Model Theory of Fields

David Marker
Margit Messmer
Anand Pillay

Contents

The model theory of fields is a fascinating subject stretching from Tarski's work on the decidability of the theories of the real and complex fields to Hrushovksi's recent proof of the Mordell-Lang conjecture for function fields. Our goal in this volume is to give an introduction to this fascinating area concentrating on connections to stability theory.

The first paper "Introduction to the model theory of fields" begins by introducing the method of quantifier elimination and applying it to study the definable sets in algebraically closed fields and real closed fields. These first sections are aimed for beginning logic students and can easily be incorporated into a first graduate course in logic. They can also be easily read by mathematicians from other areas. Algebraically closed fields are an important examples of ω-stable theories. Indeed in section 5 we prove Macintyre's result that that any infinite ω-stable field is algebraically closed. The last section surveys some results on algebraically closed fields motivated by Zilber's conjecture on the nature of strongly minimal sets. These notes were originally prepared for a two week series of lecture scheduled to be given in Bejing in 1989. Because of the Tinnanmen square massacre these lectures were never given.

The second paper "Model theory of differential fields" is based on a course given at the University of Illinois at Chicago in 1991. Differentially closed fields provide a fascinating example for many model theoretic phenomena (Sacks referred to differentially closed fields as the "least misleading example"). This paper begins with an introduction to the necessary differential algebra and elementary model theory of differential fields. Next we examine types, ranks and prime models, proving among other things that differential closures are not minimal and that for $\kappa > \aleph_0$ there are 2^κ non-isomorphic models. We conclude with a brief survey of differential Galois theory including Poizat's model theoretic proof of Kolchin's result that the differential Galois group of a strongly normal extension is an algebraic group over the constants and the Pillay-Sokolovic result that any superstable differential field has no proper strongly normal expansions. Most of this article can be read by a beginning graduate student in model theory. At some points a deeper knowledge of stability theory or algebraic geometry will be helpful.

When this course was given in 1991 there was an annoying gap in our knowledge about the model theory of differentially closed fields. Shelah had proved Vaught's conjecture for ω-stable theories. Thus we knew that there were either $\aleph_0$ or $2^{\aleph_0}$ non-isomorphic countable differentially closed fields, but did not know which. In 1993 Hrushovski and Sokolovic showed there are $2^{\aleph_0}$. The proof used the Hrushovski-Zilber work on Zariski geometries and Buium's work on abelian varieties and differential algebraic groups. This circle of ideas is also crucial to Hrushovski's proof of the Mordell-Lang conjecture for function fields. The third paper, "Differential algebraic groups and the number of countable differentially closed fields", gives a proof that the number of countable models is $2^{\aleph_0}$ which avoids the Zariski geometry machinery.

The final paper, "Some model theory of separably closed fields", is a survey of the model theory of separably closed fields. For primes $p > 0$ there are separably closed fields which are not algebraically closed. These are the only other known example of stable fields. Separably closed fields play an essential role in Hrushovski's proof of the Mordell-Lang conjecture. This paper is intended as a survey of the background information one needs for Hrushovski's paper.

We would like to thank the following people who gave helpful comments on earlier drafts of some of these chapters: John Baldwin, Elisabeth Bouscaren, Zoe Chatzidakis, Lou van den Dries, Wai Yan Pong, Sean Scroll, Zeljko Sokolivic, Patrick Speissegger and Carol Wood.

Suggestions for Further Reading

There are a number of important topics that we either barely touched on or omitted completely. We conclude by listing a few such topics and some suggested references.

o-minimal theories: Many of the important geometric and structural properties of semialgebraic subsets of $\mathbf{R^n}$ generalize to arbitrary o-minimal structures.

L. van den Dries, *Tame topology and O-minimal structures*, preprint.

J. Knight, A. Pillay and C. Steinhorn, Definable sets in ordered structures II, Trans. AMS 295 (1986), 593-605.

A. Pillay and C. Steinhorn, Definable sets in ordered structures I, Trans. AMS 295 (1986), 565-592.

One of the most exciting recent developments in logic is Wilkie's proof that the theory of the real field with exponentiation is model complete and o-minimal. Further o-minimal expansions can be built by adding bounded subanalytic sets.

A. J. Wilkie, Some model completeness results for expansions of the ordered field of reals by Pfaffian functions and exponentiation, Journal AMS (to appear).

J. Denef and L. van den Dries, p-adic and real subanalytic sets, Ann. Math. 128 (1988), 79-138.

L. van den Dries, A. Macintyre, and D.Marker, The elementary theory of restricted analytic fields with exponentiation, Annals of Math. 140 (1994), 183-205.

p-adic fields: There is also a well developed model theory of the p-adic numbers beginning with the Ax-Kochen proof of Artin's conjecture and leading to Denef's proof of the rationality of p-adic Poincare series. Macintyre's paper is a survey of the area.

S.Kochen, Model theory of local fields, *Logic Colloquium '74*,
G. Mueller ed., Springer Lecture Notes in Mathematics 499, 1975, 384-425.

J. Denef, The rationality of the Poincare series associated to the p-adic points on a variety, Inv. Math. 77 (1984), 1-23.

A. Macintyre, Twenty years of p-adic model theory, *Logic Colloquium '84*, J. Paris, A. Wilkie and G. Wilmers ed., North Holland 1986, 121-153.

Pseudofinite fields: Ax showed that the theory of finite fields is decidable. This subject is carefully presented in Fried and Jarden's book. The Chatzidakis-van den Dries-Macintyre paper gives useful properties of definable sets.

M. Fried and M. Jarden, *Field Arithmetic*, Springer-Verlag (1986).

Z. Chatzidakis, L. van den Dries and A. Macintyre, Definable sets over finite fields, J. reine angew. Math 427 (1992), 107-135.

Zariski Geometries and the Mordell-Lang Conjecture: In 1992 Hrushovski gave a model theoretic proof of the Mordell-Lang conjecture for function fields. His work depends on a joint result with Zilber which characterizes the Zariski topology on an algebraic curve. The Bouscaren-Lascar volume is the proceedings of a conference in Manchester devoted to Hrushovski's proof and the model theoretic machinery needed in its proof.

E. Hrushovski and B. Zilber, Zariski Geometries, Journal AMS (to appear).

E. Hrushovski, The Mordell-Lang conjecture for function fields, Journal AMS (to appear).

E. Bouscaren and D. Lascar, *Stability Theory and Algebraic Geometry, an introduction* preprint.

Introduction to the Model Theory of Fields

David Marker
University of Illinois, Chicago

My goal in these lectures is to survey some classical and recent results in model theoretic algebra. We will concentrate on the fields of real and complex numbers and discuss connections to pure model theory and algebraic geometry.

Our basic language will be the language of rings $\mathcal{L}_{\rm r} = \{+, -, \cdot, 0, 1\}$. The field axioms, $T_{\rm fields}$, consists of the universal axioms for integral domains and the axiom $\forall x \exists y\ (x = 0 \vee xy = 1)$. Since every integral domain can be extended to its fraction field, integral domains are exactly the $\mathcal{L}_{\rm r}$-substructures of fields. For a fixed field F we will study the subsets of F^n which are defined in the language $\mathcal{L}_{\rm r}$.

§1 Algebraically closed fields

Let ACF be $T_{\rm fields}$ together with the axiom

$$\forall a_0 \ldots \forall a_{n-1} \exists x\ x^n + \sum_{i=0}^{n-1} a_i x^i = 0$$

for each n. Clearly ACF is not a complete theory since it does not decide the characteristic of the field. For each n let ϕ_n be the formula

$$\forall x\ \underbrace{x + \ldots + x}_{n \text{ times}} = 0.$$

For p prime, let ACF_p be theory $ACF + \phi_p$, and let $ACF_0 = ACF \cup \{\neg\phi_n : n = 1, 2, \ldots\}$.

For our purposes the key algebraic fact about algebraically closed fields is that they are described up to isomorphism by the characteristic and the transcendence degree. This has important model theoretic consequences. Recall that for a cardinal κ a theory is *κ-categorical* if there is, up to isomorphism, a unique model of cardinality κ.

Proposition 1.1. Let p be prime or zero and let κ be an uncountable cardinal. The theory ACF_p is κ-categorical, complete, and decidable.

Proof. The cardinality of an algebraically closed field of transcendence degree λ is equal to $\aleph_0 + \lambda$. Thus the only algebraically closed field of characteristic p and cardinality κ is the one of transcendence degree κ.

Vaught's test (a simple consequence of the Löwenheim-Skolem theorem) asserts that if a theory is categorical in some infinite cardinal, then the theory is complete. Finally, any recursively axiomatized complete theory is decidable.

Corollary 1.2. Let ϕ be an $\mathcal{L}_{\rm r}$-sentence. Then the following are equivalent:

i) $\mathbf{C} \models \phi$

ii) $ACF_0 \models \phi$

iii) $ACF_p \models \phi$ for sufficiently large primes p.

iv) $ACF_p \models \phi$ for arbitrarily large primes p.

Proof. Clearly ii)$\rightarrow$ i), while i)$\rightarrow$ii) follows from the completeness of ACF_0.

If $ACF_0 \models \phi$, then, since proofs are finite, there is an n such that $ACF \cup \{\neg\phi_1, \ldots, \neg\phi_n\} \models \phi$. Clearly if $p > n$ is prime, then $ACF_p \models \phi$. Thus ii)$\rightarrow$iii).

Clearly iii)$\rightarrow$iv)

Suppose $ACF_0 \not\models \phi$. Then by completeness $ACF_0 \models \neg\phi$, and by ii)$\rightarrow$iii), for sufficiently large primes p $ACF_p \models \neg\phi$. Thus there aren't arbitrarily large primes p where $ACF_p \models \phi$, so iv)$\rightarrow$ ii).

Corollary 1.2 has a surprising consequence.

Theorem 1.3 (Ax [A]) Let $f : \mathbf{C}^n \rightarrow \mathbf{C}^n$ be a polynomial map. If f is one to one, then f is onto.

Proof. We can easily write down an $\mathcal{L}_{\rm r}$-sentence Φ_d such that a field $F \models \Phi_d$ if and only if for any polynomial map $f : F^n \rightarrow F^n$ where each coordinate function has degree at most d, if f is one to one, then f is onto. By 1.2, it suffices to show that for sufficiently large primes p, $ACF_p \models \Phi_d$ for all $d \in \mathbf{N}$. Since ACF_p is complete it suffices to show that if K is the algebraic closure of the p element field, then any one to one polynomial map $f : K^n \rightarrow K^n$ is onto.

If $f : K^n \rightarrow K^n$ is a polynomial map, then there is a finite subfield $K_0 \subset K$ such that all coefficients in f come from K_0. Let $\bar{x} \in K^n$. There is a finite $K_1 \subset K$ such that $K_0 \subseteq K_1$ and $\bar{x} \in K_1^n$. Since $f : K_1^n \rightarrow K_1^n$, f is one to one and K_1 is finite, $f|K_1$ must be onto. Thus $\bar{x} = f(\bar{y})$ for some $y \in K_1^n$. So f is onto.

This result was later given a completely geometric proof by Borel ([B]).

Definition. We say that an $\mathcal{L}$-theory T has *quantifier elimination* if and only if for any $\mathcal{L}$-formula $\phi(v_1, \ldots, v_m)$ there is a quantifier free $\mathcal{L}$-formula $\psi(v_1, \ldots, v_m)$ such that $T \models \forall\bar{v}\ \phi(\bar{v}) \leftrightarrow \psi(\bar{v})$.

The following theorem leads to an easy test for quantifier elimination.

Theorem 1.4. Let $\mathcal{L}$ be a language containing at least one constant symbol. Let T be an $\mathcal{L}$ theory and let $\phi(v_1, \ldots, v_m)$ be an $\mathcal{L}$ formula with free variables $v_1, \ldots, v_m$ (we allow the possibility that $m = 0$). The following are equivalent:

i) There is a quantifier free $\mathcal{L}$-formula $\psi(v_1, \ldots, v_m)$ such that $T \vdash \forall\bar{v}\ (\phi(\bar{v}) \leftrightarrow \psi(\bar{v}))$

ii) If $\mathcal{A}$ and $\mathcal{B}$ are models of T, $\mathcal{C} \subseteq \mathcal{A}$ and $\mathcal{C} \subseteq \mathcal{B}$, then $\mathcal{A} \models \phi(\bar{a})$ if and only if $\mathcal{B} \models \phi(\bar{a})$ for all $\bar{a} \in \mathcal{C}$.

proof.

[i) $\to$ ii)]: Suppose $T \vdash \forall \bar{v}\ (\phi(\bar{v}) \leftrightarrow \psi(\bar{v}))$, where ψ is quantifier free. Let $\bar{a} \in \mathcal{C}$ where $\mathcal{C}$ is a substructure of $\mathcal{A}$ and $\mathcal{B}$ and the later two structures are models of T. Since quantifier free formulas are preserved under substructure and extension

$$\begin{aligned}
\mathcal{A} \models \phi(\bar{a}) &\leftrightarrow \mathcal{A} \models \psi(\bar{a}) \\
&\leftrightarrow \mathcal{C} \models \psi(\bar{a}) \quad (\text{since } \mathcal{C} \subseteq \mathcal{A}) \\
&\leftrightarrow \mathcal{B} \models \psi(\bar{a}) \quad (\text{since } \mathcal{C} \subseteq \mathcal{B}) \\
&\leftrightarrow \mathcal{B} \models \phi(\bar{a}).
\end{aligned}$$

[ii) $\to$ i)]. First, if $T \vdash \forall \bar{v}\ \phi(\bar{v})$, then $T \vdash \forall \bar{v}\ (\phi(\bar{v}) \leftrightarrow c = c)$. Second, if $T \vdash \forall \bar{v}\ \neg\phi(\bar{v})$, then $T \vdash \forall \bar{v}\ (\phi(\bar{v}) \leftrightarrow c \neq c)$. In fact, if ϕ is not a sentence we could use "$v_1 = v_1$" in place of $c = c$.

