Strongly Minimal Sets and Geometry

David Marker*
University of Illinois, Chicago

These lectures will provide a brief introduction to the model theory of strongly minimal sets. The first two sections will develop the basic combinatorial geometry of strongly minimal sets. In sections three and four we will show how the pregeometry of the strongly minimal set detects the presence of ambient algebraic structure. Finally we will show how these ideas come together in Hrushovski's proof ([H1]) of the Mordell-Lang conjecture for function fields.

Strongly minimal sets are just the beginning of the story in *geometric model theory*. My hope is that by concentrating on strongly minimal sets I can give a reasonably self-contained introduction to this important and beautiful subject. We assume only that the reader is familiar with the treatment of ω-stable theories given in [CK] or [S]. A full development of geometric model is given in [P1].

My own appreciation of geometric model theory was slow in coming. I owe a great deal to Anand Pillay, Elisabeth Bouscaren and John Baldwin for the numerous conversations it took to enlighten me.

§1 Strongly minimal sets and pregeometries

Let $\mathcal{L}$ be a first order language and let M be an $\mathcal{L}$-structure. Recall that a formula $\phi(\bar{v})$ with parameters from M is said to be *strongly minimal* if for any elementary extension N of M and any formula $\psi(\bar{v})$ with parameters from N exactly one of $\{\bar{a} \in N : N \models \phi(\bar{a}) \wedge \psi(\bar{a})\}$ and $\{\bar{a} \in N : N \models \phi(\bar{a}) \wedge \neg\psi(\bar{a})\}$ is infinite. We say that a subset D of M^n is strongly minimal if it is defined by a strongly minimal formula. We will often consider D as a structure in its own right by taking all of the structure induced from definable subsets in M^n.

If $A \subset M$ and $b \in M$ we say that b is *algebraic* over A if there is an $\mathcal{L}$-formula $\phi(v)$ with parameters from A such that $M \models \phi(b)$ and $\{a \in M : M \models \phi(a)\}$ is finite. The set of all elements of A algebraic over A is called the *algebraic closure* of A and denoted $\mathrm{acl}(A)$. The algebraic closure relation on a strongly minimal set determines a pregeometry.

* Partially supported by NSF grant DMS-9306159 and an American Mathematics Society Centennial Fellowship.

Definition. Let X be a set and let $\mathrm{cl} : \mathcal{P}(X) \to \mathcal{P}(X)$ be an operator on the power set of X. We say that (X, cl) is a *pregeometry* if the following conditions are satisfied.

i) (monotonicity) If $A \subseteq X$, then $A \subseteq \mathrm{cl}(A)$.

ii) (transitivity) If $A \subseteq X$, then $\mathrm{cl}(\mathrm{cl}(A)) = \mathrm{cl}(A)$.

iii) (exchange) If $A \subseteq X$, $a, b \in X$ and $a \in \mathrm{cl}(A \cup \{b\})$, then $a \in \mathrm{cl}(A)$ or $b \in \mathrm{cl}(A \cup \{a\})$.

iv) (finite nature of closure) If $A \subseteq X$ and $a \in \mathrm{cl}(A)$, then there is a finite $A_0 \subseteq A$ such that $a \in \mathrm{cl}(A_0)$.

In any structure M conditions i), ii) and iii) are true of algebraic closure. If D is a strongly minimal subset of M^n we consider the operator $X \mapsto \mathrm{acl}(X) \cap D$. We abuse notation by also calling this operator acl. The important observation of Baldwin and Lachlan [BL] is that exchange holds in any strongly minimal set.

Lemma 1.1. If D be a strongly minimal set, then (D, acl) is a pregeometry.

Proof.

We need only verify that exchange holds. Suppose $a, b \in D$, $A \subseteq D$, $a \in \mathrm{acl}(A, b)$. For notational simplicity we assume that $A = \emptyset$.

Suppose $\phi(a, b)$ and $|\{x : \phi(x, b)\}| = n$. Let $\psi(w)$ be the formula "$|\{x : \phi(x, w)\}| = n$". If $\psi(w)$ defines a finite set, then $b \in \mathrm{acl}(\emptyset)$ and $a \in \mathrm{acl}(\emptyset)$. Thus we may assume that $\psi(w)$ defines a cofinite subset of D.

If $\{y : \phi(a, y) \wedge \psi(y)\}$ is finite we are done (as $b \in \mathrm{acl}(a)$). Thus we assume that
$|D - \{y : \phi(a, y) \wedge \psi(y)\}| = l$. Let $\chi(x)$ be the formula expressing

$$|D - \{y : \phi(x, y) \wedge \psi(y)\}| = l.$$

If $\chi(x)$ defines a finite set, then $a \in \mathrm{acl}(\emptyset)$ as desired. Thus we assume $\chi(x)$ defines a cofinite set.

Choose $a_1, \ldots, a_{n+1}$ such that $\chi(a_i)$. The set $B_i = \{w \in D : \psi(w) \wedge \phi(a_i, w)\}$ is cofinite for $i = 1, \ldots, n+1$. Choose $\widehat{b} \in \bigcap B_i$. Then $\phi(a_i, \widehat{b})$, for each i. So $|\{x : \phi(x, \widehat{b})\}| \geq n + 1$, contradicting the fact that $\psi(\widehat{b})$.

If (X, cl) is a pregeometry we say that A is *independent* if $a \notin \mathrm{cl}(A \setminus \{a\})$ for all $a \in A$ and B is a *basis* for Y if $B \subseteq Y$ is independent and $Y \subseteq \mathrm{acl}(B)$. In any pregeometry any two bases for Y have the same cardinality which is called the *dimension*. If $A \subseteq X$ we also consider the *localization* $\mathrm{cl}_A(B) = \mathrm{cl}(A \cup B)$ and notions of independence over A and dimension over A. We let $\dim(B)$ and $\dim(B/A)$ denote the dimension of B and dimension of B over A respectively.

