. It is now easy to check that $\overline{c} := f(\overline{a})$ is a code for X. □

Lemma 2.30. *Assume that $\mathcal{L}$ contains at least two constant symbols c_1, c_2 and $T \models c_1 \neq c_2$. Then T eliminates imaginaries if and only if every definable set in T has a code.*

Proof. See Exercise 2.12. □

Combining Lemma 2.30 with Corollary 2.25 yields the following.

Proposition 2.31. *The theory* ACF *eliminates imaginaries.*

2.4. Types

Recall the following.

Definition 2.32. A **partial type over A in variables $\overline{x}$** is simply a set of $\mathcal{L}(A)$-formulas in variables $\overline{x}$. A partial type $\pi(\overline{x})$ is **consistent** if for any finitely many formulas $\phi_1(\overline{x}), \ldots, \phi_n(\overline{x}) \in \pi(\overline{x})$ there is some $\overline{a} \in M$ such that $M \models \bigwedge_{i=1}^{n} \phi_i(\overline{a})$. A type $\pi(\overline{x})$ over A is **complete** it is consistent and for any $\mathcal{L}(A)$-formula $\phi(\overline{x})$ we have $\phi(\overline{x}) \in \pi(\overline{x})$ or $\neg\phi(\overline{x}) \in \pi(\overline{x})$.

You may think of a complete type as descriptions of an *ideal element* of M. See Appendix A for more on types.

Definition 2.33. Let $k_0 \subseteq k$ be a field and let $V \subseteq k^n$ be an affine k_0-variety. The **generic type of V over k_0** is the type $p_{V,k_0}(x) \in S_n(k_0)$ saying "I am in V but in no proper k_0-subvariety of V".

Proposition 2.34. *Every complete n-type over k_0 is the generic type of a unique k_0-variety V.*

Proof. Uniqueness is left as an easy exercise (see Exercise 2.6), so let us focus on existence. Let $p \in S_n(k_0)$ be a type and let $\mathcal{F}$ be the family of all k_0-closed sets on which p concentrates. Since p is a type, the family $\mathcal{F}$ has the finite intersection property. The intersection $V := \bigcap \mathcal{F}$ is thus a Zariski closed and clearly p concentrates on V. Moreover, V is k_0-irreducile: if $V = V_1 \cup V_2$ for some k_0-closed subsets $V_1, V_2 \subseteq V$ then p (being complete) has to concentrate on V_1 or V_2 and thus by minimality of V we have that $V_1 = V$ or $V_2 = V$. □

By the above proposition the following definition makes sense.

Definition 2.35. The **dimension of a complete type** $p \in S_n(k_0)$ is the dimension of the unique k_0-variety V for which $p = p_{V,k_0}$.

Definition 2.36. Let $k_0 \subseteq k_1$ be subfields of k, let $p \in S_n(k_0)$ be a complete type of k_0 and let $q \in S_n(k_1)$ be an extension of p (i.e. $q \supseteq p$). We say that q is a **forking extension** (or that the extension $p \subseteq q$ forks).

One should think that a non-forking extension q of p is a "free extension", in a sense that it imposes no significantly new restrictions. [3].

2.5. Two remarks on dimension

Fact 2.37. *The dimension of an affine variety V is equal to the transcendence degree of $k(V)$ over V.*

Lemma 2.38. *Work in $k \models$ ACF. Then a definable set V has dimension $\geq n + 1$ if and only if there disjoint definable sets $V_1, V_2, \ldots \subseteq V$, each of dimension $\geq n$.*

Proof. See Exercise 2.5. □

Note that Lemma 2.38 allows us to define dimension of definable sets in ACF without refering to the Zariski topology.[4]

Comments

Marker's book [1] has a nice introduction to the model theory of ACF (Chapter 3, Section 3.2). His approach to elimination of imaginaries is different and does not mention fields of definition. The proof of Proposition 2.20 (first proven by Weil) is taken from Poizat's paper [2], where he introduced the notion of elimination of imaginaries.

Not every theory T eliminates imaginaries (see Exercise 2.17 for a concrete example), but there is a canonical construction way to "expand" T to a theory T^{eq} in a bigger language $\mathcal{L}_T^{\mathrm{eq}}$, so that any model

[3] Model-theorists are peculiar creatures and they name desired properties by negating an undesired property. Because of this we have "non-forking", "not the independece property", "no finite cover property" and so on.

[4] We just invented the Morley rank!

1. $M \models T$ extends uniquely to a model $M^{\text{eq}} \models T^{\text{eq}}$.
2. All definable subsets of M inside M^{eq} are already definable in M.
3. M^{eq} eliminates imaginaries.

Essentially for every 0-definable equivalence relation E we add to M new elements corresponding to E-classes.

Exercises

Unless said otherwise, k is an algebraically closed field of characteristic zero and types, definable sets *et cetera* are considered in the theory ACF and its models.

Some basic properties of ACF

Exercise 2.1. Show that the theory ACF is model complete.

Exercise 2.2. The **Lefschetz Principle** is a rule of thumb saying that whatever hold in algebraic geometry over $\mathbb{C}$ should hold over all algebraically closed fields, at least of sufficiently large characteristic. This might be formalized, which is the goal of this exercise. For an $\mathcal{L}_{\text{rng}}$-sentence ϕ show that the following conditions are equivalent.

1. $\text{ACF}_0 \models \phi$.
2. $\text{ACF}_p \models \phi$ for all sufficiently large p.
3. $\text{ACF}_p \models \phi$ for infinitely many p.

Note that we might in the above $\overline{\mathbb{F}_p} \models \phi$ instead of $\text{ACF}_p \models \phi$ and $\mathbb{C} \models \phi$ instead of $\text{ACF}_0 \models \phi$.