Thus we may assume that both $\phi(\bar{v})$ and $\neg\phi(\bar{v})$ are consistent with T.

Let $\Gamma(\bar{v}) = \{\psi(\bar{v}) : \psi \text{ is quantifier free and } T \vdash \forall \bar{v}\ (\phi(\bar{v}) \to \psi(\bar{v}))\}$. Let $d_1, \ldots, d_m$ be new constant symbols. We will show that $T + \Gamma(\bar{d}) \vdash \phi(\bar{d})$. Thus by compactness there are $\psi_1, \ldots, \psi_n \in \Gamma$ such that $T \vdash \forall \bar{v}\ (\bigwedge \psi_i(\bar{v})\ \to \phi(\bar{v}))$. So $T \vdash \forall \bar{v}\ (\bigwedge \psi_i(\bar{v})\ \leftrightarrow \phi(\bar{v}))$ and $\bigwedge \psi_i(\bar{v})$ is quantifier free. We need only prove the following claim.

claim. $T + \Gamma(\bar{d}) \vdash \phi(\bar{d})$.

Suppose not. Let $\mathcal{A} \models T + \Gamma(\bar{d}) + \neg\phi(\bar{d})$. Let $\mathcal{C}$ be the substructure of $\mathcal{A}$ generated by $\bar{d}$. [Note: if $m = 0$ we need the constant symbol to insure $\mathcal{C}$ is non-empty.]

Let $\mathrm{Diag}(\mathcal{C})$ be the set of all atomic and negated atomic formulas with parameters from $\mathcal{C}$ that are true in $\mathcal{C}$. Let $\Sigma = T + \mathrm{Diag}(\mathcal{C}) + \phi(\bar{d})$. If Σ is inconsistent, then there are quantifier free formulas quantifier free formulas $\psi_1(\bar{d}), \ldots, \psi_n(\bar{d}) \in \mathrm{Diag}(\mathcal{C})$, such that $T \vdash \forall \bar{v}\ (\bigwedge \psi_i(\bar{v} \to \neg\phi(\bar{v}))$. But then $T \vdash \forall \bar{v}\ (\phi(\bar{v}) \to \bigvee \neg\psi_i(\bar{v}))$. So $\bigvee \neg\psi_i(\bar{v}) \in \Gamma$ and $\mathcal{C} \models \bigvee \neg\psi_i(\bar{d})$, a contradiction. Thus Σ is consistent.

Let $\mathcal{B} \models \Sigma$. Since $\Sigma \supseteq \mathrm{Diag}(\mathcal{C})$, we may assume that $\mathcal{C} \subseteq \mathcal{B}$. But by a), since $\mathcal{A} \models \neg\phi(\bar{d})$, $\mathcal{B} \models \neg\phi(\bar{d})$, a contradiction.

The next lemma shows that to prove quantifier elimination for a theory we need only prove quantifier elimination for formulas of a very simple form.

Lemma 1.5. Suppose that for every quantifier free $\mathcal{L}$-formula $\theta(\bar{v}, w)$, there is a quantifier free $\psi(\bar{v})$ such that $T \vdash \forall \bar{v}\ (\exists w\ \theta(\bar{v}, w) \leftrightarrow \psi(\bar{v}))$. Then every $\mathcal{L}$-formula $\phi(\bar{v})$ is provably equivalent to a quantifier free $\mathcal{L}$-formula.

Proof. We prove this by induction on the complexity of ϕ.

This is clear if $\phi(\bar{v})$ is quantifier free.

For $i = 0, 1$ suppose that $T \vdash \forall \bar{v}\ (\theta_i(\bar{v}) = \psi_i(\bar{v})))$ where ψ_i is quantifier free.

If $\phi(\bar{v}) = \neg\theta_0(\bar{v})$, then $T \vdash \forall \bar{v}\ (\phi(\bar{v}) \leftrightarrow \neg\psi_0(\bar{v}))$.

If $\phi(\bar{v}) = \theta_0(\bar{v}) \wedge \theta_1(\bar{v})$, then $T \vdash \forall v\ (\phi(\bar{v}) \leftrightarrow (\psi_0(\bar{v}) \wedge \psi_1(\bar{v})))$.

In either case ϕ is provably equivalent to a quantifier free formula.

Suppose that $T \vdash \forall \bar{v}(\theta(\bar{v}, w) \leftrightarrow \psi_0(\bar{v}, w))$, where ψ is quantifier free. Suppose $\phi(\bar{v}) = \exists w\ \theta(\bar{v}, w)$. Then $T \vdash \forall \bar{v}\ (\phi(\bar{v}) \leftrightarrow \exists w(\psi(\bar{v}, w))$. By our assumptions there is a quantifier free $\psi(\bar{v})$ such that $T \vdash \forall \bar{v}\ (\exists w\ \psi_0(\bar{v}, w) \leftrightarrow \psi(\bar{v}))$. But then $T \vdash \forall \bar{v}\ (\phi(\bar{v}) \leftrightarrow \psi(\bar{v}))$.

Thus to show that T has quantifier elimination we need only verify that condition ii) of theorem 1.4 holds for every formula $\phi(\bar{v})$ of the form $\exists w \theta(\bar{v}, w)$ where $\theta(\bar{v}, w)$ is quantifier free.

Theorem 1.6 The theory ACF has quantifier elimination.

Proof. Let F be a field and let K and L be algebraically closed extensions of F. Suppose $\phi(v, \bar{w})$ is a quantifier free formula, $\bar{a} \in F$, $b \in K$ and $K \models \phi(b, \bar{a})$. We must show that $L \models \exists v\ \phi(v, \bar{a})$.

There are polynomials $f_{i,j}, g_{i,j} \in F[X]$ such that $\phi(v, \bar{a})$ is equivalent to

$$\bigvee_{i=1}^{l} \Big(\bigwedge_{j=1}^{m} f_{i,j}(v) = 0 \wedge \bigwedge_{j=1}^{n} g_{i,j}(v) \neq 0 \Big).$$

Then$K \models \bigwedge_{j=1}^{m} f_{i,j}(b) = 0 \wedge \bigwedge_{j=1}^{n} g_{i,j}(b)$ for some i.

Let $\widehat{F}$ be the algebraic closure of F. We can view $\widehat{F}$ as a subfield of both K and L. If any $f_{i,j}$ is not identically zero for $j = 1, \ldots, m$, then $b \in \widehat{F} \subseteq L$ and we are done. Otherwise since

$$\bigwedge_{i=1}^{n} g_{i,j}(b) \neq 0,$$

$g_{i,j}(X) = 0$ has finitely many solutions. Let $\{c_1, \ldots, c_s\}$ be all of the elements of L where some $g_{i,j}$ vanishes for $j = 1, \ldots, m$. Thus if we pick any element d of L with $x \notin \{c_1, \ldots, c_s\}$, then $L \models \phi(d, \bar{a})$.

Quantifier elimination for algebraically closed fields was first proved by Tarski who gave an explicit algorithm for eliminating quantifiers. The following weaker property is also of interest.

Definition. A theory T is *model complete* if whenever $M \subseteq N$ and $M, N \models T$, then N is an elementary extension of M.

Since quantifier free formulas are preserved under substructure and extension, any theory with quantifier elimination is model complete. The model completeness of algebraically closed fields can also be proved be appealing to Lindstrom's result that any $\aleph_1$-categorical, $\forall\exists$-axiomatizable theory is model complete (see [C]). In fact, model completeness is a weak form of quantifier elimination. A theory T is model complete if and only if every formula is equivalent to one of the form $\exists v_1, \ldots, \exists v_n \phi(\bar{v}, \bar{w})$ where ϕ is quantifier free.

For algebraically closed fields model completeness implies that if $F \subseteq K$ are algebraically closed fields and Σ is a finite system of equations and inequations over F which have a solution in K, then Σ already has a solution in F. Model completeness gives a very simple proof of Hilbert's Nullstellensatz. (We refer the reader to Lang ([L1]) for all algebraic results. If F is a field and $I \subset F[X_1, \ldots, X_n]$ is an ideal, let $V_F(I) = \{\bar{a} \in F^n : f(\bar{a}) = 0 \text{ for all } f \in I\}$.

Corollary 1.7. (Nullstellensatz) If F is an algebraically closed field and $P \subset F[X_1, \ldots, X_n]$ is a prime ideal then $V_F(P) \neq \emptyset$.

Proof. Let K be the algebraic closure of $F[X_1, \ldots, X_n]/P$. By model completeness K is an elementary extension of F. By Hilbert's basis theorem, P is finitely generated. Say $P = \langle f_1, \ldots, f_m \rangle$.— The sentence

$$\exists v_1 \ldots \exists v_n \bigwedge_{i=1}^{n} f_i(v_1, \ldots, v_n) = 0$$

is true in K, as $(X_1/P, \ldots, X_n/P)$ is a witness. By model completeness this sentence is true in F.

Using the fact that $\sqrt{I}$ is a finite intersection of prime ideals, the above proof can easily be modified to show that if I is an ideal in $F[\bar{X}]$ and $1 \notin \sqrt{I}$, then $V_F(I) \neq 0$.

While model completeness is useful in some applications, quantifier elimination is the primary tool for understanding definable sets in algebraically closed fields.

Definition. A theory T is *strongly minimal* if for any $M \models T$, every definable subset of M is either finite or cofinite. (Note that "definable" means "definable with parameters".)

If F is algebraically closed, then every definable subset of F is a finite Boolean combination of sets of the form $\{x : f(x) = 0\}$ where $f(X) \in F[X]$. If $f(X)$ is not identically zero, then the set of zeros of f is finite. Thus algebraically closed fields are strongly minimal.

Quantifier elimination also shows that the definable sets are exactly the constructible sets of algebraic geometry.

Definition. If F is a field, we say that $X \subset F^n$ is *Zariski closed* if it is a finite union of sets of the form

$$\{\bar{x} : \bigwedge_{i=1}^{m} f_i(\bar{x}) = 0\}$$

where $f_1, \ldots, f_m \in F[X_1, \ldots, X_m]$.

By Hilbert's basis theorem the intersection of a (possibly infinite) collection of Zariski closed sets is Zariski closed. Thus the Zariski closed sets give a topology on F^n. A subset of F^n is called *constructible* if it is a finite Boolean combination of Zariski closed sets. By quantifier elimination, if F is an algebraically closed field, then the definable sets are exactly the constructible ones. The following theorem of Chevalley gives the geometric restatement of quantifier elimination.

Corollary 1.8. The projection of a constructible set is constructible.

Definition. A Zariski closed set is *irreducible* if it can not be written as a union of two proper closed subsets. We will refer to irreducible closed sets as varieties.

Since $F[\bar{X}]$ is Noetherian, there are no infinite descending chains of Zariski closed sets. Thus every Zariski closed set is a finite union of irreducible closed sets. Thus by quantifier elimination, if X is definable then $X = \bigcup_{i=1}^{n}(V_i \cap O_i)$ where V_i is an irreducible component of the Zariski closure of X and O_i is Zariski open. Later we will give a description of the definable functions.

Definition. If A is a commutative ring, let $Spec(A)$ be the set of prime ideals of A. We call $Spec(A)$ the *Zariski spectrum* of A. We topologize $Spec(A)$ by taking basic closed sets $\{P : a_1, \ldots, a_n \in P\}$ for $a_1, \ldots, a_n \in A$.

The Zarsiki spectrum has a model theoretic analog.

Definition. If T is a complete theory and $M \models T$, an *n-type* over M is a maximal set of formulas with parameters from M and free variables $v_1, \ldots, v_n$ that is consistent with T. Let $S_n(M)$ be the set of n-types. We call $S_n(M)$ the *Stone Space* of M. We topologize $S_n(M)$ by taking basic open sets$\{p \in S_n(M) : \phi \in p\}$ for each formula ϕ with parameters from M. Note that these basic sets are indeed clopen.

The compactness theorem for first order logic implies that $S_n(M)$ is a compact space.

If F is an algebraically closed field there is a natural bijection between $S_n(F)$ and $Spec(F[X_1, \ldots, X_n])$. If p is an n-type, let $I_p = \{f \in F[\bar{X}] : \text{“}f(v_1, \ldots, v_n) = 0\text{”} \in p\}$. It is easy to see that I_p is a prime ideal. Moreover, if I is any prime ideal, let p be the set of consequences of

$$\{f(\bar{v}) = 0 : f \in I\} \cup \{f(\bar{v}) \neq 0 : f \notin I\}.$$

By quantifier elimination, $p \in S_n(F)$. The map $p \mapsto I_p$ is easily seen to be continuous. Thus $Spec(F[\bar{X}])$ is compact.

Definition. A complete theory T is ω-stable if for any $F \models T$, $|S_n(F)| = |F|$.

By Hilbert's basis theorem all prime ideals are finitely generated. Thus $|Spec(F[\bar{X}])| = |F|$ for any algebraically closed field F. By the above remarks $|S_n(F)| = |F|$. Thus for p a prime or zero, ACF_p is ω-stable. Indeed a basic result from model theory says that $\aleph_1$-categorical theories are always ω-stable.

In ω-stable theories there is a notion of *Morley Rank* which associates an ordinal to each definable set. In strongly minimal theories this notion is particular simple.

Definition. Let $M \models T$ (an arbitrary theory). Let $a, b_1, \ldots, b_n \in M$. We say that a is *algebraic* over $\bar{b}$ if there is an $\mathcal{L}$-formula $\phi(v, w_1, \ldots, w_n)$ such that $M \models \phi(a, \bar{b})$ and

$\{x \in M : M \models \phi(x, \bar{b})\}$ is finite.

If T is strongly minimal then algebraic dependence satisfies the exchange lemma, namely if a is algebraic over $\bar{b}, c$ and not algebraic over $\bar{b}$, then c is algebraic over $\bar{b}, a$. In algebraically closed fields this is exactly the usual notion of algebraic dependence.