We say that a pregeometry (X, cl) is a *geometry* if $\mathrm{cl}(\emptyset) = \emptyset$ and $\mathrm{cl}(\{x\}) = \{x\}$ for any $x \in X$. If (X, cl) is a pregeometry, then there is a natural associated geometry. Let $X_0 = X \setminus \mathrm{cl}(\emptyset)$. Consider the equivalence relation $\sim$ on X given by $a \sim b$ if and only if $\mathrm{cl}(a) = \mathrm{cl}(b)$. By exchange, $\sim$ is an equivalence relation. Let $\widehat{X}$ be $X_0/\sim$. Define $\widehat{\mathrm{cl}}$ on $\widehat{X}$, by $\widehat{\mathrm{cl}}(A) = \{b/\sim : b \in \mathrm{cl}(A)\}$. It is easy to check that $(\widehat{X}, \widehat{\mathrm{cl}})$ is a geometry.

We distinguish some properties of pregeometries that will play an important role.

Definition. Let (X, cl) be a pregeometry.

i) We say that (X, cl) is *trivial* if $\mathrm{cl}(A) = \bigcup_{a \in X} \mathrm{cl}(\{a\})$ for any $A \subseteq X$.

ii) We say that (X, cl) is *modular* if for any finite dimensional closed $A, B \subseteq X$

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

iii) We say that (X, cl) is *locally modular* if (X, cl_a) is modular for some $a \in X$.

We give several examples for strongly minimal sets.

1) Let D be a set with no structure. Then for all $a \in D$, $\mathrm{acl}(a) = \{a\}$ and $\mathrm{acl}(\emptyset) = \emptyset$. Thus (D, acl) is a trivial geometry.

2) Let $D \models Th(\mathbf{Z}, s)$, where $s(x) = x + 1$. Then $\mathrm{acl}(\emptyset) = \emptyset$, $\mathrm{acl}(a) = \{s^n(a) : n \in \mathbf{Z}\}$ and $\mathrm{acl}(A) = \{s^n(a) : a \in A, n \in \mathbf{Z}\}$. Thus (D, acl) is trivial pregeometry that is not a geometry.

3) (projective geometry) Let F be a division ring and let V be an infinite vector space over F. We view V as a structure in the language $\mathcal{L} = \{+, 0, \lambda_a : a \in F\}$ where $\lambda_a(x) = ax$. Then V is a strongly minimal set and for any set $A \subseteq V$ the algebraic closure of A is equal to smallest F-subspace spanned by A. The usual dimension theorem for intersections of linear subspaces shows that this pregeometry is modular. This is not a geometry since $\mathrm{cl}(\emptyset) = \{0\}$ and for any $a \in V \setminus \{0\}$, $\mathrm{cl}(a)$ is the line through a and 0. To form the associated geometry we take as points the lines through 0. The closure of a set of lines is the set of all lines in their linear span. Thus the associated geometry is just the projective space associated to V. If $\dim V = n$, then the projective space has dimension $n - 1$.

4) (affine geometry) Let V and F be as above. We define a second geometry on V where the closure of a set A is the smallest affine space containing it and $\mathrm{cl}(\emptyset) = \emptyset$. (An affine space is a translate of a linear space). Here $\mathrm{cl}(\{a\}) = \{a\}$. So this is a geometry. Let $a, b, c \in V$ be non-colinear. Then $\dim\ (a, b, c, c + b - a) = 3$, while $\dim\ (a, b) = \dim\ (c, c + b - a) = 2$ and $\mathrm{cl}(a, b) \cap \mathrm{cl}(c, c + b - a) = \emptyset$ as these are parallel lines. Thus the geometry is not modular. If we localize at zero, then the pregeometry is exactly example 3) so this is locally modular.

For $F = \mathbf{Q}$ we can view this as the algebraic closure geometry of a strongly minimal set by viewing V as a structure in the language $\{\tau\}$ where $\tau(x, y, z) = x + y - z$. (For arbitrary F, add function symbols for $ax + y - az$ for each $a \in F$.)

5) Let K be an algebraically closed field of infinite transcendence degree. We claim that (K, acl) is not 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 $d \in \mathrm{acl}(k(a, b))$ 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 $\mathrm{acl}(k(a, b))$. 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 $a, b \in k_1$.

Algebraically closed fields are the only known natural examples of non-locally modular strongly minimal sets. Zilber conjectured that every non-locally modular strongly minimal set is essentially an algebraically closed field. This was refuted when Hrushovski ([H2]) showed that there are non-locally modular strongly minimal sets which do not even interpret infinite groups. Hrushovski ([H3]) later showed that there are strongly minimal sets which are proper expansions of an algebraically closed field. For example he showed that there are strongly minimal structures $(D, +, \cdot, \oplus, \otimes)$ where $(D, +, \cdot)$ is algebraically closed field of characteristic $p \geq 0$ and $(D, \oplus, \otimes)$ is an algebraically closed field of characteristic $q \neq p$.

Although Zilber's conjecture is false it provided the motivation for a great deal of important work. One related problem is still open.

Cherlin-Zilber conjecture. Suppose G is a simple group of finite Morley rank. Then G interprets an algebraically closed field F and G is definably isomorphic to an algebraic group over F.

We next give a useful characterization of modularity. Let (X, cl) be a pregeometry.

Lemma 1.2. The following are equivalent.

i) (X, cl) is modular.

ii) If $A \subseteq X$ is closed, $b \in X$ and $x \in \mathrm{cl}(A, b)$, then there is $a \in A$ such that $x \in \mathrm{cl}(a, b)$.

iii) If $A, B \subseteq X$ are closed and $x \in \mathrm{cl}(A, B)$, then there are $a \in A$ and $b \in B$ such that $x \in \mathrm{cl}(a, b)$.