Exercise 2.3. Prove the following fact (called sometimes the **Ax-Grothendieck theorem**): if $f\colon \mathbb{C}^n \to \mathbb{C}^n$ in an injective polynomial map, then f is surjective. *Hint:* Use the previous exercise.

Exercise 2.4. We want to explore quantifier-elimination in fields.

1. Show that over any field k (considered in the language $\mathcal{L}_{\text{rng}}$, as always) the constructible subsets of k^n coincide with quantifier-free definable subsets.
2. Show that the statement of the Chevalley Theorem for a field k is equivalent to quantifier-elimination in k.
3. Given an example of a field k which does not eliminate quantifiers in $\mathcal{L}_{\text{rng}}$. In particular, the Chevalley Theorem has to fail in k.[5]
4. $(*)$ Show that a field admiting quantifier elimination in the language $\mathcal{L}_{\text{rng}}$ is algebraically closed. *Warning:* This might be hard or borderline impossible to solve with the theory we have developed till now. After learning some ω-stability theory we will be able to prove a more general statement.

Exercise 2.5. Show that a definable set V has dimension $\geq n+1$ if and only if there disjoint definable sets $V_1, V_2, \ldots \subseteq V$, each of dimension $\geq n$.

[5]More precisely, the naive version of Chevalley's theorem fails for k; the scheme-theoretic version is valid over any field.

Types in ACF

Exercise 2.6. Let $V, W \subseteq k^n$ be k_0-varieties such that $p_{V,k_0} = p_{W,k_0}$. Show that $V = W$.

Exercise 2.7. Let $a \in k^n$ and set $p = \operatorname{tp}(a/k_0)$. From the lecture we know that there is a k_0-variety V such that $p = p_{V,k_0}$. Describe V directly in terms of a.

Exercise 2.8. Show that $p \in S_n(k_0)$ is equal to the largest number k for which there is a chain of extensions of complete types $p_0 \subseteq p_1 \subseteq \ldots \subseteq p_m$ where $p_0 = p$ and for each $i = 0, \ldots, m-1$ the extension $p_i \subseteq p_{i+1}$ forks.

Exercise 2.9. Describe the Stone topology on the space of types $S_n(k)$. Is there any connection to geometry?

Imaginaries

Exercise 2.10. Assume that T is a complete theory. Show that T eliminates imaginaries if and only if some model of T does so.

Exercise 2.11. *(An extension of Example 2.27)* Describe how to treat finite sets (of a given cardinality) as imaginary elements. Give a recipe how to eliminate them in the theory of fields.

Exercise 2.12. Let $\mathcal{L}$ be a language and let T be an $\mathcal{L}$-theory. Assume that $\mathcal{L}$ contains at least two constant symbols c_1, c_2 and that $T \models c_1 \neq c_2$. Show that T eliminates imaginaries if and only if every definable set in T has a code.

Exercise 2.13 (A good reason for eliminating imaginaries)**.** Let us introduce the following local definition: we say that a theory T **defines sections** if every surjective map $f\colon X \to Y$ admits a definable section, i.e. a definable map $g\colon Y \to X$ such that $f \circ g = \mathrm{id}_Y$.[6]

1. Show that if T defines sections then T eliminates imaginaries.
2. Show that ACF does not define sections. In particular, the converse of the previous item does not hold.

Exercise 2.14. Let T be a $\mathcal{L}$-theory and let M be a sufficiently saturated model of T. Let X be a definable set in M and let $\bar{c}$ be a tuple. Prove that the following conditions are equivalent.

1. $\bar{c}$ is a canonical parameter of X
2. There exists an $\mathcal{L}$-formula $\phi(x, y)$ such that $X = \phi(M, \bar{c})$ and whenever $\bar{c}' \neq \bar{c}$ we have $X = \phi(M, \bar{c}')$

Exercise 2.15. Let V be an affine algebraic set.

1. Let $K \subseteq L \subset M$ be a tower of field extensions. Show that if M is finitely generated over K, then L is finitely generated over K.
2. Show that the field of definition of V is finitely generated over $\mathbb{Q}$ without refering to a direct construction of k_V.

Exercise 2.16. Show that every definable set in ACF_0 has a code.

[6]The theory of $\mathbb{R}$ as an ordered field has this property. More generally, o-minimal theories define sections.

Exercise 2.17. Let K be a field. The theory of vector spaces over K is defined as follows. We define a language $\mathcal{L}$ consisting of a constant symbol 0, a binary function symbol $+$ and for each $r \in K$ a unary function symbol λ_r. If V is a vector space over K, then we consider it as an $\mathcal{L}$-structure as follows: 0 and $+$ have a guessable interpretation and λ_r for $r \in K$ is intepreted as the scalar multiplication $\lambda_r(v) = r \cdot v$.

Now, let K be a finite field with at least 3 element and let T be the theory of infinite K-vector spaces. Show that T does not eliminate imaginaries.

3. Differential fields

3.1. Basic differential algebra

Definition 3.1. Let R be a ring. A **derivation on** R is an additive map $\delta\colon R \to R$ such that

$$\delta(xy) = \delta(x)y + x\delta(y)$$

for all $x, y \in R$. In such situation we call the pair (R, δ) a **differential ring.**

Lemma 3.2. *Let (R, δ) be a differential ring, $x \in R$ and $n < \omega$. Then $\delta\left(x^{n+1}\right) = (n+1)x^n$. If moreover $y \in R$ is invertible, then $\delta\left(\frac{x}{y}\right) = \frac{\delta(x)y - x\delta(y)}{y^2}$*

Proof. The first identity follows from an easy inductive argument and the second one follows from applying Leibniz' rule to $\delta(x) = \delta\left(y \cdot \frac{x}{y}\right)$. □

By the typical abuse of notation we will ignore δ in the notation and simply write e.g. "let R be a differential ring". From now on we fix a differential ring (R, δ).