One can give a well defined notion of dimension, namely dim $(\mathrm{a}_1, \ldots, \mathrm{a}_\mathrm{n})$ is the maximal cardinality of a subset $\{a_{i_1}, \ldots, a_{i_m}\}$ such that no a_{i_j} is algebraic over $\{a_{i_1}, \ldots, a_{i_m}\} \setminus \{a_{i_j}\}$. If $M \models T$ and $X \subset M^n$ is definable, then the *Morley rank* of X is the maximum dimension of a tuple $(b_1, \ldots, b_n)$ such that for some elementary extension N of M $N \models \bar{b} \in X$.

If X has Morley rank m, then the *Morley degree* of X is the maximum number of pairwise disjoint definable rank m sets X can be partioned into.

Morley rank and degree have geometric meaning.

Definition. If V is a Zariski closed set in F^n, let $F[V]$ be the ring $F[X_1, \ldots, X_n]/I(V)$, where $I(V)$ is the ideal of all polynomials which vanish at each point in V. We call $F[V]$ the *coordinate ring* of V. If V is irreducible, then $F[V]$ is an integral domain and we let $F(V)$ be the fraction field of $F[V]$. We call $F(V)$ the function field of V.

The ring $F[V]$ corresponds to the ring of polynomial functions on V, while $F(V)$ corresponds to the field of (partial) rational functions on V. There is a classical dimension theory for varieties.

Definition. If V is an irreducible variety, we define the dimension of V to be the transcendence degree of $F(V)$ over F. If X is a constructible set its dimension defined to be the maximal dimension of an irreducible component of the Zariski closure.

Note that if O is an open subset of an irreducible variety V, then $V \setminus 0$ has dimension less than the dimension of V.

Proposition 1.9. If V is a variety, then its Morley rank is equal to its dimension.

Proof. If V is a variety of dimension m, then $F(V)$ has transcendence degree m over F. Let K be the algebraic closure of $F(V)$. Since $X_1/I(V), \ldots, X_n/I(V)$ generate $F(V)$ over F they have transcendence degree m over F. Thus $(X_1/I(V), \ldots, X_n/I(V))$ demonstrates that V has Morely rank at least m.

On the other hand, if L is a field extension of F and $L \models \bar{a} \in V$, there is a ring homomorphsim from $F[V]$ into L given by $f \mapsto f(\bar{a})$. Clearly the transcendence degree of $\bar{a}$ is at most the transcendence degree of $F[V]$ over F.

Corollary 1.10. If X is a non-empty constructible set, then its Morley rank is equal to its dimension.

Proof.

First suppose that V is an irreducible variety, O is open, and $X = V \cap O$ is non-empty. If p is the type such that $V_1 = V(I_p)$, then p is the type of maximal Morely rank in V.

The type p must contain the formula "$\bar{v} \in O$", as otherwise there is a polynomial $f \notin I_p$ such that "$f(\bar{v}) = 0$" $\in p$, a contradiction.

If X is an arbitrary constructible set, then $X = \bigcup_{i=1}^{m} V_i \cap O_i$, where $V_1, \ldots, V_m$ are the irreducible components of the Zariski closures of X, O_i is open, and $V_i \cap O_i$ is non-empty. The corollary now follows from the first case.

Finally, we will give the promised description of definable functions.

Theorem 1.11. Let F be an algebraically closed field. Let $f : F^n \to F$ be a definable function. Then there is a nonempty open set O such that:

i) If F has characteristic 0, then there is a rational function r such that $f|O = r$.

ii) If F has characteristic $p > 0$, then there is a natural number n and a rational function r such that $f|O = \sigma^{-n} \circ r$, where σ is the Frobenious automorphism $\sigma(x) = x^p$.

proof.

Let K be an elementary extension of F containing $t_1, \ldots, t_n$ which are algebraically independent over F. Since $f(\bar{t})$ are fixed by any automorphism of F which fixes $t_1, \ldots, t_n$ and F, $f(\bar{t})$ is in the perfect closure of $F(t_1, \ldots, t_n)$. Thus in characteristic 0 there is a rational function r such that $r(\bar{t}) = f(\bar{t})$. In characteristic $p > 0$, we can find a rational function r and a natural number n such that $\sigma^{-n}(r(\bar{t})) = f(\bar{t})$.

Henceforth we consider only the characteristic zero case as the characteristic p case is analogous. In F consider $Y = \{\bar{x} \in F^n : r(\bar{x}) = t(\bar{x})\}$. Since $r(\bar{t}) = f(\bar{t})$ and the t_i are independent, Y has Morely rank n. Since there is a unique n-type of Morley rank n, Y has Morely rank n and $\neg Y$ has Morely rank less than n. Thus if V is the Zariski closure of $\neg Y$, dim V < n. Let $O = F^n \setminus V$. Then O is a nonempty open subset of F^n and $f|O = r$.

[Pi4] provides a more extensive introduction to the model theory of algebraically closed fields.

§2 Real Closed Fields

We next turn our attention to the field of real numbers. We would like to prove model completeness and quantifier elimination results analogous to those for algebraically closed fields. There is one major difficulty: we can not eliminate quantifiers in the language of rings. In particular in the reals we can define the ordering by

$$x < y \Leftrightarrow \exists z\ (z^2 + x = y \wedge z \neq 0)$$

and we will see that that this is not equivalent to a quantifier free formula (in fact by a theorem of Macintyre, McKenna, and van den Dries ([**M-M-D**]). We circumvent this difficulty by extending $\mathcal{L}_{\mathrm{r}}$ to $\mathcal{L}_{\mathrm{or}} = \mathcal{L}_{\mathrm{r}} \cup \{<\}$. In this language we will prove quantifier elimination.

We begin by examining the work of Artin and Schrier on the algebraic structure of the real field (see [L1] for details). For the remainder of this section we all fields will have characteristic zero. The model theoretic study of the **R** began with the work of Tarski. See [D2] for further discussion of Tarski's work.

Definition. A field F is said to be *formally real* if -1 is not a sum of squares. We say F is real closed if it is formally real and has no proper formally real algebraic extensions.

Lemma 2.1. If F is formally real, and $a \in F$ is not a sum of squares, then $F(\sqrt{-a})$ is formally real.

It follows from 2.1, then if F is real closed and $a \neq 0$, then exactly one of a and $-a$ has a square root in F. One can then define an order on F such that the positive elements are exactly the squares. Clearly this is the only way to order F.

Theorem 2.1. (Artin-Schrier) Let $(F, <)$ be an ordered field. Then the following are equivalent.

i) F is real closed.

ii) $F(i)$ is algebraically closed (were $i = \sqrt{-1}$).

iii) If $p(X) \in F[X]$, and $a, b \in F$ such that $a < b$ and $p(a) < p(b)$ then there is $c \in F$ such that $a < c < b$ and $p(c) = 0$.

iv) For any $a \in F$ either a or $-a$ is a square and every polynomial of odd degree has a root.

Since iv) does not mention the ordering, we can axiomatize the theory of real closed fields in the language $\mathcal{L}_{\mathrm{r}}$ by axioms asserting that F is formally real field of characteristic zero where iv) holds. We call this theory RCF.

Definition. If F is formally real we say that $K \supseteq F$ is a *real closure* of F if it is a real closed algebraic extension of F.

Clearly every real field has a real closure, however, unlike algebraic closures, the real closure of a formally real field need not be unique. For example, if t is transcendental, $\mathbf{Q}(\sqrt{t})$ and $\mathbf{Q}(\sqrt{-t})$ are real. Let F_1 and F_2 be real closures of $\mathbf{Q}(\sqrt{t})$ and $\mathbf{Q}(\sqrt{-t})$ respectively. Both F_1 and F_2 are real closures of $\mathbf{Q}(t)$, but they are not isomorphic over $\mathbf{Q}(t)$. (Note that this shows that the theory RCF does not eliminate quantifiers in the language $\mathcal{L}_{\mathrm{r}}$.) On the other hand, if $(F,<)$ is an ordered field, then there is a unique real closure K, where the ordering on K extend the ordering on F. The proof uses Sturm's algorithm to bound the location of the roots of a polynomial (see [L1]).

Let $RCOF$ be the theory of real closed ordered fields in the language $\mathcal{L}_{\mathrm{or}}$. The axioms for RCF are the axioms for ordered fields and an axiom schema asserting the intermediate value theorem for polynomials (2.2 iii).

Theorem 2.3. The theory $RCOF$ has quantifier elimination in $\mathcal{L}_{\mathrm{or}}$.

Proof.

We apply theorem 1.4. Let F_0 and F_1 be models of $RCOF$ and let $(R,<)$ be a common substructure. Then $(R,<)$ is an ordered domain. Let L be the real closure of the fraction field of R. By the uniqueness of real closures we can may assume that $(L,<)$ is a substructure of F_0 and F_1. Suppose $\phi(v,\bar{w})$ is quantifier free, $\bar{a}\in R$, $b\in F_0$ and $F_0\models\phi(b,\bar{a})$. We need to show that $F_1\models\exists v\ \phi(v,\bar{a})$. It suffices to show that $L\models\exists v\ \phi(v,\bar{a})$.

As in the proof of theorem 1.6 (and fooling around with the order), we may assume that there are polynomials $f_1,\ldots,f_n,g_1,\ldots,g_m\in R[X]$ such that $\phi(v,\bar{a})$ is

$$\bigwedge_{i=1}^{n} f_i(v)=0\wedge\bigwedge_{i=1}^{m} g(v)>0.$$

If any of the f_i is not zero, then since $\phi(b,\bar{a})$, a is algebraic over R and thus in L. So we may assume $\phi(v,\bar{a})$ is

$$\bigwedge_{i=1}^{m} g_i(v)>0.$$

Since L is a real closed field, by 2.1 ii) we can factor each g_i as a product of factors of the form $(X-c)$ and (X^2+bX+c) where $b^2-4c<0$. The linear factors change sign at c, while the quadratic factors do not change signs. If follows that we can find $\alpha_1,\ldots,\alpha_l\in\mathcal{L}\cup\{-\infty\}$ and $\beta_1,\ldots,\beta_l\in\mathcal{L}\cup\{+\infty\}$ such that for $v\in F_0$, $\phi(v,\bar{a})$ if and only if

$$\bigvee_{i=1}^{l}\alpha_i<v<\beta_i.$$

Since $F_0\models\phi(b,\bar{a})$, for some i, $\alpha_i<b<\beta_i$. Then $L\models\phi(\frac{\alpha+\beta}{2},\bar{a})$.

Corollary 2.4. *RCOF* and *RCF* are complete, model and decidable.

proof

Model completeness for $RCOF$ is immediate from quantifier elimination. For RCF model completeness follows because if $F \subseteq K$ are real closed fields, then, when viewed as $\mathcal{L}_{\text{or}}$-structures F is still a substructure of K. Thus K is an elementary extension in $\mathcal{L}_{\text{or}}$ and hence in $\mathcal{L}_{\text{r}}$.

Any real closed field contains $(\mathbf{Q}, <)$. Thus the real closure of $\mathbf{Q}$, the real algebraic numbers, is an elementary submodel of every real closed field, so the theory is complete.

Since RCF and $RCOF$ are recursively axiomatized and complete, both are decidable.

Since RCF and $RCOF$ have the same models, we will forget about $RCOF$ and refer to the theory as RCF.

The next concept is the correct analog of strong minimality for ordered structures.

Definition. A structure $(M, <, \ldots)$ is *o-minimal* if every definable subset of M is a finite union of points and intervals.

Corollary 2.5. Every real closed field F is o-minimal.

Proof.

For $f(X) \in F$, $\{x : f(x) > 0\}$ is a union of intervals. From this o-minimality follows easily.

The notion of o-minimality was introduced by van den Dries [D1] and studied extensively by Pillay and Steinhorn, among others (see for example [P-S] and [K-P-S]). Of particular interest is the fact that o-minimality leads to a deep structure theory for definable sets in n-space. In §3 will give classical proofs of some of the consequences of o-minimality for real closed fields.

Quantifier elimination leads to a geometric characterization of the definable sets. Let F be a real closed field

Definition. We say that $X \subset F^n$ is *semialgebraic* if it is a finite Boolean combination of sets of the form $\{\bar{x} : f(\bar{x}) > 0\}$ or $\{\bar{x} : f(\bar{x}) = 0\}$, $f \in F[\bar{X}]$.

Clearly, the semialgebraic sets are exactly the quantifier free definable sets. Quantifier elimination then has the following geometric interpretation.

Corollary 2.6. (Tarski-Seidenberg Theorem) The projection of a semialgebraic set is semialgebraic.

The next corollaries are typical applications.

Corollary 2.7. If A is a semialgebraic set then the closure of A is semialgebraic.

Proof.
Let $d(\bar{x},\bar{y})=z$ if and only if $z^2=\sum(x_i-y_i)^2$ and $z>0$. Then the closure of A is

$$\{\bar{x}:\forall\epsilon>0\ \exists\bar{y}\ \bar{y}\in A\wedge d(\bar{x},\bar{y})<\epsilon\}.$$

Corollary 2.8. Let F be real closed. If $X\subset F^n$ is a closed and bounded semialgebraic set and $f:X\to F^m$ is continuous and semialgebraic, then the image of X is closed and bounded.

Proof. If $F=\mathbf{R}$ this is trivial as X is compact if and only if X is closed and bounded and the continuous image of a compact set is compact. On the other hand if $\phi(\bar{v},\bar{a})$ defines X and $\psi(\bar{x},\bar{y},\bar{b})$ defines f. There is an $\mathcal{L}_{\rm or}$ sentence Φ asserting that for all $\bar{\alpha}$ and $\bar{\beta}$ if $\phi(\bar{v},\bar{\alpha})$ is a closed bounded set Y and $\psi(\bar{x},\bar{y},\bar{\beta})$ defines a continuous function with domain Y, then the image is closed and bounded. This sentence is true in $\mathbf{R}$ and hence true in F.

Model completeness has several important applications. The first is Robinson's version of Artin's solution to Hilbert's $17^{\rm th}$ problem.

Definition. Let $f(X_1,\ldots,X_n)$ be a rational function over a real closed field R. We say that f is *positive semi-definite* if $f(\bar{a})\geq 0$ for all $\bar{a}\in R$.