Proof.

i)$\Rightarrow$ ii) By the finite nature of closure we may assume that dim A is finite. If $x \in \text{cl}(b)$ we are done, so we may assume $x \notin \text{cl}(b)$. By modularity

$$\text{dim } (A, b, x) = \text{dim } A + \text{dim } (b, x) - \text{dim } (A \cap \text{cl}(b, x))$$

and

$$\text{dim } (A, b, x) = \text{dim } (A, b) = \text{dim } A + \text{dim } b - \text{dim } (A \cap \text{cl}(b)).$$

Since dim $(b, x) =$ dim $(b) + 1$, there is $a \in A$ such that $a \in \text{cl}(b, x) \setminus \text{cl}(b)$. By exchange, $x \in \text{cl}(b, x)$.

ii)$\Rightarrow$ iii) We may suppose A and B are finite dimensional. We proceed by induction on dim A. If dim A is zero then iii) holds. Suppose that $A = \text{cl}(A_0, a)$ where
dim $A_0 =$ dim $A - 1$. Then $x \in \text{cl}(A_0, B, a)$. By ii) there is $c \in \text{cl}(A_0, B)$ such that $x \in \text{cl}(c, a)$. By induction there is $a_0 \in A_0$ and $b \in B$ such that $c \in \text{cl}(a_0, b)$. Again by ii), there is $a^* \in \text{cl}(a_0, a) \subseteq A$, such that $x \in \text{cl}(a^*, b)$.

iii)$\Rightarrow$ i) Suppose $A, B \subset X$ are finite dimensional and closed. We prove i) by induction on dim A. If dim $A = 0$, then we are done. Suppose $A = \text{cl}(A_0, a)$ where dim $A_0 =$ dim $A - 1$, and we assume, by induction, that

$$\text{dim } (A_0, B) = \text{dim } A_0 + \text{dim } B - \text{dim } (A_0 \cap B).$$

First, assume that $a \in \text{cl}(A_0, B)$. Then dim $(A_0, B) =$ dim (A, B) and, since $a \notin A_0$, dim $A =$ dim $A_0 + 1$. Since $a \in \text{cl}(A_0, B)$, by iii) there is $a_0 \in A$ and $b \in B$ such that $a \in \text{cl}(a_0, b)$. Since $a \notin \text{cl}(a_0)$, by exchange, $b \in \text{cl}(a, a_0)$. Thus $b \in A$. But $b \notin A_0$, since otherwise $a \in A_0$. Therefore dim $(A \cap B) =$ dim $(A_0 \cap B) + 1$ as desired.

Next, suppose that $a \notin \text{cl}(A_0, B)$. In this case we need to show that $A \cap B = A_0 \cap B$. Suppose $b \in B$ and $b \in \text{cl}(A_0, a) \setminus \text{cl}(A_0)$. Then by exchange, $a \in \text{cl}(A_0, b)$, a contradiction.

Remark: If V is a vector space, then it is easy to see that if $a_1, \ldots, a_n$ is a basis for A and $b_1, \ldots, b_m$ is a basis for B. Then any x in the span of $A \cup B$ is the sum of a linear combination of the a_i and a linear combination of the b_j. Thus condition iii) above holds.

Exercise: If K is an algebraically closed field, $x, a_0, \ldots, a_n$ are algebraically independent and

$$y = \sum_{i=0}^{n} a_i x^i$$

then y is not algebraic over $k(x)$ for k a subfield of $\text{acl}(a_0, \ldots, a_n)$ of dimension less than $n + 1$.

We conclude this section by illustrating the close connection between Morley rank and dimension for strongly minimal sets.

Let D be a strongly minimal set and let $A \subseteq D$. There are two kinds of types in $S_1(A)$. We say that $p \in S_1(A)$ is an *algebraic* type if there is a formula $\phi(v, \bar{w})$ and $\bar{a} \in A$ such that $\phi(v, \bar{a})$ defines a finite set and $\phi(v, \bar{a}) \in p$. There will be a minimal n such that p contains a formula $\phi(v, \bar{b})$ which defines a set of size n. It is easy to see that this formula isolates p.

Let $p_1 = \{\neg\phi(v, \bar{a}) : \bar{a} \in A$, and $\phi(v, \bar{a})$ defines a finite set$\}$. By strong minimality p_1 is complete and consistent. Clearly p_1 is the unique non-algebraic one type. Clearly $\mathrm{RM}(p_1) = 1$, while $\mathrm{RM}(p) = 0$ if p is algebraic.

We inductively define the type of n-independent elements $p_n \in S_n(A)$ as follows:

$\phi(v_1, \ldots, v_{n-1}, \bar{a})$ is in p_{n+1} if and only if the formula

$$|\{w : \neg\phi(v_1, \ldots, v_{n-1}, w, \bar{a})\}| \leq m$$

is in p_{n-1} for some m. Since p_{n-1} is a complete type, strong minimality implies that either "$|\{w : \phi(v_1, \ldots, v_{n-1}, w, \bar{a}\}| \leq m$" or "$|\{w : \neg\phi(v_1, \ldots, v_{n-1}, w, \bar{a}\}| \leq m$" is in p_{n-1} for some m.

Let $q \in S_n(A)$. We let dim q be the maximum m such that there are $i_1, \ldots, i_m$ such that q restricted to $v_{i_1}, \ldots, v_{i_m}$ is p_m. We reorder the variables so that $i_j = j$. If $\bar{b}$ is a realization of q then $b_1, \ldots, b_m$ are independent over A and $b_{m+1}, \ldots, b_n \in \mathrm{acl}(A, b_1, \ldots, b_m)$.

We argue by induction that $\mathrm{RM}(p_n) = n$. If $q \in S_n(A)$, dim $q = m < n$ and $\bar{b}$ realizes q, then we can (by reordering the variables) assume that $b_1, \ldots, b_m$ are independent over A and $b_{m+1}, \ldots, b_n \in \mathrm{acl}(A, b_1, \ldots, b_m)$. But then $\mathrm{RM}(\bar{b}/A) = \mathrm{RM}(b_1, \ldots, b_m/A) = \mathrm{RM}(p_m) = m < n$.