Definition 3.3. Let $I \trianglelefteq R$. We say that I is a **differential ideal** of R (and write $I \trianglelefteq^{\delta} R$) if for every $x \in R$ we have $\delta(x) \in R$.

Remark 3.4. If $I \trianglelefteq^{\delta} R$ then the quotient ring R/I is equipped with a natural derivation $\widetilde{\delta}\colon R/I \to R/I$ (well) defined as

$$\widetilde{\delta}\,(x + I) = \delta(x) + I$$

for $x \in I$. The quotient map $\pi\colon R \to R/I$ is a differential homomorphism.

Definition 3.5. The **ring of differential polynomials** $R\{X\}$ is defined as follows. As a pure ring $R\{X\}$ is the ring of polynomials over R in countably many variables $X^{(0)}, X^{(1)}, \ldots, X^{(n)}, \ldots$ and we equipp it with the unique derivation $\widetilde{\delta}\colon R\{X\} \to R\{X\}$

Theorem 3.6. *Let R be a Ritt-Noetharian differential $\mathbb{Q}$-algebra. Then $R\{X\}$ is also Ritt-Noetherian.*

Corollary 3.7. *If K is a differential field, then the ring of $K\{X_1, \ldots, X_n\}$ is Ritt-Noetherian for any $n < \omega$.*

3.2. Differential fields

Let (K, δ) be a differential field of characteristic zero.

Lemma 3.8. *The field of constants C_K is a field and moreover C_K is **relatively algebraically closed** in K, i.e. whenever $a \in K$ is algebraic over C_K we have that $a \in C_K$.*

Proof. Let $a \in K$ be algebraic over C_K with minimal polynomial $f \in C_K[X]$.
Thus... □

Remark 3.9. Lemma 3.8 as stated is false in characteristic $p > 0$, since by Lemma 3.2 we have $K^p \subseteq C_K$. It is however true that C_K is relatively *separably* closed in K and this can be proven in the same manner as Lemma 3.8.

Definition 3.10. Let $I \subseteq K\{X_1, \ldots, X_n\}$. We define the **vanishing set of** I as

$$V^\delta(I) = \{\overline{a} \in K^n | f(a) = 0 \text{ for all } f \in I\}$$

A **Kolchin closed set** is a set of the form $V^\delta(I)$ for some I.

Remark 3.11.

The above results allows us to formulate the following (surely very suprising) definition.

Definition 3.12. The **Kolchin topology** on K^n is the topology on K^n whose closed sets are precisely the Kolchin closed subsets of K^n.

As in the case of case of the Zariski topology we have the following interpretation of Theorem 3.6.

Corollary 3.13. *The Kolchin topology is Noetherian.*

Proof. □

Definition 3.14. Let $k \subseteq K$ be a differential field and let $a \in K$. There are two possibilities

1. For some $n < \omega$ the element $\delta^n a$ is algebraic over the (pure) field $k(\delta^{<n} a)$ or
2. The sequence $a, \delta a, \delta^2 a, \ldots$ is algebraically independent over k.

In the first case we say that a is **differentially algebraic over** k and in the second case we say that a (or the field $k < x >$) is **differentially transcendental over** k over k. If a is differentially algebraic over k then we call the smallest n for which (1) holds the **order of** a **over k**.

Lemma 3.15. *Let $a \in K$ be differentially algebraic over k and let n be the order of a over k. Then $k < a >= k(\delta^{\leq n} a) = k(\delta^{<n} a)[\delta^n a]$.*

Remark 3.16.

3.3. Differentially closed fields

Definition 3.17. We define the **language of differential rings** as the language $\mathcal{L}_\delta = \mathcal{L}_{\text{rng}} \cup \{\delta\}$ where δ is a unary functional symbol. We treat any differential ring as an $\mathcal{L}_\delta$–structure in any obvious manner.

Definition 3.18. We say that a differential field (K, δ) is **differentially closed** if the following condition holds:

sdasda

Remark 3.19. The name "differentially *closed* fields" might be a bit misleading for the following reason. Whenever $f \in K\{X\}$ is a differential polynomial of order at least one (i.e. f is not an ordinary polynomial) there exists a differential field extension $K \subseteq L$ and $a \in L \setminus K$ for which $f(a) = 0$ – that is (proper) differential equations can (and will) attain new solutions in extensions.

At this point we do not even now whether there are any differentially closed fields. The following results shows that they do in fact exist and more over every differential field sits inside a differentially closed one.

Lemma 3.20. *Any differential field extends to a differentially closed field.*

Proof. Let (K, δ) be a differential field. It is enough to construct for any K-pair (f, g) an extension $K \subset L$ in which (f, g) has a solution: if we manage to do that, then by iterating it transfinitely many times we can construct a differentially closed extension of K. □

Lemma 3.21. *Let K_1, K_2 be ω-saturated differentially closed fields, let k be a common differential subfield of K_1, K_2 and let $a \in K_1$. Then there is a differential embedding $\sigma\colon k\langle a\rangle \to K_2$ over k (i.e. fixing k pointwise).*

Proof. □

Proposition 3.22. *The theory* DCF_0 *eliminates quantifiers.*

Proof. We will use the semantic criterion ... Possibly passing to an elementary extension we may assume that K_1, K_2 are ω-saturated. □

Again just as in the case of ACF_p we get the following consequence of Proposition 3.22...

Corollary 3.23. *The theory* DCF_0 *is complete and model complete.*

Proof. Model completeness follows from quantifier elimination. Regarding completeness, it is enough to notice that $\mathbb{Q}$ equipped with the trivial derivation is a common substructure of all differential fields of characteristic zero. □

...and model completeness together with Lemma 3.20 immediately yields the following.