Theorem 2.9. (Artin) If f is a positive semi-definite rational function over a real closed field R, then f is a sum squares of rational functions over R.

The proof uses one algebraic lemma (see [L1]).

Lemma 2.10. If F is real and $a\in F$ is not a sum of squares, then there is an ordering of F where a is negative.

Proof of 2.9.
Suppose $f(X_1,\ldots,X_n)$ is a positive semi-definite rational function which is not a sum of squares. Then, by 2.10, there is $<$ an ordering of $R(\bar{X})$ where f is negative. Let K be the real closure of the ordered field $(R(\bar{X}),<)$. Then $K\models\exists\bar{v}\ f(\bar{v})<0$. By model completeness this sentence also holds in R, contradicting the fact that f is positive semi-definite.

A similar argument can be used to prove the following real nullstenllensatz.

Theorem 2.11. (Dubois-Reisler) Let R be a real closed field and let I be an ideal in $R[\bar{X}]$. Then $I=I(V(I))$ if and only if $a_1,\ldots,a_n\in I$ whenever $\sum a_i^2\in I$.
(For a proof see [Di] or [B-C-R].

This style of argument can also be used (and seems essential) to prove some of the basic properties of Nash functions.

We next examine the definable functions in real closed fields. We let R be a real closed field.

Lemma 2.12. If $f : R \to R$ is definable, then for any open set $U \subseteq R$, there is a point $x \in U$ such that f is continuous at x.

Proof. (van den Dries [D1]) By completeness it suffices to prove this for $\mathbf{R}$.

case 1: There is an open set $V \subseteq U$ such that f has finite range on V.

In this case we can find an open subset of V on which f is constant.

case 2. Otherwise.

We build $V_0 \supseteq V_1 \supseteq \cdots$ open subsets of U such that the closure of V_{n+1} is contained in V_n. Given V_n, let X be the range of f on V_n. By o-minimality X contains an interval (a, b) of length less than $\frac{1}{n}$. Let V_{n+1} be a suitable open subinterval of $V_n \cap f^{-1}(a, b)$.

Let $x \in \bigcap V_i$. Clearly f is continuous at x.

Lemma 2.12 will generalize to R^n once we know that R^n can not be partitioned into finitely many sets with non-empty interior.

Corollary 2.13. If $f : R \to R$ is definable, then we can partition $R = I_1 \cup \ldots I_n \cup F$ where F is finite and the I_j are disjoint open sets where f is continuous on each I_j.

Proof.

Otherwise, by o-minimality, $\{x : f \text{ is discontinuous at } x\}$ has non-empty interior, contradicting lemma 2.12.

Proposition 2.14 (van den Dries [D3]) Let $X \subset R^{m+n}$ be definable. There is a definable function $f : R^m \to R^n$ such that for all $x \in R^m$ if $\exists y \in R^n\ (x, y) \in X$, then $(x, f(x)) \in X$. (We say that the theory of real closed fields has *definable Skolem functions.*)

Proof. By induction it suffices to prove this for $n = 1$. For $a \in R^m$ let $X_a = \{y : (a, y) \in X\}$. By o-minimality X_a is a finite union of points and intervals. If X_a is empty let $f(a) = 0$, otherwise we define $f(a)$ by cases.

case 1: If $X_a = R$, let $f(a) = 0$.

case 2: If X_a has a least element b, let $f(a) = b$.

case 3: If the leftmost interval of $X_a = (c, d)$, let $f(a) = \frac{c+d}{2}$.

case 4: If the leftmost interval of $X_a = (-\infty, c)$, let $f(a) = c - 1$.

case 5: If the leftmost interval of $X_1 = (c, +\infty)$, let $f(a) = c + 1$.

This exhausts all possibilities. Clearly f is definable and does the job.

Definable functions have a very nice application. The following theorem of Milnor ([Mi]) was first proved by geometric techniques.

Theorem 2.15. (Curve selection) Let X be a definable sunset of R^n and let a be a point in the closure of X. There is $\epsilon > 0$ and a continuous function $f : (0, \epsilon) \to R^n$. Such that $f(x) \in X$ for all $x \in (0, \epsilon)$ and $\lim_{x \to 0} f(x) = a$.

Proof.

Let $D = \{(\delta, x) : x \in X \text{ and } |x - a| < \delta\}$. Since R has definable Skolem functions, there is an $\eta > 0$ and a definable $f : (0, \eta) \to X$ such that$f(\delta) \in X$ and $|f(\delta) - a| < 0$ for all $\delta \in (0, \eta)$. By 2.13 there is an $\epsilon \in (0, \eta)$ such that f is continuous on $(0, \eta)$.

§3 Cell Decomposition

Let R be a real closed field. We next study the structure of semi-algebraic subsets of R^n. As a warm up we prove Thom's Lemma. Let

$$\operatorname{sgn}(x) = \begin{cases} -1 & x < 0 \\ 0 & x = 0 \\ 1 & x > 0 \end{cases}.$$

Theorem 3.1. (Thom's lemma) Let $f_1, \ldots, f_s$ be a sequence of polynomials in $R[X]$ closed under differentiation. For $\sigma \in \{-1, 0, 1\}^s$ let

$$A_\sigma = \{x \in R : \bigwedge_{i=1}^{s} \operatorname{sgn}(f_i(x)) = \sigma(i)\}.$$

Then each A_σ is either empty, a singleton or an open interval.

Proof.

We proceed by induction on s. If $s = 1$, then f_1 must be identically zero and the theorem is true.

Assume the theorem is true for s. Without loss of generality assume that f_{s+1} has maximal degree. Let $\eta = \sigma|s$. By induction, we can apply the theorem to $f_1, \ldots, f_s$ and η. Clearly $A_\eta \supseteq A_\sigma$. If A_η is empty or a singleton then so is A_σ. Thus we may assume A_η is an open interval $I = (c, d)$. Since $f_i = f'_{s+1}$ for some $i \leq s$, and f_i does not change sign on I, f_{s+1} is monotonic on I. If f_{s+1} does not change sign on I, then $A_\sigma = I$ or $A_\sigma = \emptyset$. Otherwise $f_{s+1}(\alpha) = 0$ for some $\alpha \in I$ and $A_\sigma = \{\alpha\}$, $A_\sigma = (c, \alpha)$ or $A_\sigma = (\alpha, d)$.

The next theorem can be thought of as a higher dimensional version of Thom's theorem. Let $X = X_1, \ldots, X_n$.

Theorem 3.2. (Cylindric Decomposition) Suppose $f_1, \ldots, f_s \in R[X, Y]$. There is a partition of R^n into semi-algebraic sets $A_1, \ldots, A_m$ such that for each $i \leq m$, there are continuous semialgebraic functions $\xi_{i,1}, \ldots, \xi_{i,l_i}.A_i \to R$ such that:

i) for all $x \in A_i$, $\xi_{i,1}(x) < \xi_{i,2}(x) < \ldots < \xi_{i,l_i}(x)$ and $\{\xi_{i,1}(x), \ldots, \xi_{i,l_i}(x)\}$ contains the isolated zeros of the polynomials $f_1(x, Y), \ldots, f_s(x, Y)$ [It is convenient to let $\xi_{i,0}(x) = -\infty$ and $\xi_{i,l_i+1} = +\infty$.], and

ii) if x_1 and x_2 are in A_i and either there a) is a j such that $\xi_{i,j}(x_1) = y_1$ and $\xi_{i,j}(x_2) = y_2$, or b) there is a j such that $\xi_{i,j}(x_k) < y_k < \xi_{i,j+1}(x_k)$, for $k = 1, 2$, then

$$\bigwedge_{i=1}^{s} \operatorname{sgn}(f_i(x_1, y_1)) = \operatorname{sgn}(f_i(x_2, y_2)).$$

[Intuitively ii) says that for $x \in A_i$ $\operatorname{sgn}(f_j(x, y))$ depends only on the relative position of y with respect to $\xi_{i,1}(x), \ldots, \xi_{i,l_i}(x)$.]

Proof.

Without loss of generality we may assume that $f_1, \ldots, f_s$ is closed under $\frac{\partial}{\partial Y}$.

Let q be the maximal degree of any f_i with respect to Y. Fix $x \in R^n$. If $f_i(x, Y)$ is not identically zero, it has at most q zeros. Let $y_1 < \ldots < y_{l(x)}$ be the isolated zeros of $f_1(x, Y), \ldots, f_s(x, Y)$. Then $l(x) \leq sq$. For $j = 1, \ldots, l(x) - 1$, let $I_{x,j} = (y_j, y_{j+1})$ and let $I_{x,0} = (-\infty, y_1)$ and $I_{x,l(x)} = (y_j, +\infty)$. Then each $f_j(x, y)$ has constant sign for $y \in I_{x,i}$. Call this sign $\beta_{j,i}(x)$. We define P_x the *pattern* at x to be the the $s \times 2l(x) + 1$ matrix where the i^{th}-row is:

$$[\beta_{i,0}(x), \ldots, \beta_{i,l(x)}(x), \operatorname{sgn}(f_i(x, y_1)), \ldots, \operatorname{sgn}(f_i(x, y_n))].$$

Since the entries of P_x are just -1, 0 or 1, there are only finitely many (at most $3^{s(2sq+1)}$) possible pasterns. Moreover if P is a pattern, it is routine to show that $A_P = \{x : P_x = P\}$ is definable and hence semialgebraic.

Let $A_1, \ldots, A_m$ be all the nonempty A_P. For each i, let $l_i = l(x)$ for $x \in A_i$. Let $\xi_{i,j}(x)$ be the j^{th}-element of $\{y : y \text{ is an isolated zero of some } f_k(x, Y)\}$ for $j = 1, \ldots, l(i)$. Clearly $\xi_{i,j}$ is semialgebraic. It is clear from the construction that i) and ii) hold. We need only show that each $\xi_{i,j}$ is continuous.

Let $x \in A_i$. Let $y_j = \xi_{i,j}(x)$. Thus some y_j is an isolated zero of some $f_k(x, Y)$. Since the f_i are closed under $\frac{\partial}{\partial Y}$, we may assume that $f_k(x, Y)$ changes sign at y_j. Since for sufficiently small $\epsilon > 0$, $f_k(x, y_j - \epsilon) f_k(x, y_j + \epsilon) < 0$, there is a neighborhood B_j of x such that this is true for all $z \in B_j$. Thus $f_k(z, Y)$ has a root in $(y_j - \epsilon, y_j + \epsilon)$ for all $z \in B_j$. Thus if $x \in A_i$ then for all sufficiently small δ, there is an open neighborhood B of x such that if $z \in B$, then some $f_k(z, Y)$ has an isolated zero in $(\xi_{i,j}(x) - \delta, \xi_{i,j}(x) + \delta)$ for $j = 1, \ldots, l(i)$. Hence if $z \in A_i \cap B$, $\xi_{i,j}(z) \in (\xi_{i,j}(x) - \delta, \xi_{i,j}(x) + \delta)$. Thus $\xi_{i,j}$ is continuous at x.

Cylindric decomposition will be our primary tool for studying semialgebraic sets. It gives an inductive procedure for building up definable sets.

Definition. -A subset X of R is a 0-cell if $X = \{a\}$ for some $a \in \mathbf{R}$.

-A subset X of R is a 1-cell if it is an open interval.

- If $X \subseteq R^m$ is an n-cell and $f : X \to R$ is a continuous semialgebraic function, then

$$Y = \{(x, y) \in R^{m+1} . x \in X, f(x) = y\}$$

is an n-cell.

-If $X \subseteq \mathbf{R}^m$ is an n-cell, $f, g : X \to R$ are continuous semialgebraic functions such that $f(x) < g(x)$ for all $x \in X$ [we also allow f to be constantly $+\infty$ or g identically $-\infty$], then

$$Y = \{(x, y) \in R^{m+1} . x \in X, f(x) < y < g(x)\}$$

is an $n + 1$-cell.

Theorem 3.3 (Cell Decomposition) If $A \subseteq \mathbf{R}^n$ is semialgebraic, then A is a finite union of disjoint cells.

Proof. Let X denote $X_1, \ldots, X_n$. If $f_1, \ldots, f_s \in R[X]$ and $\sigma \in \{-1, 0, 1\}^s$, let

$$A_\sigma = \{x : \bigwedge \mathrm{sgn}(f_i(x)) = \sigma(i)\}.$$

Clearly for any semialgebraic set Y we can find polynomials $f_1, \ldots, f_s$ and $S \subseteq \{-1, 0, 1\}^s$ such that

$$Y = \bigcup_{\sigma \in S} A_\sigma.$$

The theorem is proved by induction on n. By o-minimality it is true for $n = 1$. Assume the theorem holds for n. By the above remarks it suffices to show that for $f_1, \ldots, f_s \in R[X, Y]$ and $\sigma \in \{-1, 0, 1\}^s$, the theorem holds for A_σ. We apply cylindric decomposition to $f_1, \ldots, f_s$. This gives $B_1, \ldots, B_m$ a semialgebraic partition of R^n. By induction we may assume that each B_i is a cell. Let

$$C_{i,j} = \{(x, y) : x \in B_j, y = \xi_{i,j}(x)\}$$

for $j = 1, \ldots, l(i)$ and let

$$D_{i,j} = \{(x, y) : x \in B_j, \xi_{i,j}(x) < y < \xi_{i,j+1}(x)\}$$

for $j = 0, \ldots, l(i)$. The $C_{i,j}$ and $D_{i,j}$ are cells partitioning R^{n+1} such that each f_k has constant sign on each of the cells and A_σ is a finite union of cells of this kind.

In [K-P-S] it is shown that cell decomposition holds for any o-minimal theory. We can now extend 2.13 to R^n.

Corollary 3.4. If A is a semialgebraic subset of $\mathbf{R}^n$ and $f : A \to R$ is semialgebraic, then there is $B_1, \ldots, B_m$ a partition of A into semialgebraic sets such that $f|B_i$ is continuous for $i = 1, \ldots, m$.

Far more is true.