It is easy to easy to see that $\mathrm{RM}(E^n) \geq \mathrm{RM}(E)n$ for any definable set E. Thus $\mathrm{RM}(D^n) \geq n$. If $q \neq p_n$, then $\mathrm{RM}(q) < n$. Since there must be some type of rank at least n, that type must be p_n. Since p is isolated once we discard types of rank less than n, $\mathrm{RM}(p_n) = n$. Thus $\mathrm{RM}(D^n) = n$.

Thus for any $p \in S_n(A)$, $\mathrm{RM}(p) = \dim p$. Also $\mathrm{RM}(\bar{a}/A) = \dim(\bar{a}/A)$. From this, and the fact that the corresponding equation is clearly true for dimension, we see that in strongly minimal sets we have the following version of the Lascar equality

$$\mathrm{RM}(\bar{a}, \bar{b}/A) = \mathrm{RM}(\bar{a}/A) + \mathrm{RM}(\bar{b}/A, \bar{a}).$$

The equivalence of Morley rank and dimension will allow us to conclude that in strongly minimal sets Morley rank is definable.

Lemma 1.3. Let D be strongly minimal. Suppose $C \subseteq D^{m+n}$ is definable. Let $C_a = \{x \in D^n : (a, x) \in C\}$ for $a \in D^m$. The set $Y_{n,k} = \{a \in D^m : \mathrm{RM}\ C_a \geq k\}$ is definable for each $k \leq n$.

Proof.

We prove this by induction on n.

Suppose $n = 1$. We first note that there is a number N such that $|C_a| < N$ or $|D \setminus C_a| < N$, for all $a \in D^m$; since otherwise the type

$$\Gamma(\bar{w}) = \{\exists v_1, \ldots, v_{2s} \bigwedge_{i \neq j} v_i \neq v_j \wedge \bigwedge_{i=1}^{s} \phi(\bar{w}, v_i) \wedge \bigwedge_{i=s+1}^{2s} \neg\phi(\bar{w}, v_i) : s = 1, 2, \ldots\}$$

is consistent and a realization violates strong minimality.

Thus $\mathrm{RM}(C_a) \geq 1$ if and only if $|C_a| > N$. So $Y_{1,1}$ is definable. Clearly $Y_{1,0} = D^m$.

Suppose $n = s + 1$. We work by induction on k. Clearly $Y_{n,0}$ is definable. For $a \in D^m$, let $B_a = \{\bar{b} \in D^s : \exists y\ (\bar{b}, y) \in C_a\}$. Clearly if $\mathrm{RM}(B_a) \geq k$, then $\mathrm{RM}(C_a) \geq k$. Suppose $\mathrm{RM}(B_a) < k$. If $\bar{b} \in B_a$ and $(b, c) \in C_a$, then $\dim\ (b, c) = \dim\ b + \dim\ (c/b)$. Let $A_a = \{\bar{b} \in D^s : \{y : (b, y) \in C_a\}$ is infinite$\}$. As above, there is an N (independent of a) such that

$$\bar{b} \in A_a \leftrightarrow |\{y : (b, y) \in C_a\}| > N.$$

Thus A_a is definable and $\mathrm{RM}(C_a) \geq k$ if and only if $\mathrm{RM}(A_a) \geq k - 1$.

Thus $\mathrm{RM}(C_a) \geq k$ if and only if $\mathrm{RM}(B_a) \geq k$ or $\mathrm{RM}(A_a) > k - 1$. So, by induction, $Y_{n,k}$ is definable.

Finally we make one very useful definition.

Definition. Let $v = v_1, \ldots, v_n$, $b = b_1, \ldots, b_m$ and suppose $\phi(v, b)$ has Morley rank k and Morley degree 1. If $b \in B$ and $p \in S_n(B)$ is the unique type of rank k containing $\phi(v, b)$, then we call p the *generic* type for $\phi(v, b)$ over B.

§2 Families of plane curves

Let D be a strongly minimal set. In this section we will consider families of strongly minimal subsets of D^2. We first consider two illustrative examples. Suppose V is a $\mathbf{Q}$ vector space. Let $E = \{(x, y, z) \in V^3 : y = mx + z\}$ where $m \in \mathbf{Q}$. For $a \in V$, let $E_a = \{(x, y) : (x, y, a) \in E$. We think of E as describing the *family of plane curves* $\{E_a : a \in V\}$. We call V the *parameter space* for the family E. Note that in this case the parameter space is rank one. Indeed, if E is a family of plane curves in V^2 of higher rank, then for many distinct a and b E_a and E_b agree except perhaps on a finite set.

On the other hand suppose K is an algebraically closed field. Fix $n \in N$ and consider

$$E = \{(x, y, z_0, \ldots, z_{n-1}) : y = x^n + z_{n-1}x^{n-1} + \ldots + z_1 x + z_0\}.$$

If

$$E_a = \{(x, y) : y = x^n + \sum_{i=0}^{n-1} a_i x^i\}$$

for $a = (a_0, \ldots, a_{n-1}) \in K^n$, then $\{E_a : a \in K^n\}$ is an n-dimensional family of strongly minimal sets.

In this section we will examine families of plane curves and use them to give an alternative characterization of local modularity. To make these notions precise we must first digress and discuss M^{eq} and canonical bases.

Let M be any $\mathcal{L}$-structure. We associate to M a new structure M^{eq} in many sorted language $\mathcal{L}^{\mathrm{eq}} \supseteq \mathcal{L}$. For each $\emptyset$-definable equivalence relation E on M^n, we add a new sort S_E and a new n-ary function symbol f_E. We interpret S_E as M^n/E and f_E as the quotient map

$$x \mapsto x/E.$$

We can think of M as being the sort $S_=$. Clearly if $M \prec N$, then $M^{\mathrm{eq}} \prec N^{\mathrm{eq}}$. Moreover if $\mathcal{A}$ is an $\mathcal{L}^{\mathrm{eq}}$-structure elementarily equivalent to M^{eq}, then $\mathcal{A}$ is N^{eq} for some $N \equiv M$. Also note that if $\sigma \in Aut(M)$, then there is a unique extension of σ to $\widehat{\sigma} \in Aut(M^{\mathrm{eq}})$. Clearly every automorphism of M^{eq} restricts to an automorphism of M.