Corollary 3.24 (The Differential Nullstellensatz)**.** *Let $K \models \mathrm{DCF}_0$ and let Σ be a finite set of differential equations over K, which has a solution in some differential extension $L \supseteq K$.*

3.4. Types in DCF_0

From now on we work in a differentially closed field $(\mathcal{U}, \delta)$ which is moreover **ω_1-saturated**, i.e. any consistent type over a countable set of parameters $A \subseteq \mathcal{U}$ is realized in $\mathcal{U}$. By default sets of parameters are algebraically closed countable differential subfields of $\mathcal{U}$, typically denoted k, k' and so on. We denote by $\mathcal{C}$ the field of constants of $\mathcal{U}$.

Remark 3.25. $\mathcal{U}$ serves as a "universal domain" for differential algebra here, a sort of big enough playground. It is "just" a convinient device and all meaningful results should not depend on the choice of $\mathcal{U}$. In model theory such an object is typically called a **monster model** though these are usually *much* bigger.

Quantifier elimination in ACF yields to a geometric description of types using the Zariski topology. The same spiel happens with DCF_0 and the Kolchin topology.

Definition 3.26. Let X be a differential k-variety. The **generic type of X over k** is the complete n-type over k saying "I am in X but in no proper Kolchin k-closed subset of X".

Remark 3.27. We will sometimes talk about generic types (over some k) of equations Σ. By this we mean the following: take the differential algebraic set X defined by the Σ, pick a k-component X_0 of X and take the generic type of X_0 over k.

Corollary 3.28. *Let $p \in S_n(k)$ where k is a (countable) differential subfield of $\mathcal{U}$. Then there exists a unique differential k-variety $X \subseteq \mathcal{U}^n$*

Proof. See Exercise 3.3 □

Definition 3.29. A definable set $X \subseteq \mathcal{U}^n$ is called **finite-dimensional** if there is some constant N such that for any trdeg()... A formula $\varphi(x)$ is **finite-dimensional** if the set $X = \varphi(\mathcal{U})$ is finite-dimensional. A type $p \in S_n(k)$ is **finite-dimensional** if it contains a finite-dimensional formula.

It is easy to see that the generic type of a differential k-variety of X is finite-dimensional if and only if X is finite-dimensional.

Remark 3.30. We defined being finite-dimensional while not defining dimension at all - funny, isn't it? There are several meaningful notions of dimension for types in DCF_0...

Definition 3.31. A type $p \in S_n(k)$ is **internal to $\mathcal{C}$** (or **internal to the constants**) if for some (equivalenty: all) $a \models p$ there are $b \mathop{\smile\!\!\!\!\!\;|}_k a$ and $c \in \mathcal{C}$ such that $a \in k\langle b, d\rangle$.

The idea of internality is the following: there is a definable function f such that

Example 3.32. Pick any $r \in \mathcal{U}$ and let p be the generic type of the equation $x' = rx$ over some $k \ni r$.

The following is the first serious theorem in this notes. It is the heart of the model-theoretic proof of the Mordell-Lang theorem, which we will discuss soon. We postpone the proof of Theorem 3.33 to Section 3.7, as we will need to develop some machinery first.

Theorem 3.33 (The Canonical Base Property for DCF_0)**.** *Fix two countable algebraically closed differential fields $k \subseteq k'$ Let p be a finite-dimensional type over k, let $a \models p$ and let c be the canonical base of* $\mathrm{tp}(a/k')$. *Then* $\mathrm{tp}(c/k\langle a\rangle)$ *is internal to $\mathcal{C}$.*

intuition, picture

3.5. Tangent spaces and jets

Let K be an algebraically closed field of arbitrary characteristic.

Definition 3.34. $\mathfrak{m}_{X,p} = \{f \in \mathcal{O}(X) | \, f(p) = 0\}$ The m**-th jet space of** X **at** p is dual space of $\mathfrak{m}_{X,p}/\mathfrak{m}_{X,p}^{m+1}$. The 1th jet space of V at p is also called the **tangent space of** X **at** p.

The

Lemma 3.35. *sd*

Proof. asd □

Specializing to $R = \mathcal{O}(X)$, $I = \mathfrak{m}_{X,p}^m$ yields the following.

Corollary 3.36. *For any affine variety X and any $p \in V$ we have $\bigcap_{m<\omega} \mathfrak{m}_{X,p}^m = (0)$.*

Lemma 3.37. *Suppose X, Y are subvarieties of K^n and $p \in X \cap Y$. If* $\mathrm{Jet}_p^m(X) = \mathrm{Jet}_p^m(Y)$ *for all $m < \omega$, then $X = Y$.*

3.6. A touch of differential algebraic geometry

We work inside a differential field (K, δ) of characteristic zero.

Definition 3.38. A **δ-module over** (K, δ) (or a **differential module over** (K, δ)) is a finite-dimensional vector space V over K together with an additive endomorphism $D_V \colon V \to V$ such that

$$D_V(rv) = \delta(r)v + rD_V(v)$$

for all $r \in K$ and $v \in V$. We denote by V^δ the kernel of D_V and call it the **module of constants of** (V, D_V) (which is a vector space over C_K).

Fix a basis $v_1, \ldots, v_n$ of (V, D_V) and set $v_i := D_V(v_i)$ for $i = 1, \ldots, n$. Expanding $v_1', \ldots, v_n'$ in terms of the basis $v_1, \ldots, v_n$ yields

$$\begin{cases} v_1' = a_{11}v_1 + \ldots + a_{1n}v_n \\ v_2' = a_{21}v_1 + \ldots + a_{2n}v_n \\ \qquad\qquad \vdots \\ v_n' = a_{n1}v_1 + \ldots + a_{nn}v_n \end{cases}$$

for some coefficients $(a_{ij})_{i,j} \in K$. But this looks just like a system of linear ordinary-differential equations! So in a way differential modules are algebraic counterparts of such systems. In this analogy V^δ is simply the set of solutions of our system. There is much more to this story, but unfortunately we will barely touch it.