Definition. If A is a semialgebraic subset of R^n and $f : A \to R$ we say that f is *algebraic* if there is a polynomial $p(X_1, \ldots, X_n, Y)$ such that $p(x, f(x)) = 0$ for all $x \in A$.

Corollary 3.5. Every semialgebraic function is algebraic.

Proof.

Suppose $f : A \to R$ is semialgebraic. Apply cylindric decomposition to a family of polynomials $f_1, \ldots, f_s \in R[X, Y]$ which is closed under $\frac{\partial}{\partial Y}$ such that the graph of f can be defined in a quantifier free way using $f_1, \ldots, f_s$. Let $B_1, \ldots, B_m$ be a partition of R^n into cells given by cylindric decomposition. On each B_i there is a j such that $f|B_{i,j} = \xi_{i,j}$ and there is a $p_i \in \{f_1, \ldots, f_s\}$ such that $\xi_{i,j}(x)$ is an isolated zero of $p(x, Y)$ for all $x \in B_i$. Let $p = \prod p_i$. Then $p(x, f(x))$ for all $x \in A$.

For $\mathbf{R}$ we can say much more. In the above setting suppose U is an open subset of $\mathbf{R}^n$ contained in B_i. If $x \in U$, then since $\xi_{i,j}(x)$ is an isolated zero of p_i,

$$\frac{\partial p_i}{\partial Y}(x, \xi_{i,j}(x) \neq 0.$$

Thus the partial derivative is nonzero on all of B_i. By the implicit function theorem we see that $f|U$ is real analytic.

While "analytic functions" do not make sense in an arbitrary o-minimal structure, van den Dries [D1] showed that in an o-minimal expansion of an ordered field then for any definable function and any n we can partition the domain so that the function is piecewise $\mathcal{C}^n$

Definition. If $U \subset \mathbf{R}^n$ is an open semialgebraic and $f : U \to \mathbf{R}$ is semialgebraic and analytic, we say that f is a *Nash function*.

Corollary 3.5 shows that the study of semialgebraic functions reduces to the study of Nash functions.

The next lemma is proved by an easy induction. For the purpose of this lemma $\mathbf{R}^0 = \{0\}$.

Lemma 3.6. If A is a k-cell in $\mathbf{R}^n$, then there is a projection map $\pi : \mathbf{R}^n \to \mathbf{R}^k$ such that π is a homeomorphism from A to an open set in $\mathbf{R}^k$. Also if $k > 0$, there is a homeomorphism between A and $(0,1)^k$.

By Corollary 3.6, every cell in $\mathbf{R}^n$ is connected. This type of result will not hold for arbitrary real closed fields R because even R need not be connected. For example, if R is the real algebraic numbers $R = \{x : x < \pi\} \cup \{x : x > \pi\}$.

Let R be a real closed field. We say that a definable $X \subset R^n$ is *definably connected* if there are no definable open sets U and V such that $U \cap X$ and $V \cap X$ are disjoint and $X \subseteq U \cup V$. It is easy to see that in any real closed field cells are definably connected.

Cell decomposition easily implies the following important theorem of Whitney.

Theorem 3.7. If $A \subseteq \mathbf{R}^n$ is semialgebraic then $A = C_1 \cup \ldots \cup C_m$ where $C_1, \ldots, C_m$ are semialgebraic, connected and closed in A (ie. every semialgebraic set has finitely many connected components).

In real closed fields we can develop a dimension theory paralleling the theory for algebraically closed fields.

Definition. Let R be real closed and let K be a $|R|^+$-saturated elementary extension of R. If $a_1, \ldots, a_n \in K$, let dim $(\mathrm{a}_1, \ldots, \mathrm{a}_n/\mathrm{R})$ be the transcendence degree of $R(a_1, \ldots, a_n)$ over R. If A is a definable subset of R^n defined by $\phi(v_1, \ldots, v_n, \bar{b})$, let $A^K = \{\bar{x} \in K^n : K \models \phi(\bar{x}, \bar{b})\}$. Note that by model completeness, A^K does not depend on the choice of ϕ.

We define dim (A) the *dimension* of A to be the maximum of dim (ā/R) for $\bar{a} \in A^K$. Our final proposition shows that this corresponds to the topological and geometric notions of dimension.

Proposition 3.8. i) dim (A) is the largest k such that A contains a k-cell.

ii) dim (A) is the largest k such that there is a projection of A onto R^k with non-empty interior.

iii) dim (A) = dim (V) where V is the Zariski closure of A.

For further information on semialgebraic sets and real algebraic geometry the reader should consult [Di] or [BCR].

§4 **Definable Equivalence Relations**.

In algebra and geometry we often want to consider quotient structures. For this reason it is useful to study definable equivalence relations. The best we could hope for is that a definable equivalence relation has a definable set of representatives. This is possible in real closed fields. Let R be real closed.

Lemma 4.1. Let A be a definanble subset of R^{m+n}. For $a \in R^m$ let $A_a = \{x \in R^n : (a, x) \in A\}$. There is a definable function $f : R^m \to R^n$ such that $f(a) \in A_a$ for all $a \in R^m$ and $f(a) = f(b)$ if $A_a = A_b$. We call f an *invariant* Skolem function.

Proof. Let f be the Skolem function defined in 2.14. It is clear from the proof of 2.14 that $f(a) = f(b)$ whenever $A_a = A_b$.

Corollary 4.2. If E is a definable equivalence relation on a definable subset of R^n then there is a definable set of representatives.

In algebraically closed fields we will not usually be able to find definable sets of representatives. For example suppose $xEy \Leftrightarrow x^2 = y^2$, then by strong minimality E does not have a definable set of representatives. The next best thing would be if there is a definable function f such that $f(x) = f(y)$ if and only if $f(x) = f(y)$. Our next goal is to show this is true in algebraically closed fields.

Definition. Let T be any theory and let M be a suitably saturated model of T. Let $X \subset M^n$ be definable with parameters. We say that $\bar{b} \in M^n$ is a *canonical base* for X if and only if for any automorphism σ of M, σ fixes X setwise if and only if $\sigma(\bar{b}) = \bar{b}$.

We say that T *eliminates imaginaries* if and only if every definable subset of M^n has a canonical base.

We first illustrate the connection between elimination of imaginaries and equivalence relations.

Lemma 4.3. Suppose T eliminates imaginaries and at least two elements of M are definable over $\emptyset$. If E is a definable equivalence relation on M^n, there is a definable $f : M^n \to M^m$ such that $x\ E\ y$ if and only if $f(x) = f(y)$.

Proof.

We first show that for any formula $\phi(v, a)$ there is a formula $\psi_a(v, w)$ and a unique b such that

$$\phi(v, a) \leftrightarrow \psi_a(v, b).$$

By elimination of imaginaries we can find a canonical base b for $X = \{v : \phi(a, v)\}$. Clearly X must be definable over b. Thus there is a formula $\psi(v, w)$ such that $X = \{v : \psi(v, b)\}$. Further there is a formula $\theta(w)$ such that $\theta(b)$ and if $c \neq b$ and $\theta(c)$, then $\psi(v, c)$ does not define X. Let $\psi_a(v, w)$ be $\theta(w) \wedge \psi(v, w)$.

By compactness we can find $\psi_1, \ldots, \psi_n$ such that one of the ψ_i works for each a. By the usual coding tricks we can reduce to a single formula ψ (a sequence of parameters made up of the distinguished elements is added to the witness b to code into the parameters the least i such that ψ_i works for a).

The lemma follows if we let $\phi(v, w)$ be $v\ E\ w$ and let $f(a)$ be the unique b such that $v\ E\ a$ if and only if $\psi(v, b)$.

We will show that algebraically closed fields eliminate imaginaries. This will follow from the following two lemmas.

Lemma 4.4. Let K be a saturated algebraically closed field and let $X \subset K^n$ be definable. There is a finite $C \subset K^m$ such that if σ is an automorphism of K, then σ fixes X setwise if and only if σ fixes C setwise.

Proof.

Let $\phi(\bar{v}, a_1, \ldots, a_m)$ define X. Consider the equivalence relation E on K^m given by

$$\bar{a}\ E\ \bar{b} \Leftrightarrow (\phi(\bar{v}, \bar{a}) \leftrightarrow \phi(\bar{v}, \bar{b})).$$

Let α denote the equivalence class $\bar{a}/E$. Any automorphism of σ fixes X setwise if and only if it fixes α. (Note: α is an example of an "imaginary" element that we would like to eliminate.) We say that an element $x \in K$ is algebraic over α if and only if there are only finitely many conjugates of x under automorphisms which fix α.

Our first claim is that there is $\bar{b} \in K^m$ algebraic over α such $\bar{a}\ E\ \bar{b}$. Choose $\bar{b}$ such that $\bar{b}\ E\ \bar{a}$, and $j = |\{i \le m : b_i \text{ is algebraic over } \alpha\}|$ is maximal. We must show that $j = m$. Suppose not. By reordering the variables we may assume that $b_1, \ldots, b_j$ are algebraic over α and b_i is not algebraic over α for $i > j$. Let

$$Y = \{x \in K : \exists y_{j+2} \ldots \exists y_n\ (b_1, \ldots, b_j, x, y_{j+2}, \ldots, y_n) \in X \text{ and}$$
$$(b_1, \ldots, b_j, x, y_{j+1}, \ldots, y_n)\ E\ \bar{a}\}.$$

Clearly $b_{j+1} \in Y$. If Y is finite, then any element of Y is algebraic over $b_1, \ldots, b_j, \alpha$, and hence algebraic over α. Thus by choice of $\bar{b}$, Y is finite. If Y is infinite, then since K is strongly minimal, Y is cofinite. In particular they is $d \in K$ such that d is algebraic over $\emptyset$. But then we can find $d_{j+2}, \ldots, d_m$ such that $(b_1, \ldots, b_j, d, d_{j+2}, \ldots, d_m)/E = \alpha$ and $b_1, \ldots, b_j, d$ are algebraic over α. contradicting the maximality of j.

Let C be the set of all conjugates of $\bar{b}$ under automorphisms fixing α. So C is fixed setwise by any automorphism which fixes α. If $\bar{c} \in C$, then $\bar{c}/E = \alpha$. Thus α is fixed under all automorphisms which permute C. In particular an automorphism fixes X setwise if and only if it fixes C setwise.

The proof above is due to Lascar and Pillay and works for any strongly minimal set D where the algebraic closure of $\emptyset$ is infinite.

The second step is to show that if $C \subset K^m$ is finite, then there is $\bar{b} \in K^l$ such that any automorphsim of K fixes C setwise if and only if it fixes $\bar{b}$ pointwise. This step holds for any field

Lemma 4.5. Let F be any field. Let $\bar{b}_1, \ldots, \bar{b}_m \in F^n$. There is l and a $\bar{c} \in F^l$ such that if σ is any automorphism of F, then $\sigma\bar{c} = \bar{c}$ if and only if σ fixes $C = \{\bar{b}_1, \ldots, \bar{b}_m\}$ setwise.

Proof.

This is very easy if $n = 1$. If $b_1, \ldots, b_m \in F$, consider the polynomial

$$p(X) = \prod_{i=1}^{m}(X - b_i) = X^m + \sum_{i=0}^{m-1} c_i X^i.$$

Then an automorphism of F fixes $\{b_1, \ldots, b_m\}$ setwise if and only if it fixes $(c_0, \ldots, c_{m-1})$. Here $c_0, \ldots, c_{m-1}$ are obtained by applying the elementary symmetric functions to $b_1, \ldots, b_m$.

The general case is an easy amplification of that idea. Suppose $\bar{b}_i = (\beta_{i,1}, \ldots, \beta_{i,n})$. Let

$$q_i(X_1, \ldots, X_m, Y) = Y - \sum_{i=1}^{n} \beta_{i,j} X_j$$

for $i = 1, \ldots, m$. Let

$$p(\bar{X}, Y) = \prod_{i=1}^{m} q_i(\bar{X}, Y).$$

By unique factorization, an automorphsim of K fixes p if and only if it permutes the q_i if and only if it permutes the $\bar{b}_i$. Let $\bar{c}$ be the coefficients of $p(\bar{X}, Y)$.

Corollary 4.6. (Poizat [P]) The theory of algebraically closed field eliminates imaginaries.

In [M2] we give a different proof of elimination of imaginaries for algebraically closed fields using "fields of definition" from algebraic geometry (see [L2]).

Suppose E is a definable equivalence relation on K. If any $\sim$-class is infinite, then there is a unique cofinite class. Suppose all $\sim$ classes are finite. There is a number n such that all but finitely many equivalence classes have size n. Let B be the number of points not in a class of size n. A moment's thought shows that the best we can hope to do is characterize the possible values of $|B|(\text{mod n})$.

Theorem 4.7. (van den Dries-Marker-Martin [D-M-M]) Let K be an algebraically closed field of characteristic zero and let $\sim$ be a definable equivalence relation on K where all but finitely many classes have size n. Let B be the set of points not in a class of size n. Then $|B| = 1(\text{mod n})$.

Albert generalized theorem 4.7. We give his argument here. Since the projective line $\mathbf{P}^1$ is $K \cup \{\infty\}$ and the Euler characteristic of $\mathbf{P}^1$ is 2, theorem 4.7 is a corollary to the following result of Albert.

Theorem 4.8 Let K be a field of characteristic zero and let C be a smooth projective curve over K. If $\sim$ is a definable equivalence relation on K where almost all classes have size n and B is the number of points not in a class of size n, then $|B| = \chi(C)(\mathrm{mod\ n})$, where $\chi(C)$ is the Euler characteristic of C mod n.

Our proof of 4.8 will use the following simple combinatorial fact.

Lemma 4.9. Let $\sim_0$ and $\sim_1$ be equivalence relation on C such that all but finitely many E_i-classes have size n for $i = 1, 2$. Let $B_i = \{x \in C : |x/\sim_i| \neq n\}$. Suppose for all but finitely many x, $x/\sim_0 = x/\sim_1$, then $|B_0| = |B_1|(\mathrm{mod\ n})$.