One function of M^{eq} is that any structure interpretable in M is isomorphic to a structure definable in M^{eq}. For our purposes the most important property of M^{eq} is the existence of canonical bases.

Definition. Suppose M is saturated. Let $X \subseteq M^n$ be definable. We say that A is a *canonical base* for X if σ fixes X setwise (ie. $X = \{\sigma(x) : x \in X\}$) if and only if σ fixes A pointwise (ie. $\sigma(a) = a$ for $a \in A$) for all $\sigma \in Aut(M)$).

If $p \in S_n(M)$ then A is a canonical base for p if $\sigma(p) = p$ if and only if σ fixes A pointwise for all $\sigma \in Aut(M)$.

Note that if A is a canonical base for X and $\mathrm{dcl}^{\mathrm{eq}}(A) = \mathrm{dcl}^{\mathrm{eq}}(B)$, then B is also a canonical base for X.

Suppose X is defined by the formula $\phi(\bar{x}, \bar{a})$. Let E be the equivalence relation

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

Let $\alpha = \bar{a}/E \in M^{\mathrm{eq}}$. Then α is a canonical base for X.

We next show that if D is strongly minimal, $A \subseteq D$ and $p \in S_n(A)$. Then p has a canonical base $\alpha \in M^{\mathrm{eq}}$.

Suppose p has rank r and Morley degree 1. There is a formula $\phi(v, b) \in p$ such that ϕ has Morley rank r and Morley degree one. By definability of rank there is a formula $\Psi(w)$ such that $\Psi(b)$ and

$$\Psi(w) \Leftrightarrow \mathrm{RM}(\{x : \phi(x, w)\}) = k.$$

Let $\theta(w)$ be the formula

$$\Psi(w) \wedge \forall z\ \neg\big[\Psi(z) \wedge \mathrm{RM}(\{x : \phi(x, b) \wedge \phi(x, z)\}) = k\ \wedge$$
$$\mathrm{RM}(\{x : \phi(x, b) \wedge \neg\phi(x, z)\}) = k\big].$$

Clearly $\theta(b)$ holds.

We can define an equivalence relation on $Y = \{y \in D^m : \theta(y)\}$ by

$$y \sim z \Leftrightarrow \mathrm{RM}\{x : \phi(x, y) \wedge \phi(x, z)\}) = k.$$

Let α be the equivalence class $b/\sim$.

Then $\sigma(\alpha) = \alpha$ iff $\sigma(b) \sim b$. But $\sigma(p) = p$ iff $\sigma(p)$ is the generic of $\phi(v, b)$. Since $\sigma(p)$ is the generic of $\phi(v, \sigma(b))$, $\sigma(p) = p$ if and only if $\sigma(b) \sim b$. Thus α is a canonical base for p. Clearly $\alpha \in \mathrm{dcl}^{\mathrm{eq}}(b)$.

If p has rank r and Morley degree $k > 1$ and $\phi(v, b)$ is a rank r degree k formula in p, then a similar argument shows that $\alpha \in \mathrm{acl}^{\mathrm{eq}}(b)$.

We summarize these arguments in the following theorem.

Theorem 2.1. Suppose $A \subseteq D$ and $p \in S_n(A)$, then there is a canonical base for p is in $\mathrm{acl}^{\mathrm{eq}}(A)$. If p has Morley degree 1, then the canonical base for p is in $\mathrm{dcl}^{\mathrm{eq}}(A)$.

We next need to consider the computation of ranks in D^{eq}. The key is the following unpublished lemma of Lascar and Pillay.

Lemma 2.2. Let D be a strongly minimal set and let $D_0 \subseteq D$ be infinite. Suppose E is an $\emptyset$-definable equivalence relation on D^m. Let $a \in D^m$ and $\alpha = a/E$. There is a finite $C \subset D$ such that an automorphism of D fixing D_0 fixes α if and only if it fixes the C setwise.

Proof.

By adding D_0 to our language we assume that $\mathrm{acl}(\emptyset)$ is infinite.

Our first claim is that there is $b = (b_1, \dots b_m) \in D^m$ algebraic over α such $a\ E\ b$. Choose b such that $b\ E\ a$, 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 $b_1, \dots, b_j$ are algebraic over α and b_i is not algebraic over α for $i > j$. Let

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

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

Let C be the set of all conjugates of $\bar{b}$ under automorphisms fixing α. Then C is fixed setwise by any automorphism which fixes α and D_0. 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.

Lemma 2.2 gives an easy description of Morley rank in D^{eq}. If p is a $\mathcal{L}_{\mathrm{eq}}$-type over D. Let a realize p. By lemma 2.2 there is a finite set C such that the set C is interalgebraic with a over D. Then $\mathrm{RM}(p)$ is equal to the dimension of C.

Definition. We say that a strongly minimal set D is *linear* if for all $p \in S_2(D)$, the canonical base for p has rank at most one.

Suppose $\phi(v_1, v_2, b)$ is strongly minimal. Let $\mathcal{F}$ be the family of sets C_β where β and b realize the same type. There is a natural equivalence relation on $\mathcal{F}$, $C_\alpha \sim C_\beta$ if and only if $C_\alpha \delta C_\beta$ is finite. If p is the generic type of ϕ, then the Morley rank of the canonical base of p intuitively corresponds to the dimension of $\mathcal{F}/\sim$. Thus D is linear if and only if there is no family of plane curves of dimension greater than one. Algebraically closed fields are nonlinear since we have the family of curves $C_{(a,b)} = \{(x,y) : y = ax + b\}$, while vector spaces are linear.

We next show that the linear strongly minimal sets are exactly the locally modular ones.

Theorem 2.3. Let D be a strongly minimal set. The following are equivalent.

i) For some small $B \subset D$, the pregeometry D_B is modular.

ii) D is linear.

iii) D is locally modular (ie. there is $b \in D$ such that D_b is modular).