Lemma 3.39. *Let (V, D_V) be a differential module over (K, δ) and assume that K is differentially closed. Then there is a basis $v_1, \ldots, v_n \in V^\delta$ of V^δ over C_K which is also a basis of V over K. In particular, $\dim_{C_K} V^\delta = \dim_K V$.*

Proof. ... □

Lemma 3.40.

3.7. The Canonical Base Property.

We begin the proof of Theorem 3.33.

For $m < \omega$ let V_m be $\mathrm{Jet}_p^m X$ equipped with its canonical δ-module structure. By Lemma 3.40 $\mathrm{Jet}_p^m Y$ is a δ-submodule of V_m.

3.8. Interlude: the birth of certain ideas

The beginning of model theory (as an autonomous part of logic) is typically dated at 1964 when Morley published his famous

Comments

Exercises

We work inside a monster model $\mathcal{U} \models \mathrm{DCF}_0$. We denote by $\mathcal{C}$ the field of constants of $\mathcal{U}$.

Exercise 3.1. Let R be the ring of continuous functions on $\mathbb{R}$ and let δ be a derivation of R which vanishes on $\mathbb{R}$. Show that $\delta \equiv 0$.

Exercise 3.2.

Exercise 3.3.

4. ω-stable theories

4.1. Some history

The beginning of model theory is typically dated... Morley's categoricity theorem... ... An uncountable model of T is controlled by certain special sets... Strongly minimal sets... In a way atoms...

Think about vector spaces (linear dimension), algebraically closed fields (transcendence degree), pure sets (cardinality)

In fact Zilber conjectured that every strongly minimal structure look like one of the above examples, in a precise way we will soon see. This statement is called the *Zilber trichotomy*. Really turned out to be harsher – Hrushovski constructed... However, Zilber trichotomy tends to hold for strongly minimal sets defined in theories "with a geometric flavours" – ...

Morley rank

4.2. The Morley rank

Let us fix a complete first order theory T without finite models and let $\mathfrak{C} \models T$ be a monster model.

Definition 4.1. Let $X \subseteq \mathfrak{C}^n$ be a definable set. For $\alpha \in \mathbf{On}$ we define recursively the statement "$\mathrm{RM}(X) \geq \alpha$" as follows.

- *Base step.* $\mathrm{RM}(X) \geq 0$ if X is nonempty.
- *Successor step.* If $\alpha = \beta+1$ then $\mathrm{RM}(X) \geq \alpha$ when there are disjoint definable sets $X_0, \ldots, X_n, \ldots \subseteq X$ with $\mathrm{RM}(X_i) \geq \beta$ for all $i < \omega$.
- *Limit step.* If α is a limit ordinal, then $\mathrm{RM}(X) \geq \alpha$ if $\mathrm{RM}(X) \geq \beta$ for all $\beta < \alpha$.

If there is some α such that $\mathrm{RM}(X) \geq \alpha$ does not hold, then we say that X is **ranked** and define its **Morley rank** as

$$\mathrm{RM}(X) = \sup \{\alpha \in \mathbf{On} \mid \mathrm{RM}(X) \geq \alpha\}.$$

For completeness we set $\mathrm{RM}(X) = \infty$ if $X \neq \emptyset$ is not ranked and $\mathrm{RM}(\emptyset) = -1$.

4.3. Strongly minimal sets

Definition 4.2. A **pregeometry** consists of a set X and a function $\mathrm{cl}\colon \mathcal{P}(X) \to \mathcal{P}(X)$ called a **closure operator** satisfying the following properties.

1. $A \subseteq \mathrm{cl}\, A$ and $\mathrm{cl}(\mathrm{cl}\, A) = \mathrm{cl}\, A$.
2. If $A \subseteq X$ and $a \in \mathrm{cl}\, A$ if and only if there is a finite set $A_0 \subseteq A$ such that $a \in \mathrm{cl}\, A_0$.
3. *(The exchange property)* If $a \in \mathrm{cl}(A \cup \{b\}) \setminus \mathrm{cl}\, A$ then $b \in \mathrm{cl}(A \cup \{a\})$.

Example 4.3. three...

Example 4.4. Let (X, cl) be a pregeometry. A subset $Y \subseteq X$ gives rise to two new pregeometries:

1. The induced pregeometry on Y defined via $A \mapsto Y \cap \mathrm{cl}\, A$.
2. The **localization** X/Y which is X together with the closure operator $\mathrm{cl}_Y\, A = \mathrm{cl}\,(A \cup Y)$.

(It is easy to check that the above are really pregeometries).

For the remainder this subsection let (X, cl) be a pregeometry.

Definition 4.5. We say that a set $A \subseteq X$ is **independent** if for any $a \in A$ we have $a \notin \mathrm{cl}\,(A \setminus \{a\})$. We say that A is a **basis** of X if X is independent and $\mathrm{cl}\, A = X$.

Lemma 4.6. *There exists a basis of X and any two bases of X are equinumerous.*

In the light of the above fact the following definition makes sense.

Definition 4.7. We call the cardinality of some/any basis of X the **dimension** of X and denote it by $\dim X$.

Example 4.8.

Definition 4.9. We say that a structure M is **minimal** if every definable set $X \subseteq M$ is either finite or cofinite. We say that a structure M is **strongly minimal** if any $M' \equiv M$ is a minimal structure. Finally, a theory T is **strongly minimal** if any model of T is minimal (equivalently: strongly minimal).