Proof of 4.8

Suppose $C \subset \mathbf{P}^m$. Let $C_0 = C \cap K^m$. By 4.6 there is a definable $f : C_0 \to K^l$ such that $x \sim y$ if and only if $f(x) = f(y)$ for $x, y \in C_0$. By 1.11 there is a Zariski open $U \subseteq C_0$ and a rational $\rho : U \to K^l$ such that $f|U = \rho$. Let C_1 be the Zariski closure of the image of C_0 under ρ. Then C_1 is an irreducible affine curve. There is a smooth projective curve C_2, an open $V \subset C_2$, and a rational one-to-one $\tau : V \to C_1$ (see [H] for the facts about curves used in this proof). The composition $\tau \circ \rho$ maps a dense open subset of C into C_2. There is a total rational $g : C \to C_2$ extending $\tau \circ \rho$. There is a cofinite subset Z of C such that $g(x) = g(y)$ if and only if $x \sim y$ for $x, y \in Z$. Consider the equivalence relation $\sim_1$ on C given by $x \sim_1 y$ if and only if $g(x) = g(y)$. By 4.9 we may assume $\sim = \sim_1$.

Let (V, E, F) be a triangulation of C_2 such that the set of verticies V contains $V_0 = \{g(x) : x \in B\}$. Let (V^*, E^*, F^*) be the triangulation of C obtained by pulling back the triangulation of C_2. Since the edges and faces do not contain images of points in B, $|E^*| = n|E|$ and $|F^*| = n|F|$, while $|V^*| = |B| + n|V - V_0|$.

Thus

$$\begin{aligned}\chi(C) &= |B| + n|V - V_0| - n|E| + n|F| \\ &= |B|(\mathrm{mod\ n}).\end{aligned}$$

The situation in characteristic p is more complex.

Theorem 4.10.([D-M-M]) Let K be an algebraically closed field of characteristic p and let $\sim$ be a definable equivalence relation on K such that all but finitely many $\sim$-classes have size n. Let B be the set of points not in a class of size n.

i) If $n < p$, then $|B| = 1(\mathrm{mod\ p})$.

ii) If $n = p = 2$, then $|B| = 0(\mathrm{mod\ p})$.

iii) If $n = p + s$ where $1 \leq s \leq \frac{p}{2}$, then $|B| \neq p + 1(\mathrm{mod\ n})$.

iv) Everything else is possible.

A consequence of Hurwitz theorem (see [H]) is that if X and Y are smooth projective curves and $f : X \to Y$ is a non-trivial rational map, then the genus of Y is at most the genus of X. This has two interesting consequences for us. First, in the proof of 4.9, if $C = \mathbf{P}^1$, then the curve C_2 has genus zero and we may assume that C_2 is $\mathbf{P}^1$. Thus if $\sim$ is a definable equivalence relation on K there is a rational function $f : K \to K$ such that there is a Zariski open $U \subseteq K$ such that $x \sim y \Leftrightarrow f(x) = f(y)$ for all but $x, y \in U$ (this is proved in [D-M-M] by an appeal to Lüroth's theorem).

Second, let C be a curve of genus $g \geq 1$. View C as a structure by taking as relations all definable subsets of C^n. This is a strongly minimal set which does eliminate imaginaries. Suppose, for example, that $C \subset K^2$. Let $\sim$ be the equivalence relation on C given by $(x, y) \sim (u, v)$ if and only if $x = u$. Then $C/\sim$ is essentially K. If we could eliminate imaginaries there would be a definable map $f_0 : C/\sim \to C^n$ and by composing with a projection, there would be a nontrivial definable map from $C/\sim$ to C. As in the proof of 4.9 this induces a rational map from $\mathbf{P}^1$ into C, violating Hurwitz's theorem.

§5 ω-stable groups.

In this section we will survey some of the basic properties of ω-stable groups. Comprehensive surveys of these subjects can be found in [BN], [Po3] and [NP]. Here we assume passing acquaintance with the results about ω-stable theories. The reader is referred to [B1], [Pi1] and [$Po4$].

Definition. An *ω-stable group* is an ω-stable structure $(G,\cdot,\ldots)$ where $(G,\cdot)$ is a group.

Lemma 5.1. (Baldwin-Saxel [BS]) An ω-stable group has no infinite chain of definable subgroups.

Proof.

Let $H_0 \supset H_1 \supset \cdots$ be an infinite descending chain of definable subgroups. We can find elements $\{a_\sigma : \sigma \in 2^{<\omega}\}$ such that

i) if $\sigma \supset \tau$ then $a_\sigma H_{|\sigma|} \subset a_\tau H_{|\tau|}$, and

ii) if $a_{\sigma 1} H_{|\sigma|+1}$ and $a_{\sigma 0} H_{|\sigma|+1}$ are distinct cosets.

This gives a countable set of parameters over which there are $2^{\aleph_0}$ types, contradicting ω-stability.

Definition. A group G is *connected* if it has no definable subgroup of finite index.

Lemma 5.2. If G is an ω-stable group, then there is G^0 a definable connected subgroup of G of finite index.

Proof.

If not then we can build an infinite descending sequence of finite index subgroups.

We call G^0 the *connected component* of G. Note that G^0 is fixed by all group automorphisms of G.

Definition. If $A \subset G$ we say that $p(v) \in S_1(A)$ is a *generic type* over A if $\mathrm{RM}(p) = \mathrm{RM}(G)$.

Generic types are our main tool in studying ω-stable groups. We begin by summarizing basic facts about generic types. We fix G an ω-stable group.

Lemma 5.3. i) There are only finitely many types generic over A.

ii) If b is generic over A and $a \in A$, then ab and b^{-1} are generic over A.

iii) Any element of G is the product of two generics (in an elementary extension).

Proof.

i) There are only finitely many types of maximal rank.

ii) The maps $x \mapsto ax$ and $x \mapsto x^{-1}$ are definable bijections and definable bijections preserve rank.

iii) Let $a \in G$. Let b be generic. Then ab^{-1} is also a generic and $a = (ab^{-1})b$.

Lemma 5.4. An ω-stable group G is connected if and only if there is a unique generic type in $S_1(G)$.

Proof.

Suppose H is a proper definable subgroup of finite index. Then each coset of H contains a type of maximal Morley rank. Thus the generic type is not unique.

On the other hand suppose $p_1, \ldots, p_n$ are the generic types of G. Let $H = \{g \in G :$ for all realizations b of p_1 (in, say, a saturated elementary extension), gb is also a realization of $p_1\}$. We call H the *left-stabilizer* of p in G.

claim. H is definable.

There is a formula $\theta(v)$ which isolated p_1 from the other generic types. Then $H = \{g : \theta(g \cdot v) \in p_1\}$. By definability of types there is a formula $d\theta(w)$ such that $G \models d\theta(w)$ if and only if $\theta(g \cdot v) \in p_1$. Clearly $H = \{g : d\theta(g)\}$.

Suppose b realizes p_1 (in an elementary extension) and $a \in G$, then ab realizes p_i for some i. Thus the coset aH contains a generic. Hence H has finite index so $H = G$. Similarly G stabilizes each p_i. A similar argument works for right stabilizers.

Let a and b be independent realizations of p_1 and p_2. Let p_1^* be the heir of p_1 to $G \cup \{b\}$ (ie. p_1^* is the unique extension of p_1 to $G \cup \{b\}$ of maximal rank). By the above arguments b stabalizes p_1^*, thus ba realizes p_1^* and, in particular, ba realizes p_1. A similar argument (using right stabilizers) shows that ba realizes p_2.

We now have enough tools to prove the following theorem of Macintyre ([Mac]).

Theorem 5.5. Let $(K, +, \cdot, \ldots)$ be an infinite ω-stable field. Then K is algebraically closed.

Proof.

Suppose K is not algebraically closed. Let F be a finite Galois extension of K. There is L such that $K \subseteq L \subset F$ and the Galois group of F/L is a cyclic extension of prime order q. Since L is a finite extension of K, we can interpret L in K. Thus L is ω-stable so we may, without loss of generality assume that F/K is cyclic of prime order. By Galois theory (see [L1]) $F = K(\alpha)$ where either $q \neq p$ and $\alpha^q \in K$ or $q = p$ and $\alpha^p + \alpha \in K$.

We first show that $(K, +, \ldots)$ is connected. Suppose not. Let H be the connected component. For any $a \in K$, $x \mapsto ax$ is an automorphism of $(K, +)$ and hence preserves H. But then H is a proper ideal of K, a contradiction.

Since $(K, +)$ is connected, there is a unique type of maximal rank. Thus there is a unique type of maximal rank in the group $(K^\times, \cdot, \ldots)$ and hence it is connected.

Consider the multiplicative homomorphism $x \mapsto x^n$. If a is a generic of K, then, since a is algebraic over a^n, $\mathrm{RM}(a^n) = \mathrm{RM}(a)$. Thus $\{x^n : x \in K^\times\}$ is a subgroup of $K^\times$ of maximal rank. Since $K^\times$ is connected, every element of K has an n^{th}-root in K. This rules out the case $\alpha^q \in K$.

Suppose K has characteristic $p > 0$. Consider the additive homomorphism $x \mapsto x^p + x$. As above if a is generic, so is $a^p + a$. Thus since the additive group is connected, for any $b \in K$, there is a solution to $X^p + X = b$. This rules out the case $\alpha^p + \alpha \in K$.

As an aside, we note the following theorem of Pillay and Steinhorn ([PS]) can be thought of as the real version of Macintyre's theorem.

Theorem 5.6. Let $(F, +, \cdot, <, \ldots)$ be an o-minimal ordered field. Then F is real closed.

Proof.

Let $f(X) \in F[X]$. Suppose $a, b \in F$, $a < b$ and $f(a) < 0 < f(b)$. Consider the set $X^- = \{x \in (a,b) : f(x) < 0\}$ and $X^+ = \{x \in (a,b) : f(x) > 0\}$. Since f is continuous X^- and X^+ are open. By o-minimality there is $c \in (a,b) \setminus (X^- \cup X^+)$. Clearly $f(c) = 0$. By 2.1, F is real closed.

One important problem in the model theory of groups is to understand the simple groups of finite Morley rank.

Cherlin's Conjecture. Every simple group of finite Morley rank is an algebraic group over an algebraically closed field.

We recall the definition of an algebraic group.

Definition. An *abstract variety* is a topological space B with a finite open cover $U_1, \ldots, U_n$, affine Zariski closed sets $V_1, \ldots, V_n$ and homeomorphisms $f_i : U_i \to V_i$ such that if $V_{i,j} = f_i(U_i \cap U_j)$ and $f_{i,j} : V_{i,j} \to V_{j,i}$ is the map $f_j \circ f_i^{-1}$, then $V_{i,j}$ is Zariski open and $f_{i,j}$ is a morphism. If W is a second abstract variety with cover $Z_1, \ldots, Z_m$ where $g_i : Z_i \to W_i$ is a homeomorphism onto an affine Zariski closed set, then $h : V \to W$ is a *morphism* if all the maps $h_{i,j} : V_i \to W_j$ by $g_j \circ h \circ f_i^{-1}$ are morphisms of affine varieties.

Abstract varieties are the algebraic-geometric analog of manifolds. Clearly affine and projective varieties are examples of abstract varieties, as are open subsets of projective varieties. We drop the modifier "abstract".

Definition. An *algebraic group* is a group $(G, \cdot)$ where G is a variety and $\cdot$ and inverse are morphisms.

The standard examples of algebraic groups are matrix groups. For example consider $GL_n(K)$, the invertible $n \times n$ matrices. As the underlying set we take $\{(a_{i,j}, b) \in K^{n^2+1} : b \det(a_{(i,j)}) = 1\}$. This is a Zariski closed set in affine $n^2 + 1$-space. The extra dimension codes the fact that the determinant is non-zero. Matrix multiplication is easily seen to be given by polynomials. Using Cramer's rule one sees that the inverse is also given by polynomials.

The group law on an elliptic curve is an example of a non-affine algebraic group.

It is easy to see that every algebraic group G over an algebraically closed field K is interpretable in K. Thus, by elimination of imaginaries, G is isomorphic to a constructible group. *A priori* one might expect there to be constructible groups which are not isomorphic to algebraic groups. This is not the case.

Theorem 5.7. (van den Dries [D4]) Let K be an algebraically closed field. Every constructible group over K is K-definably isomorphic to an algebraic group.

Van den Dries' proof uses a theorem of Weil's on group chunks. Weil's theorem actually shows that if V is an irreducible variety and $f : V \times V \to V$ is a generically surjective rational map such that $f(x(f(y,z)) = f(f(x,y),z)$ for independent generic x, y, z, then there is a birationaly equivalent algebraic group G, such that generically f agrees with the multiplication of G.

Hrushovski (see [Bo1] or [Po3]) gave a model theoretic proof of theorem 5.7 avoiding Weil's theorem. In [Hr1] Hrushovski proved the following result which can be though of a general model theoretic form of Weil's theorem.

Theorem 5.8. (Hrushovski) Let T be an ω-stable theory. Let $p \in S_n(A)$ be a stationary type and let f be a partial A-definable function such that

i) if a and b are independent realizations of p, then $f(a,b)$ realizes p and $f(a,b)$ is independent over A from a and b separately, and

ii) if a, b and c are independent realizations of p, then $f(a, f(b,c)) = f(f(a,b),c)$.

Then there is a definable connected group $(G, \cdot)$ such that p is the generic type of G and if a, b are independent generics of G, then $a \cdot b = f(a,b)$.

Pillay [Pi2] proved the following o-minimal analog of theorem 5.6.

Theorem 5.9. If G is a group definable in an o-minimal expansion of $\mathbf{R}$, then G is definably isomorphic to a Lie Group.

Finally we remark that Peterzil, Pillay and Starchenko have recently proved the following o-minimal analog of Cherlin's conjecture.

Theorem 5.10. If G is a simple group definable in an o-minimal theory, then there is a definable real closed field K such that G is definably isomorphic to a group definable in K. Indeed there is an algebraic group H definable over K such that G is definably isomorphic to H^0.