Proof.

i)$\Rightarrow$ ii) Adding the parameters B to the language we assume that $B = \emptyset$ and D is modular. Let $p \in S_2(A)$ be strongly minimal. Let $\phi(v_1, v_2, \bar{a})$ be a strongly minimal formula in p. Let b_1, b_2 realize p. Let $X = \mathrm{acl}(\bar{a}) \cap \mathrm{acl}(b_1, b_2)$. By modularity

$$\dim X = \dim\ (a) + \dim\ (b_1, b_2) - \dim\ (a, b_1, b_2).$$

Since $\dim\ (a, b_1, b_2) = \dim\ (a) + 1$ and $1 \leq \dim\ (b_1, b_2) \leq 2$, $\dim X \leq 1$.

By modularity

$$\begin{aligned}\dim\ (b_1, b_2)/\bar{a}) &= \dim\ (b_1, b_2, a) - \dim\ (\bar{a})\\ &= \dim\ (b_1, b_2) - \dim X\\ &= \dim\ (b_1, b_2/X).\end{aligned}$$

Thus $\dim\ (b_1, b_2/X) = 1$. Let c be a canonical base for p, then, by 2.1, $c \in \mathrm{acl}^{\mathrm{eq}}(X)$, so $\mathrm{RM}(c) \leq 1$.

ii)$\Rightarrow$ iii) Let $b \in D - \mathrm{acl}(\emptyset)$. We will show that D localized at b is modular. We will use the fact that 1.2ii) is equivalent to modular. Suppose B is a finite dimensional closed set. Suppose $a_1 \in \mathrm{acl}(a_2, B, b)$. We must find $d \in \mathrm{acl}(B, b)$ such that $a_1 \in \mathrm{acl}(a_2, d, b)$. Clearly we may assume that $a_1 \notin \mathrm{acl}(B, b)$, $a_2 \notin \mathrm{acl}(B, b)$ and $a_1 \notin \mathrm{acl}(a_2, b)$ (else we are done). Thus $\dim\ (a_1, a_2/b) = 2$ and $\dim\ (a_1, a_2/Bb) = 1$.

Let c be a canonical base for the type of a_1, a_2 over $\mathrm{acl}^{\mathrm{eq}}(B, b)$. By 2.1 $c \in \mathrm{acl}^{\mathrm{eq}}(B, b)$.

claim: $c \in \mathrm{acl}^{\mathrm{eq}}(a_1, a_2)$

Since c is the canonical base for p, $\mathrm{RM}(a_1, a_2/c) = 1$. Since $\mathrm{RM}(a_1, a_2/c) < \mathrm{RM}(a_1, a_2)$, $\mathrm{RM}(c/a_1, a_2) < \mathrm{RM}(c)$. By ii) $\mathrm{RM}(c) = 1$, thus $c \in \mathrm{acl}^{\mathrm{eq}}(a_1, a_2)$.

Since $\mathrm{RM}(a_1, a_2/b) = 2$ and $\mathrm{RM}(a_1, a_2/c) = 1$, $c \notin \mathrm{acl}(b)$. Thus, since $b \notin \mathrm{acl}(\emptyset)$, $b \notin \mathrm{acl}(c)$. Thus a_1 and b realize the same type over c and, by saturation, there is $d \in D$ such that $tp(a_1, a_2/c) = tp(b, d/c)$. Then

$$d \in \mathrm{acl}(b, c) \subseteq \Big(\mathrm{acl}(a_1, a_2, b) \cap \mathrm{acl}(Bb)\Big)$$

and $d \notin \mathrm{acl}(b)$.

We claim that $d \notin \mathrm{acl}(a_2, b)$. If $d \in \mathrm{acl}(a_2, b)$, then, since $d \notin \mathrm{acl}(b)$, $a_2 \in \mathrm{acl}(d, b) \subseteq \mathrm{acl}(B, b)$, a contradiction.

Thus since $d \in \mathrm{acl}(a_1, a_2, b) \setminus \mathrm{acl}(a_2, b)$, $a_1 \in \mathrm{acl}(a_2, b, d)$ as desired.

We next give an "incidence geometry" interpretation of local modularity. This material will not be used in the subsequent sections.

Definition. Suppose P and L are sets and $I \subseteq P \times L$. We think of P as a set of *points*, L as a set of *lines*, and I as the incidence relation (ie. $I(p,l)$ if and only if p is on l). We say that (P,L,I) is a *quasi-design* if

i) for any p, $\{l : I(p,l)\}$ is infinite

ii) for any l, $\{p : l(p,l)\}$ is infinite, and

iii) for any $l_1 \neq l_2$, $\{p : I(p,l_1)$ and $I(p,l_2)\}$ is finite.

If in addition

iv) for any $p_1 \neq p_2$, $\{l : I(p_1,l)$ and $I(p_2,l)\}$ is finite

then we call (P,L,I) a *pseudo-plane*.

We say that (P,L,I) is *complete-type definable* if there is a complete type $r(x,y)$ such that $P = \{x : \exists y\ r(x,y)\}$, $L = \{y : \exists x\ r(x,y)\}$ and I is the set of realizations of r.

Lemma 2.4. Let M be any saturated structure. If there is a complete type definable quasi-design in M^{eq}, then there is a complete type definable pseudo-plane.

Proof.

Let $c \in L$ and let $B = \{b_1, b_2, \ldots\} \subset P$, such that $r(b_i, c)$ for all i. Let σ be any automorphism of M fixing B pointwise. Since L is the set of realizations of a type, $\sigma(c) \in L$ and $r(b_i, \sigma(c))$ for all i. Thus by iii) $c = \sigma(c)$. Hence $\sigma(c) \in \mathrm{dcl}^{\mathrm{eq}}(B)$.