Example 4.10. the three...

Comments

Exercises

5. ω-stable groups

Let us work in a model M. A **definable group** is a definable subset $G \subseteq M^n$ together with a group operation $*\colon G \times G \to G$ which is also a definable map.
In the context of ω-stable theories definable groups are especially well-behaved.

5.1. Algebraic groups

5.1.1. Affine algebraic groups

Let K be an algebraically closed field. For convenience we will assume that $\operatorname{char} K = 0$.

Definition 5.1. An **affine algebraic group** is an affine algebraic set $G \subseteq K^n$ together with together with a group operation $*\colon G \times G \to G$ which is also a regular morphism.

Example 5.2. There is a plethora of examples of affine algebraic groups.

1. The simplest one is perhaphs the additive group $\mathbb{G}_{\mathrm{a}}(K) = (K, +)$.
2. There is also the multiplicative group $\mathbb{G}_{\mathrm{m}}(K) = (K^\times, \cdot)$. As written $\mathbb{G}_{\mathrm{m}}(K)$ is not an affine algebraic group since $K^\times$ is not closed in K. To remedy that we identify it with the hyperbola
$$\{(x, y) \in K^2 | xy = 1\}$$
with coordinatewise multiplication as the group operation.
3. Let $M_{n\times n}(K)$ be the set of all $n \times n$ matrices over K, identified with the affine space $K^{n\times n}$. Clearly $M_{n\times n}(K)$ is an affine algebraic group, the group operation being addition. Note that for $n = 1$ we get again $\mathbb{G}_{\mathrm{a}}(K)$
4. The general linear group $\mathrm{GL}_n(K)$ which consists of all invertible $n \times n$ matrices with coefficients in K. We encounter the same problem as in the previous example: $\mathrm{GL}_n(K)$ treated as a subset of $K^{n\times n}$ is not a closed set. To remedy that, we identify $\mathrm{GL}_n(K)$ with the following set
$$G = \{(A, t) \in M_{n\times n}(K) \times K | t \det A = 1\}.$$
The set G is a bona fide affine algebraic set and it is easy to see that the operation
$$(A, s) \cdot (B, t) = (AB, st) \cdot$$
makes $(G,)$ into an affine algebraic group. We identify G with $\mathrm{GL}_n(K)$ via the map
$$\mathrm{GL}_n(K) \ni A \longmapsto (A, \det A) \in G$$
which is of course an isomorphism of groups and moreover a homeomorphism in the Zariski topology. Note that $\mathrm{GL}_1(K) = \mathbb{G}_{\mathrm{m}}(K)$.
5. There are various interesting subgroups of the above examples, e.g. the special linear group $(\mathit{SL})_n(K) \leq \mathrm{GL}_n(K)$ consisting of all $A \in \mathrm{GL}_n(K)$ with $\det A = 1$.

5.1.2. Elliptic curves and abelian varieties

Naively $y^2 = x^3 + ax + b$

If three point $p, q, r \in E$ are colinear then we declare $p \oplus q \oplus r = 0_E$.

The proper approach is to replace the affine plane K by the *projective* plane $\mathbb{P}^2(K)$. The $\mathbb{P}^2(K)$ is obtained from K^2 by adding for direction L (the family of all lines parallel to a given one) a point ∞_L which belongs to each $l \in L$. Point of the form ∞_L are called **points at infinity**. All the points at infinity lay on the **line at infinity**.

There is a nice way of representing points of $\mathbb{P}^2(K)$. For neat geometric reason we will not go into we can identify $\mathbb{P}^2(K)$ with the quotient $(K^3 \setminus \{(0,0,0)\}) / \sim$ where $(a, b, c) \sim (a', b', c')$ if there is some $\lambda \in K^\times$ such that $(a, b, c) = \lambda(a', b', c')$. The equivalence class of (a, b, c) is denoted by $[a : b : c]$. Under this identification a point $(a, b) \in K^2$ corresponds to $[a : b : 1]$ and If L is the direction parallel to the vector (a, b) then $\infty_L = [a : b : 0]$.[7].

In general $\mathbb{P}^n(K) = (K^{n+1} \setminus \{0\}) / \sim$.

Homogeneous polynomial $F(X_0, \ldots, X_n)$

$Z(F) = \{[a_0 : \ldots : a_n] \in \mathbb{P}^n(K) | F(a_0, \ldots, a_n) = 0\}$

The Zariski topology on K^n coincides with the subspace topology coming from the inclusion $K^n \subseteq \mathbb{P}^n(K)$.

Definition 5.3. An **abelian variety** is a projective variety A together with a group operation $*\colon G \times G \to G$ which is also a regular morphism.

Abelian varieties are beautiful, magical objects. As one might

An important source of abelian varieties arises as follows. To a non-singular projective curve C on can associate an abelian variety $J(C)$ called **Jacobian variety of** C. This variety comes with a map $C \to J(C)$ (typically is a closed embedding) which is universal among maps from C to an abelian variety. Since abelian varieties are well-behaved (e.g. Jacobian varieties where crucial in Weil's work on Riemann hypothesis for curves over finite fields).

5.1.3. The general case

Definition 5.4. [8] An **algebraic group** is quasi-projective variety G together with a group operation $*\colon G \times G \to G$ which is also a regular morphism.

Fact 5.5 (A special case of Chevalley's theorem). *Assume that K is an algebraically closed field of characteristic zero. Then any connected algebraic group G contains a normal affine subgroup $L \leq G$ so that the quotient $A := G/L$ is an abelian variety. In particular G is an extension of an abelian variety by an affine group and this extension is essentially unique.*

The group L appearing in the above theorem can be characterized as the largest affine subgroup of G, in particular it is unique! The existence of a largest affine subgroup of G boils down to the fact that the compositum of two affine subgroups is an affine subgroup, which is relatively easy. The tricky part is to show that the quotient G/L is an abelian variety.