§6 Expansions and reducts of algebraically closed fields.

Suppose D is a strongly minimal set. The algebraic closure relation on D has the following properties.

i) $X \subseteq \mathrm{acl}(X)$,

ii) $\mathrm{acl}(\mathrm{acl}(X)) = \mathrm{acl}(X)$,

iii) if $a \in \mathrm{acl}(X, b) \setminus \mathrm{acl}(X)$, then $b \in \mathrm{acl}(X, a)$, and

iv) if $a \in \mathrm{acl}(X)$, then there is a finite $X_0 \subset X$ such that $a \in \mathrm{acl}(X_0)$.

We say that $X \subset D$ is *independent* if $x \notin \mathrm{acl}(X \setminus \{x\}$, for all $x \in X$. We say that X is a *basis* for A if $A \subseteq \mathrm{acl}(X)$ and X is independent. A simple generalization of the arguments from linear algebra show that any two basis for A have the same cardinality. We call this cardinality dim A.

Definition. We say that a strongly minimal set D is *trivial* if whenever $A \subseteq D$, then

$$\mathrm{acl}(A) = \bigcup_{a \in A} \mathrm{acl}(a).$$

We say that D is *modular* if

$$\dim\,(A \cup B) = \dim\, A + \dim\, B - \dim\,(A \cap B)$$

for any finite dimensional algebraically closed $A, B \subseteq D$.

We say that D is *locally modular* if we can name one point and make it modular (this is equivalent to being make it modular by naming a small number of points).

The theory of $\mathbf{Z}$ with the successor function $x \mapsto x + 1$ is a trivial strongly minimal set. Here $a \in \mathrm{acl}(X)$ if and only if $a = s^n(x)$ for some $n \in \mathbf{Z}$ and $x \in X$.

If V is a vector space over the rationals. The strongly minimal set $(V, +)$ is modular. Here $\mathrm{acl}(X)$ is the linear span of X. We can modify this to give a locally modular example. Consider (V, f) where f is the ternary function $f(x, y, z) = x + y - z$. In this language, $\mathrm{acl}(X)$ is the smallest coset of a linear subspace that contains X. For example $\mathrm{acl}(a) = \{a\}$ and $\mathrm{acl}(a, b)$ is the line containing a and b. It is easy to see that (V, f) is not modular. Let a, b, c be independent points and let $d = c + b - a$. Then $\dim\,(a, b, c, d) = 3$ while $\dim\,(a, b) = \dim\,(c, d) = 2$ and $\mathrm{acl}(a, b) \cap \mathrm{acl}(c, d) = \emptyset$. On the other hand if we name 0, we are essentially back to the structure $(V, +)$.

Let K be an algebraically closed field of infinite transcendence degree. We claim that $(K, +, \cdot)$ is not locally modular. Let k be an algebraically closed subfield of transcendence degree n. We will show that even localizing at k the geometry is not modular. Let a, b, x be algebraically independent over k. Let $y = ax + b$. Then $\dim\,(k(x, y, a, b)) = 3 + n$ while $\dim\,(k(x, y)) = \dim\,(k(a, b)) = 2$. But $\mathrm{acl}(k(x, y)) \cap \mathrm{acl}(k(a, b)) = k$ contradicting modularity. To see this suppose $d \in k_1 = acl(k(a, b))$ and y is algebraic over $k(d, x)$. Let $k_1 = \mathrm{acl}(k(d))$. Then there is $p(X, Y) \in k_1[X, Y]$ an irreducible polynomial such that $p(x, y) = 0$. By model completeness $p(X, Y)$ is still irreducible over $\mathrm{acl}(k(a, b))[X, Y]$.

Thus $p(X,Y)$ is $\alpha(Y-aX-b)$ for some $\alpha\in \mathrm{acl}(k(a,b))$ which is impossible as then $\alpha\in k_1$ and $a,b\in k_1$.

The geometry of strongly minimal sets has been one of the most important topics in model theory for the last decade. Much of this work was motivated by the following conjecture.

Zilber's Conjecture. If D is a non-locally modular strongly minimal set, then D is bi-interpretable with an algebraically closed field.

Zilber's conjecture was refuted by Hrushovski in [Hr2] (see also [BSh]). Though false Zilber's conjecture led to two interesting problems about algebraically closed fields.

Expansion Problem: Can an algebraically closed field have a nontrivial strongly minimal expansion?

Interpretability Problem: Suppose D is a non-locally modular strongly minimal set interpretable in an algebraically closed field K . Does D interpret K?

In [Hr3] Hrushovski showed that there are nontrivial strongly minimal expansions of algebraically closed fields. Indeed, one can find a strongly minimal structure $(F,+,\cdot,\oplus,\odot)$ such that $(F,+,\dot{)}$ and $(F,\oplus,\odot)$ are algebraically closed fields of different characteristics! Prior to Hrushovski's work several positive results were obtained. The first is an unpublished result of Macintyre.

Proposition 6.1. If $f:\mathbf{C}\to\mathbf{C}$ is a non-rational analytic function,then $(\mathbf{C},+,\cdot,f)$ is not strongly minimal.

Proof.
Suppose not. By strong minimality f must have only finitely many zeros and poles. Thus (see [L3]) $f(x)=g(x)e^{h(x)}$ where g is rational and h is entire. Since g is definable so is $f_0(x)=e^{h(x)}$. But f_0 is infinite to one, so the inverse image of some point is infinite and cofinite, contradicting strong minimality.

Is this structure stable?

Definition. Suppose $S\subset\mathbf{R}^{2n}$. Let

$$\widehat{S}^*=\{(a_1+a_2i,\ldots,a_{2n-1}+a_{2n}i)\in\mathbf{C}^n:(a_1,\ldots,a_{2n})\in S\}.$$

A *semialgebraic* expansion of $\mathbf{C}$ is an expansion $(C,+,\cdot,S^*)$ where $S\subseteq R^{2n}$ is semialgebraic.

There are two obvious ways to get a semialgebraic expansion. The first is to add a predicate for a set which is already constructible. The second is to add a predicate for $\mathbf{R}$. The next theorem shows that these are the only two possibilities. Since the reals are unstable, this shows in a very strong way that there are no nontrivial strongly minimal semialgebraic expansions of $\mathbf{C}$.

Theorem 6.2([M1]) If $\mathcal{A} = (\mathbf{C}, +, \cdot, S^*)$ is a semialgebraic expansion then $\mathbf{R}$ is $\mathcal{A}$-definable.

We will prove this theorem using four lemmas. The first lemma is the basic step. We omit the proof, but remark that it works in a more general setting.

Lemma 6.3 If $\mathcal{A} = (\mathbf{C}, +, \cdot, S^*)$ where S^* is an infinite coinfinite subset of $\mathbf{C}$ definable and S is definable in an o-minimal expansion of $\mathbf{R}$, then $\mathbf{R}$ is definable in $\mathcal{A}$.

We give here a proof of 6.2 from 6.3 which is more direct that the original argument from [M1] and is based on an argument from [Hr3]. Assume that S^* is not constructible and $\mathbf{R}$ is not definable. By 6.3 we may assume that every $\mathcal{A}$-definable subset of $\mathbf{C}$ is finite or cofinite. Since $\mathbf{C}$ is uncountable, this suffices to show that the structure $\mathcal{A}$ is strongly minimal. The next lemma of Hrushovski shows that we may assume that $S^* \subseteq \mathbf{C}^2$. It replaces a less general inductive argument using Bertini's theorem.

Lemma 6.4. If $X \subseteq \mathbf{C}^n$ is non-constructible and $\mathcal{A} = (\mathbf{C}, +, \cdot, S^*)$ is strongly minimal, then there is a non-constructible $\mathcal{A}$-definable $h : \mathbf{C} \to \mathbf{C}$.

Proof.

Without loss of generality assume that every definable subset of $\mathbf{C}^m$ is constructible for $m < n$. Let $X_a = \{x \in \mathbf{C}^{n-1} : (a, x) \in X\}$ for $a \in \mathbf{C}$. Each X_a is constructible. Thus for each $a \in \mathbf{C}$ we can find a number m_a, a formula $\phi_a(v_1, \ldots, v_{n-1}, w_1, \ldots, w_{m_a})$ in $\mathcal{L}_{\mathrm{r}}$, and parameters $b_a \in \mathbf{C}^{m_a}$ such that

$$x \in X_a \Leftrightarrow \phi_a(x, b_a).$$

Since $\mathcal{A}$ is saturated, compactness insures there are formulas $\phi_1, \ldots, \phi_k$ such that for each a at least one of the ϕ_i works. By standard coding tricks one formula $\phi(v_1, \ldots, v_n, w_1, \ldots, w_m)$ suffices.

Define an equivalence relation E on $\mathbf{C}^m$ by

$$a\ E\ b \Leftrightarrow \forall x\ \Big(\phi(x, a) \leftrightarrow \phi(x, b)\Big).$$

By elimination of imaginaries, there is a constructible function $g : \mathbf{C}^m \to \mathbf{C}^l$ such that $a\ E\ b$ if and only if $g(a) = g(b)$.

Define $f : \mathbf{C} \to \mathbf{C}^l$ by

$$f(a) = y \leftrightarrow \forall b\ \Big(\forall z\ (\phi(z, b) \leftrightarrow z \in X_a) \to g(b) = y\Big).$$

Clearly f is definable and $(a, y) \in X \Leftrightarrow \exists b\ (g(b) = f(a) \wedge \phi(y, b))$. Since g is constructible and X is not, f is not constructible. Let h be a non-constructible coordinate of f.

Lemma 6.5. Suppose S^* is semialgebraic and non-constructible. Let h be as in 6.4 and let H be it graph. There is an irreducible curve C such that $H \cap C$ and $C \setminus H$ are infinite.

Proof. In our setting h is semialgebraic. Consider the following two predicates over $\mathbf{R}$:

$$\mathbf{R}_0(x,y) \leftrightarrow \exists z\ h(x) = y + zi$$

$$\mathbf{R}_1(x,z) \leftrightarrow \exists y\ h(x) = y + zi$$

Let V_i be the Zariski closure of R_i in $\mathbf{R}^2$. Each R_i is one dimensional, thus, by 3.8, each V_i has dimension one. In particular, since each one dimensional irreducible component of V_i is a curve, we can find non-trivial polynomials $f_i(X,Y)$ such that

$$R_i(x,y) \to f_i(x,y) = 0.$$

We now move back to $\mathbf{C}$. Let

$$A_0 = \{(x,y,z,w) \in \mathbf{C}^4 : f_0(x,y) = f_1(x,z) = 0 \wedge w = y + zi\}.$$

Let

$$A = \{(x,w) : \exists y, z\ (x,y,z,w) \in A_0\}.$$

Clearly A and A_0 are constructible and one dimensional. Moreover $(x,h(x)) \in A$ for $x \in \mathbf{R}$. Thus by strong minimality $(x,h(x)) \in A$ for all but finitely many $x \in \mathbf{C}$. Thus there is C an irreducible component of the Zariski closure of A such that$(x,h(x)) \in \mathbf{C}$ for all but finitely many $x \in \mathbf{C}$. Since h is not constructible, for a generic x there is more than one y such that $(x,y) \in C$. Thus $H \cap C$ and $C \setminus H$ are infinite.

The following lemma of Hrushovski finishes the proof. In [M1] this was proved in the semialgebraic case by appealing to a weak version of the Riemann-Roch theorem.

Lemma 6.6. Let $\mathcal{A} = (\mathbf{C}, +, \cdot, X)$ be a nontrivial expansion of $\mathbf{C}$, where X is an infinite coinfinite subset of an irreducible curve C. Then $\mathcal{A}$ is not strongly minimal.

Proof.

We assume $\mathcal{A}$ is strongly minimal. The proof breaks into cases depending on the genus of C. If C has genus 0 there is a Zariski open $U \subseteq C$ and a one to one rational $\rho : U \to \mathbf{C}$. Clearly $\rho(X)$ is an infinite coinfinite subset of $\mathbf{C}$.

Any curve is birationally equivalent to a smooth projective curve. Since projective curves can be interpreted in $\mathbf{C}$ and rational maps are definable, we may, without loss of generality, assume that C is a smooth projective curve.

If C has genus 1, then there is a morphism $\oplus : C \times C \to C$ making C a divisible abelian group (see [H] or [F]). We consider the ω-stable group $\mathcal{G} = (C, \oplus, X)$. The sets X and $C \setminus X$ are Morley rank one subsets of C. Thus there are distinct types of maximal Morley rank. Hence, by 5.4, $\mathcal{G}$ has a definable subgroup of finite index. But a divisible abelian group has no finite index subgroups, a contradiction.

If C has genus $g > 1$, we must pass to $J(C)$ the *Jacobian Variety* of C. We summarize the facts we use (see [L2] or [Mu]). (Note: If C has genus 1, then $J(C) = C$.)

i) $J(C)$ is an irreducible g dimensional variety.

ii) There is a rational $\rho : \mathbf{C}^g \to J(C)$ which takes g independent generic points of C to the generic of $J(C)$.

iii) There is a morphism $\oplus : J(C) \times J(C) \to J(C)$ making $J(C)$ a divisible abelian group.

By ii) $\rho(X^g)$ and $\rho((C \setminus X)^g)$ both have Morley rank g. Thus, as in the genus 1 case, we are lead to a contradiction

That concludes to proof of theorem 6.2.

Here are three natural open questions related to the expansion problem. Let K be algebraically closed.

1) Is there a non-trivial infinite multiplicative subgroup G of K such that $(K, +, \cdot, G)$ has finite Morley rank?

2) Suppose K has characteristic $p > 0$. Is there a non-trivial infinite additive subgroup G of K such that $(K, +, \cdot, G)$ has finite Morley rank? The answer is no if K has characteristic zero ([Po3]).

3) Suppose K has characteristic $p > 0$. Is there an undefinable automorphism σ of K such that $(K, +, \cdot, \sigma)$ is strongly minimal?

The Interpretability Problem is still open. An important special case was proved by Rabinovich [R].