Let n be maximal such that there are distinct $b_1, \ldots, b_n$ such that $r(b_i, c)$ and $c \notin \mathrm{acl}^{\mathrm{eq}}(b_1, \ldots, b_n)$. Let $d \in M^{\mathrm{eq}}$ be the unordered set $\{b_1, \ldots, b_n\}$. Let r^* be the type of (d, c).

Since $b_i \in \mathrm{acl}(d) \backslash \mathrm{acl}(c)$, $d \notin \mathrm{acl}(c)$. Thus i) holds. By choice of n, $c \notin \mathrm{acl}(d)$. If $r^*(d_1, c_1)$ and $r^*(d_1, c_2)$ then $d_1 = \{b_1, \ldots, b_n\}$ where $r(b_i, c_j)$ for $i = 1, \ldots, n$ and $j = 1, 2$. Clearly since $\{b : r(b, c_1) \wedge r(b, c_2)\}$ is finite, $\{d : r^*(d, c_1) \wedge r^*(d, c_2)\}$ is finite. By choice of n if $r(d_1, c), r(d_2, c)$ and $d_1 \neq d_2$, then $c \in \mathrm{acl}(d_1, d_2)$. By saturation, there are only finitely many c such that $r(c, d_1)$ and $r(c, d_2)$. Thus r^* determines a pseudoplane.

Proposition 2.5. Let D be strongly minimal. If D is non-locally modular then there is a complete-type definable pseudoplane.

Proof.

By 2.4 it suffices to show that there is a complete-type definable quasi-design. Suppose D is not locally modular. Then by 2.3 there is a strongly minimal $p \in S_2(D)$ such that if c is the canonical base for p, then $\mathrm{RM}(c)$=2. Let $a = (x, y)$ realize p and let r^* be the type of (a, c). Since $\mathrm{RM}(p) = 1$, $a \notin \mathrm{acl}(c)$. Since $\mathrm{RM}(a, c) = \mathrm{RM}(c) + 1 \geq 3$, $c \notin \mathrm{acl}(a)$. Suppose $c \neq c_1$ and both (a, c) and (a, c_1) realize r. Let $\phi(\bar{v}, \bar{b})$ be a strongly minimal formula in the type with canonical base c and let $\phi(\bar{v}, \bar{b}_1)$ be a formula in the type with canonical base c_1. Since $c_1 \neq c$, $\{\bar{v} : \phi(\bar{v}, \bar{b}) \wedge \phi(\bar{v}, \bar{b}_1)\}$ is finite. Thus $\{x : r(x, c)$ and $r(x, c_1)\}$ is finite.

§3 Algebraic structure

A remarkable insight of Hrushovski's is that in many situations algebraic structure can be detected from the geometry of forking. In this section we will give one version of this result and apply it to show that a locally modular strongly minimal set interprets a group. We will also state a theorem of Hrushovski and Pillay describing groups interpretable in locally modular strongly minimal sets.

Throughout this section D will be a saturated strongly minimal set. Our main tool is the *group configuration*. Suppose we have elements a, b, c, x, y, z in $D^{\rm eq}$ such that:

i) $\mathrm{RM}(a) = \mathrm{RM}(b) = \mathrm{RM}(c) = \mathrm{RM}(x) = \mathrm{RM}(y) = \mathrm{RM}(z) = 1$;

ii) any pair of elements has rank 2;

iii) $\mathrm{RM}(a, b, c) = \mathrm{RM}(a, x, y) = \mathrm{RM}(c, y, z) = \mathrm{RM}(b, x, z) = 2$;

iv) any other triple has rank 3.

Look at Diagram 1. Conditions iii) and iv) assert that each line has rank two while any three non-colinear points have rank two.

There is one easy way that a group configuration arises. Suppose G is a strongly minimal abelian group (indeed strongly minimal groups must be abelian). Let a, b, x be independent elements of G. Let $c = ba$, $y = cx$ and $z = bx$, then $y = az$ and it is easy to check that conditions i)-iv) hold. Remarkably this observation has a converse.

Theorem 3.1 (Hrushovski) (see [Bo1] or [P1] chapter 5) Suppose there is a group configuration in $D^{\rm eq}$. Then D interprets a strongly minimal abelian group.

Let D be a saturated non-trivial locally modular strongly minimal set D. By adding a parameter to our language we assume that D is modular. We will show how to use theorem 3.1 to find a group in $D^{\rm eq}$.

Since D is non-trivial we can find a finite $A \subset D$ and $b, c \in D \setminus \mathrm{acl}(A)$ such that $c \in \mathrm{acl}(A, b) \setminus (\mathrm{acl}(A) \cup \mathrm{acl}(b))$. By modularity

$$\dim\,(b, c, A) = \dim\,(b, c) + \dim\,(A) - \dim\,C$$

where $C = \mathrm{acl}(A) \cap \mathrm{acl}(b, c)$. Since $\dim\,(b, c, A) = \dim\,A + 1$ and $\dim\,(b, c) = 2$, $\dim\,C = 1$. Thus there is $a \in C$ with $\dim\,a = 1$. Note that $\dim\,(a, c) = \dim\,(a, b) = 2$, but $\dim\,(b, c/a) = 1$.

Choose $y, z \in D$ such that (b, c) and (y, z) realize the same type over $\mathrm{acl}^{\rm eq}(a)$ and (y, z) are independent from (b, c) over a (ie. $\dim\,(y, z/a, b, c) = \dim\,(y, z/a) = \dim\,(b, c/a) = 1$). Since $a \in \mathrm{acl}(b, c)$, $z \in \mathrm{acl}(b, c, y)$. Thus $\dim\,(b, c, y) = 3$ and $\dim\,(c, y) = 2$. Similarly $\dim\,(b, z) = 2$. By modularity

$$\dim\,(c, y, b, z) = \dim\,(c, y) + \dim\,(b, z) - \dim\,X$$

where $X = \mathrm{acl}(c, y) \cap \dim\,\mathrm{acl}(b, z)$. Thus $\dim\,X = 1$ and there is $x \in \mathrm{acl}(c, y) \cap \mathrm{acl}(b, z)$ with $\dim\,x = 1$.