[7] Note that point on the line passing through $(0, 0)$ and (a, b) have projective coordinates of the form $[at : bt : 1] = [a : b : \frac{1}{t}]$. Formally passing to the limit $t \to \infty$ yields the point at infinity $[a : b : 0]$

[8] The following definition includes a small cheat. There is a general notion of a algebraic variety, defined similarly to the definition of a smooth manifolds. One should define algebraic groups as such a abstract varieties together with a compatible group structure. It is is then a theorem that any algebraic group is a quasi-projective variety. Actually one can deduce this from Fact 5.5

extending abelian varieties

For our purposes especially important are extensions of abelian varieties by **vector groups** i.e. the groups ${\mathbb{G}_{\mathrm{a}}}^n(K)$.

Fact 5.6. *Let A be an abelian variety of dimension g, let V be a vector group and let*

$$1 \to V \to G \to A \to 1$$

be an extension of A by V. Then there exists an algebraic subgroup $G_0 \subseteq G$ such that $\dim G_0 \leq 2g$ which projects onto A.

Fact 5.7. *Any group definable in* ACF *is definably isomorphic to an algebraic group.*

5.1.4. Differential algebraic groups

Manin kernels!!!

5.2. Speedrunning the basics of ω-stable groups

Let T be a countable complete ω-stable theory, let $\mathcal{U} \models T$ be a monster model and fix a definable group $(G, \cdot)$ with $G \subseteq \mathcal{U}^n$. By adding constants to the language we might (and will) assume that G is definable without parameters by a formula $G(x)$.

For a set $A \subseteq \mathcal{U}$ we denote by $S_G(A)$ the set of complete types over A **concentrated on** G, i.e. all types $p \in S_n(G)$ such that $G(x) \in p(x)$.

A type $p \in S_G(A)$ is called a **generic type of** G if $\mathrm{RM}(p) = \mathrm{RM}(G)$.

5.2.1. Chain conditions

Lemma 5.8 (The chain condition)**.** *Every strictly descending sequence of definable subgroups of G is finite.*

Corollary 5.9. *Let $(G_i : i \in I)$ be a family of definable subgroups of G. Then, there is some finite subset $I_0 \subseteq I$ such that*

$$\bigcap_{i \in I} G_i = \bigcap_{i \in I_0} G_i$$

holds.

In particular, we may apply the above corollary to the family of all definable finite-index subgroups of G. This yields the following.

Definition 5.10. We define the **connected component of** G as the smallest definable finite-index subgroup $G^0 \leq G$.

Note that G^0 is a normal subgroup of G, since for any $g \in G$ the subgroup $gG^0g^{-1} \leq G$ is definable and of finite index and thus $G^0 \subseteq gG^0g^{-1}$.

5.2.2. Generic types and stabilizers

The group G acts naturally on the type space $S_G(A)$ via

$$g \cdot p = \left\{ \varphi\left(g^{-1}x, a\right) : \varphi(x, a) \in p \right\}$$

for $p \in S_1(G)$ and $g \in G$. Here $\varphi\left(g^{-1}x, a\right)$ is formally the formula

$$(\exists y)\, x = g \cdot y \wedge \varphi(y, a).$$

Semantically, we have that $g \cdot p = \mathrm{tp}(ga/A)$ for some (equivalently: any) $a \models p$.

Definition 5.11. The **stabilizer of** $p \in S_G(A)$ is the group $\mathrm{Stab}(p) = \{g \in G | g \cdot p = p\}$.

Lemma 5.12. *For a type $p \in S_G(A)$ the following conditions are equivalent.*

1. *p is a generic type of G.*
2. *$\mathrm{Stab}(p)$ has finite index in G.*
3. *$\mathrm{Stab}(p) = G^0$.*

Lemma 5.13. *Assume that $H \leq G$ is a connected A-definable subgroup and let p be the generic type of H over A. Then any element of H is a product of two realizations of p.*

Proof. □

Corollary 5.14. *Assume that $H \leq G$ is a connected A-definable subgroup and let $X \subseteq H$ be a definable subset with $\mathrm{RM}(X) = \mathrm{RM}(H)$. Then $H = XX$.*

Proof. Pick a set A over which both H and X are defined. Let p be the generic type of H over A. Then p is concentrated on X. By Lemma 5.13 we have

$$H = p(\mathcal{U})p(\mathcal{U}) \subseteq XX \subseteq H$$

hence $H = XX$. □

5.2.3. Zilber's indecomposability theorem

Definition 5.15. A set $X \subseteq G$ is called **indecomposable** if for any definable subgroup $H \leq G$ the orbit space X/H is either infinite or consits of a single elements.

Example 5.16. We will prove that any conjugacy class in a connected group is indecomposable. Let $a \in G$ and define $X = \{gag^{-1} \colon g \in G\}$. Let $H \leq G$ be a definable subgroup (exercise!)

Theorem 5.17. *Assume that G is a group of finite Morley rank. Let $\mathcal{X} = \{X_i \colon i \in I\}$ be a family of definable indecomposable subsets of G and assume that each of them contains the identity $e \in G$. Then the group generated by $\bigcup_{i \in I} X_i$ is definable and connected.*

Remark 5.18. Before we prove Theorem 5.17, let us make a few comments.

1. The conclusion of Theorem 5.17 and an easy compactness argument imply in particular that the group H generated by $\mathcal{X}$ is generated by a finite subfamiy $\mathcal{X}_0$. In fact the proof of Theorem 5.17 will reveal that there is some $m < \omega$ and some $i_0, \ldots, i_m \in I$ (not neccesarily distinct) such that $H = X_{i_0}^{\varepsilon_0} \cdot \ldots \cdot X_{i_m}^{\varepsilon_m}$, where $\varepsilon_0, \ldots, \varepsilon_m \in \{-1, 1\}$.