Theorem 6.7. Let K be algebraically closed and let $X_1, \ldots, X_n$ be constructible. If $\Omega = (K, X_1, \ldots, X_n)$ is non-locally modular, then Ω interprets and algebraically closed field isomorphic to K.

Prior to Rabinovich's theorem results were know in some special cases.

Theorem 6.8. (Martin[Ma]) Let $\rho : \mathbf{C} \to \mathbf{C}$ be a non-linear rational function. Then multiplication is definable in $(\mathbf{C}, +, \rho$.

The next result gives a complete description of reducts of $\mathbf{C}$ that contain $+$. For each $a \in \mathbf{C}$, let $\lambda_a(x) = ax$. We say that a subset $X \subset \mathbf{C}^n$ is *module definable* if it is definable in the structure $(\mathbf{C}, +, \lambda_a : a \in \mathbf{C})$. If X is module definable, then there is no field definable in $(\mathbf{C}, +, X)$. This is the only restriction.

Theorem 6.9. (Marker-Pillay [MP]) If X is constructible but not module definable, then multiplication is definable in $(\mathbf{C}, +, X)$.

There are three steps to the proof. The main step is due to Rabinovich and Zilber. The proof below, follows their basic ideas, but is simplification of their original argument.

Theorem 6.10 If C is an irreducible non-linear curve, then there is a field interpretable in $\mathcal{A} = (\mathbf{C}, +, C)$.

Proof. (sketch)

Without loss of generality we assume that $(0,0) \in \mathbf{C}$. If $p \in C$, let C_p be the curve obtained by translating p to the origin. If p is a nonsingular point on C, let $m(p)$ be the slope of the curve at p. Let C and D be curves through the origin. We define two new curves

$$C \oplus D = \{(x, y+z) : (x,y) \in C, (x,z) \in D\}$$

and

$$C \otimes D = \{(x,z) : \exists y \ (x,y) \in C \wedge (y,z) \in D\}.$$

If C and D have slopes m and n at the origin, then, if they are smooth at (0,0), $C \oplus D$ and $C \otimes D$ respectively have slopes $m+n$ and mn at the origin.

We show how to define a "fuzzy" field structure on C. Let a and b be independent generic points of C. There is a point d on C such that $m(a) + m(b) = m(d)$. We show that d is algebraic over a and b.

Let D be the curve $C_a \oplus C_b$. There is a number s such that $|C_x \cap D| = s$ for all but finitely many points $x \in C$. We claim that $|C_d \cap D| < s$. Clearly C_d and D have the same slope at (0,0). Thus the origin is a multiple point of intersection. If we make a small translation along the curve, the point of intersection at the origin will become two or more simple points of intersection. Moreover, no new multiple points of intersection will form. Thus the number of points of intersection goes up. Since this translation was generic, we must have originally had fewer that the generic number of point of intersection.

Similarly if $m(a)m(b) = m(e)$, then e is algebraic over a and b. Thus there are formulas $A(x,y,z)$ and $M(x,y,z)$ such that if a and b are independent generic points on C, then $\{z : A(a,b,z)\}$ and $\{z : M(a,b,z)\}$ are finite, if $m(a) + m(b) = m(d)$, then $A(a,b,d)$ and if $m(a)m(b) = m(e)$ then $M(a,b,e)$. This is what we call a "fuzzy field". Using Hrushovski's group configuration (see [Bo2]) one sees that in an ω-stable fuzzy field one can interpret a field.

The proof of 6.9 also works if C is a strongly minimal set (in $(\mathbf{C}, +, C)$) which is a finite union of non-linear curves. The next lemma shows that this is the only case we need consider.

Lemma 6.11. If X is a constructible set which is not module definable, then there is a strongly minimal subset of $\mathbf{C}^2$ which is a finite union of non-linear curves.

The proof is an inductive argument using Bertini's theorem. Theorem 6.10 now follows from the next lemma.

Lemma 6.12. If K is an algebraically closed field of characteristic zero and $\mathcal{A} = (K, +, \ldots)$ is a reduct in which there is an infinite iterpretable field F, then $\cdot$ is definable in $\mathcal{A}$.

Proof.

Since $\mathcal{A}$ is strongly minimal, K is contained in the algebraic closure of F. By a theorem of Hrushovski (see for example [Pi3]) or [Po3]) there is a proper definable normal subgroup N of K^+ such that K^+/N is definably (in A) isomorphic to a group G contained in F^n. Since K as characteristic 0, by a result of Poizat (see [Po3]) $N = \{0\}$, so $G \cong K^+$. It is known ([Po3]) that any infinite field F interpretable in a pure algebraically closed field K is definably (in K) isomorphic to K. It then follows that F is also a pure algebraically closed field. In out case this implies that the group G is definable in F.

Since G is definable in F, by theorem 5.6, G is definably isomorphic to an algebraic group over F. It is easy to see that G is one dimensional and connected. It is well known (see [Sp]) that any such group is either an elliptic curve or isomorphic to the additive or multiplicative group of the field. Since G is torsion free it must be isomorphic to the additve group of the F. In particular in $\mathcal{A}$, there is a definable isomorphism between K^+ and F^+. We identify F^+ and K^+ and define $\otimes$ a multiplication on K, induced by the multiplication on F.

Let $B = \{a \in K : \forall x, y\ (x \otimes (ay) = a(x \otimes y)\}$. We claim that $B = K$. Clearly all the natural numbers are in B. Thus B must be cofinite. Since any element of K can be written as the sum of two elements of B, it is easy to see that $B = K$. Let σ be the map $x \mapsto 1 \oplus x$. It is easy to see that σ is definable in $\mathcal{A}$ and

$$xy = z \Leftrightarrow \sigma^{-1}(x) \oplus \sigma^{-1}(y) = \sigma^{-1}(z).$$

So multiplication is definable in $\mathcal{A}$.

One could also ask about analogous problems for $\mathbf{R}$. Some of the most important recent work in model theory has been the study of o-minimal expansions of $\mathbf{R}$. The most exciting breakthrough was Wilkie's proof that the theory of $(\mathbf{R}, +, \cdot, e^x)$ is model complete and o-minimal. We refer the reader to [W], [MMD] and [DD] for more information on this subject.

The problem of additive reducts was solved in the series of papers [PSS], [Pe] and [MPP].

Theorem 6.13 i) (Pillay-Scowcroft-Steinhorn) If $B \subset \mathbf{R}^n$ is bounded then multiplication is not definable in the structure $(\mathbf{R}, +, <, B, \lambda_a : a \in \mathbf{R})$.

ii) (Peterzil) If $X \subset \mathbf{R}^n$ is semialgebraic but not definable in $(\mathbf{R}, +, <, \cdot|[0,1]^2, \lambda_a : a \in \mathbf{R})$,then multiplication is definable in $(\mathbf{R}, +, <, X)$.

iii) (Marker-Peterzil-Pillay) If $X \subset \mathbf{R}^n$ is semialgebraic but not definable in $(\mathbf{R}, +, <, \lambda_a : a \in \mathbf{R})$, then $\cdot|[0,1]$ is definable in $(\mathbf{R}, +, <, X)$.

Recently Peterzil and Starchenko ([PeS]) have proved the o-minimal analog of Zilber's conjectue.

Let M be an o-minimal structure. We say that M is *nontrivial* at a if there is an open interval I containing a and a definable continuous $F : I \times I \to M$ such that for all $b \in I \times I$ the functions $x \mapsto F(b, x)$ and $x \mapsto F(x, b)$ are strictly monotone. Otherwise we say that M is *trivial* at a.

Theroem 6.14. (Perterzil-Starchenko) Let M be an $\aleph_1$-saturated o-minimal structure. If $a \in M$, then exactly one of the following hold:

i) M is trivial at a,

ii) the sturucture that M induces on a neighborhood of a is a reduct of an ordered vector space, or

iii) the structure that M induces on a neighborhood of a is an o-minimal expansion of a real closed field.

References

[A] J. Ax, The elementary theory of finite fields, Ann. Math. 88 (1968).

[B-1] J. Baldwin, *Fundamentals of Stability Theory*, Springer Verlag (1988).

[B-2] J. Baldwin and N Shi, Stable generic structure, Ann. Pure and Applied Logic (to appear).

[B-S] J. Baldwin and J. Saxl, Logical stability in group theory, J. Australian Math. Soc., 21, (1976).

[B-C-R] J. Bochnak, M. Coste, and M. F. Roy, *Geometrie Algebrique Reelle*, Springer Verlag (1986).

[B] A. Borel, Injective endomorphisms of algebraic varieties, Arch. Math. 20 (1969).

[BN] A. Borovik and A. Nesin, *Groups of Finite Morley Rank*, Oxford University Press (1994).

[Bo-1] E. Bouscaren, Model theoretic versions of Weil's theorem for pre-groups, in [N-P].

[Bo-2] E. Bouscaren, The group Configuration–after E. Hrushovski, in [N-P].

[C-K] C.C. Chang and H.J. Keisler, *Model Theory*, North Holland (1977).

[C] G. Cherlin,*Model Theoretic Algebra*, Springer Verlag, SLN 521, (1976).

[Di] M. Dickman, Applications of model theory to real algebraic geometry, in Methods in Mathematical Logic, Springer Verlag, SLN 1130, (1985).

[D-D] J. Denef and L. van den Dries, p-adic and real subanalytic sets, Ann. Math. 128 (1988).

[D-1] L. van den Dries, Remarks on Tarski's problem concerning (R,+,[lozenge],exp), in *Proc. Peano Conference 1982*, North Holland (1984).

[D-2] L. van den Dries, Alfred Tarski's elimination theory for real closed fields, JSL 53, (1988).

[D-3] L. van den Dries, Algebraic theories with definable Skolem functions, JSL 49 (1984).

[D-4] L. van den Dries, Weil's group chunk theorem: a toplogical setting Illinois J. of Math. 34 (1990).

[D-Mac-M] L. van den Dries, A. Macintyre, and D.Marker, The elementary theory of restricted analytic fields with exponentiation, Annals of Math. 140 (1994), 183-205.

[D-M-M] L. van den Dries, D. Marker and G. Martin, Definable equivalence relations on algebraically closed fields, JSL 54 (1989).

[F] W. Fulton, *Algebraic Curves*, Benjamin Cummings, (1974).

[H] R. Hartshorne, *Algebraic Geometry*, Springer Verlag (1977).

[Hr-1] E. Hrushovski, Contributions to Stable Model Theory, Ph.D. dissertation, University of California, Berkeley (1986).

[Hr-2] E. Hrushovski,A new strongly minimal set, Ann. Pure and Applied Logic 62 (1993).

[Hr-3] E. Hrushovski, Strongly minimal expansions of algebraically closed fields, Israel J. Math 79 (1992).

[K-P-S] J. Knight, A. Pillay and C. Steinhorn, Definable sets in ordered structures II, Trans. Amer. Math. Soc. 295 (1986).

[L-1] S. Lang, *Algebra*, Addison-Wesley (1971).

[L-2] S. Lang, *Introduction to Algebraic Geometry*, Interscience, (1958).

[L-3] S. Lang, *Complex Analysis*, Addison-Wesley (1977).

[Mac] A. Macintyre, On ω_1-categorical theories of fields, Fund. Math. 71 (1971).

[M-M-D] A. Macintyre, K. McKenna and L. van den Dries, Quantifier elimination in algebraic structures, Adv. in Math. 47 (1983).

[M1] D. Marker, Semi-algebraic expansions of C, Trans. Amer. Math. Soc. 320 (1990).

[M2] D. Marker, Model theory of differential fields, this volume.

[M-P-P] D.Marker, Y. Peterzil and A. Pillay, Additive reducts of real closed fields, JSL 57 (1992).

[M-P] D. Marker and A. Pillay, Reducts of (C,+,.) which contain +, JSL 55 (1990).

[Ma] G. Martin, Definability in reducxts of algebraically closed fields, JSL 53 (1988).

[Mi] J. Milnor, *Singular points of Complex Hypersurfaces*, Princeton University Press (1968).

[Mu] D. Mumford,*Abelian Varieties*, Oxford University Press (1970).

[N-P] A. Nesin and A. Pillay, *The Model Theory of Groups*, Notre Dame Press (1989).

[Pe] Y. Peterzil, Ph.D. thesis, University of California Berkeley, 1991.

[Pe-S] Y. Peterzil and S. Starchenko, A trichotemy theorem for o-minimal structures (in preparation).

[Pi-1] A. Pillay, Introduction to Stability Theory, Clarendon Press (1983).

[Pi-2] A. Pillay, Groups and fields definable in O-minimal structures, J. Pure and Applied Algebra 53 (1988).

[Pi-3] A. Pillay, On the existence of [delta]-definable normal subgroups of a stable group in [N-P].

[Pi-4] A. Pillay, Model theory of algebraically closed fields, *Stability theory and algebraic geometry, an introduction* (proceedings of Manchester workshop) E. Bouscaren and D. Lascar ed., preprint.

[P-S] A. Pillay and C. Steinhorn, Definable sets in ordered structures I, Trans. Amer. Math. Soc. 295 (1986).

[P-S-S] A. Pillay, C. Steinhorn and P. Scowcroft, Between groups and rings, Rocky Mountain J. 19 (1989).

[Po-1] B. Poizat, Une theorie de Galois imaginaire, JSL 48 (1983).

[Po-2] B. Poizat, An introduction to algebraically closed fields and varieties, in [N-P].

[Po-3] B. Poizat, *Groupes Stables*, Nur Al-Mantiq wal-Ma'rifah, (1987).

[R] E. Rabinovich, *Interpreting a field in a sufficiently rich incidence system*, QMW Press (1993).

[Sp] T.A. Springer, *Linear Algebraic Groups*, Birkhauser (1980).

[W] A. J. Wilkie, Some model completeness results for expansions of the ordered field of reals by Pfaffian functions and exponentiation, Journal AMS (to appear).

[Z-R] B. Zilber and E.F. Rabinovich, Additive reducts of algebraically closed fields, (1988) manuscript (in Russian).