2. Note that we do not assume that the family $\mathcal{X}$ is in itself definable!

3. The assumption $e \in G$ is indispensible: any singleton is an indecomposable set, thus *any* subset of G is a union of a family of indecomposable sets.

4. Likewise, the assumption that G has finite Morley rank cannot be dropped.

Proof of 5.17. Denote by H the group generated by $\mathcal{X}$. By possibly enlargening $\mathcal{X}$ may assume that for any $X_i \in \mathcal{X}$ we have $X_i^{-1} \in \mathcal{X}$. For $s = (i_0, \dots, i_m) \in I^{<\omega}$ define

$$X_s = X_{i_0} \cdot \ldots \cdot X_{i_m} \subseteq H.$$

Since $X_s \subseteq G$ and $\mathrm{RM}(G)$ is finite, there is some $s \in I^{<\omega}$ for which $\mathrm{RM}(X_s)$ is maximal. Let A be a (finite) set over which X_s is defined and pick a type $p \in S_G(A)$ such that p concentrates on X_s and $\mathrm{RM}(X_s) = \mathrm{RM}(p)$.

Claim. $H \subseteq \mathrm{Stab}(p)$.

$\vdash$ sdf $\dashv$

We have $X_t \subseteq H \subseteq \mathrm{Stab}(p)$ thus **ref...**

$$\mathrm{RM}(X_s) \leq \mathrm{RM}(\mathrm{Stab}(p)) \leq \mathrm{RM}(p) = \mathrm{RM}(X_s)$$

hence $\mathrm{RM}(X_s) = \mathrm{RM}(\mathrm{Stab}(p)) = \mathrm{RM}(p)$. In particular p is a generic type of $\mathrm{Stab}(p)$ and therefore **ref...** $\mathrm{Stab}(p)$ is connected. Now since $\mathrm{RM}(X_s) = \mathrm{RM}(\mathrm{Stab}(p))$ we have by Corollary that $\mathrm{Stab}(p) = X_s X_s \subseteq H \subseteq \mathrm{Stab}(p)$. Hence $H = \mathrm{Stab}(p)$, thus H is definable and connected. □

Example 5.19. Assume that G is connected and of finite Morley rank. We will show that its derived group G' (i. e. the group generated by all commutators $ghg^{-1}h^{-1}$ for $g, h \in G$) is definable and connected. Consider the family $(X_g \colon g \in G)$ where $X_g = \{ghg^{-1}h^{-1} \colon h \in G\}$. By Exercise 5.4 we have that X_g are indecomposable and moreover clearly $e \in G$, thus by Theorem 5.17 we have that the group generated by $\bigcup_{g \in G} X_g$ is definable and connected. But this group is by definition the derived group G' of G.

5.3. Manin kernels

Let A be an abelian variety over K and let Γ be a finite rank subgroup of $A(K)$. As already mentioned, we introduced differentially closed fields for a very specific reason: we want to enlarge Γ to a definable object (so that we can nuke it with model-theoretic machinery) which is still "small" in some sense (so that we can still use it to deduce something interesting about Γ). A precise meaning of this replacement is given by the following theorem, which we will prove in this subsection.

Theorem 5.20. *Let A be an abelian variety over K and let Γ be a finite rank subgroup of $A(K)$. Then there is a δ-definable subgroup $H \leq A$ such that $\Gamma \subseteq H$ and the Morley rank of H is finite.*

Proof. . □

Corollary 5.21. *Assume that $A \neq 0$ is a* ***simple*** *abelian variety. Then among all infinite δ-definable subgroups of A there is a smallest one. This subgroup is δ-connected, of finite Morley rank and contains all torsion points of A.*

Proof. Let B be the intersection of all infinite δ-definable subgroups of A of finite Morley rank. This is a type-definable group in DCF_0, thus by ω-stability we conclude that B is δ-definable. By the previous paragraph, B contains the torsion part of A, hence B is infinite. So we showed that B is the smallest infinite δ-definable subgroup of A and that $\mathrm{Tor}(A) \subseteq B$. Clearly B is δ-connected, as otherwise B^0 would contradict the minimality of B. Moreover, B has finite Morley rank since it is contained in A_0. □

Definition 5.22. For a simple abelian variety $A \neq 0$ inside a model of DCF_0 we call its smallest infinite δ-definable subgroup the **Manin kernel of** A and denote by $A^\sharp$.

Comments

Exercises

Throughout this list we work in an ω-stable theory T
Around indecomposability...

Around indecomposability

In this part we assume that G has finite Morley rank.

Exercise 5.1. Let $X \subseteq G$ be a definable *normal* subset of G (i. e. for any $g \in G$ we have $gXg^{-1} = X$). Assume that for every definable normal subgroup $H \leq G$ the set of orbits X/H is either infinite or consists of one element. Prove that X is indecomposable.

Exercise 5.2. Let X be definable strongly minimal subset of G. Prove that there exists an indecomposable set $X_0 \subseteq X$ such that $X \setminus X_0$ is finite.

Exercise 5.3. Show that Zilbers Indecomposability Theorem fails for groups of infinite Morley rank. Find a counterexample of Morley rank ω.

Exercise 5.4. Assume that G is connected. Prove that for any $g \in G$ the set $\{ghg^{-1}h^{-1} \colon h \in G\}$ is indecomposable.

Exercise 5.5. Prove that G' is definable even if G is not connected.

Index

References

[1] David Marker. *Model Theory. An Introduction.*

[2] Bruno Poizat. “???” In: ().