It is easy to see that a, b, c, x, y, z is a group configuration. Thus D interprets a rank 1 abelian group.

The next theorem summarizes a much finer version of this result (see [P1] chapter 5)]). It says that not only is there an interpretable group, but the group determines most of the structure of the the strongly minimal set.

Theorem 3.2. (Hrushovski) Let D be a non-trivial locally modular strongly minimal set. Then there is a rank 1 abelian group G definable in D^{eq} such that G acts definably as a group of automorphisms of the generic type of D.

In §5 we will use a structure theorem for groups interpretable in a locally modular strongly minimal set. This result is true in a much more general setting. We say that a stable theory T is *1-based* if for any a and B the canonical base for the strong type of a over B is contained in $\mathrm{acl}^{\mathrm{eq}}(a)$.

Lemma 3.3. If M is interpretable in a locally-modular strongly minimal set then $Th(M)$ is 1-based.

Indeed a finite Morley rank theory T is 1-based if and only if every strongly minimal set is locally modular (see [P1] chapter 2).

Theorem 3.4. (Hrushovski-Pillay) (see [HP] or [P1] chapter 4) Suppose G is a 1-based group. Then every definable subset of G^n is a finite boolean combination of cosets of definable subgroups.

We conclude by stating a generalization of the group configuration which detects the presence of a field. A *field configuration* is a collection of elements $a, b, c, x, y, z \in D^{\mathrm{eq}}$ such that

i) $\mathrm{RM}(a) = \mathrm{RM}(b) = \mathrm{RM}(c) = 2$ and $\mathrm{RM}(x) = \mathrm{RM}(y) = \mathrm{RM}(z) = 1$;

ii) $\mathrm{RM}(a, b) = \mathrm{RM}(a, c) = \mathrm{RM}(b, c) = 4$ and $\mathrm{RM}(a, b, c) \leq 5$;

iii) $\mathrm{RM}(a, x, y) = \mathrm{RM}(b, x, z) = \mathrm{RM}(c, y, z) = 3$;

iv) any three non-colinear points (see diagram 1) are independent;

v) If we replace a, b, c by a^*, b^*, c^* with $\mathrm{RM}(a^*) = \mathrm{RM}(b^*) = \mathrm{RM}(c^*) = 1$ then a^*, b^*, c^*, x, y, z is not a group configuration.

Suppose K is an algebraically closed field and $\alpha_1, \alpha_2, \beta_1, \beta_2, x$ are algebraically independent. Let a, b, c be elements of the rank 2 group of affine transformations where a is the transformation $z \mapsto \alpha_1 z + \alpha_2$ and b is $z \mapsto \beta_1 z + \beta_2$. Let c be the composition. Let $y = cx$ and $z = bx$. Then $az = y$. Note that $\mathrm{RM}(a/z, y) = \mathrm{RM}(b/x, z) = \mathrm{RM}(c/x, y) = 1$. Thus we have a field configuration. Remarkably this is the only way this can happen.

Theorem 3.5 (Hrushovski) (see [Bo1]) If there is a field configuration in D^{eq}, then D interprets an algebraically closed field.

§4 Zariski Geometries

Zariski geometries were introduced by Hrushovski and Zilber in [HZ1], [HZ2] and [Z] . In addition to providing an important class of strongly minimal sets where Zilber's conjecture is true, they answer the metamathematical question: Can one characterize the topological spaces that arise from the Zariski topology on an algebraic curve?

We say that a topological space is *Noetherian* if there are no infinite descending chains of closed sets. If K is a field, then the *Zariski topology* on K^n is given by taking the solutions to systems of polynomial equations as the basic closed sets. Since the polynomial ring $K[X_1, \ldots, X_n]$ has no infinite ascending chains of ideals, the Zariski topology is Noetherian.

A closed set X is *irreducible* if there are no proper closed subsets X_0 and X_1 such that $X = X_0 \cup X_1$. A simple König's lemma argument shows that in any Noetherian topological space, every closed set X is a union of finitely many irreducible closed sets, called the irreducible components of X.

In Noetherian topological spaces we can inductively assign an ordinal dimension to any non-empty irreducible closed set X by $\dim X = \sup\{\dim Y + 1 : Y \subset X$ closed and irreducible$\}$.

Definition. A *Zariski geometry* is an infinite set D and a sequence of Noetherian topologies on $D, D^2, D^3, \ldots$ such that the following axioms hold.

(Z0) [Coherence]: i) If $f : D^n \to D^m$ is defined by $f(x) = (f_1(x), \ldots, f_m(x))$ where each $f_i : D^n \to D$ is either constant or a coordinate projection, then f is continuous.

ii) Each diagonal $\Delta^n_{i,j} = \{x \in D^n : x_i = x_j\}$ is closed.

(Z1) [Weak QE]: If $C \subseteq D^n$ is closed and irreducible, and $\pi : D^n \to D^m$ is a projection, then there is a closed $F \subset \overline{\pi(C)}$ such that $\pi(C) \supseteq \overline{\pi(C)} \setminus F$.

(Z2) [Uniform one-dimensionality]: i) D is irreducible.

ii) Let $C \subseteq D^n \times D$ be closed and irreducible. For $a \in D^n$, let $C(a) = \{x \in D : (a, x) \in C\}$. There is a number N such that for all $a \in D^n$, either $|C(a)| \leq N$ or $C(a) = D$. In particular any proper closed subset of D is finite.

(Z3) [Dimension theorem]: Let $C \subseteq D^n$ be closed and irreducible. Let W be a non-empty irreducible component of $C \cap \Delta^n_{i,j}$. Then $\dim C \leq \dim W + 1$.

The basic example of a Zariski geometry is a smooth algebraic curve C over an algebraically closed field where C^n is equipped with the Zariski topology. In this case Z0 is clear, Z1 follows from quantifier elimination and Z2 follows from the fact that C is strongly minimal. The verification of Z3 uses the smoothness of C (though a weaker condition suffices). The remarkable result of Hrushovski and Zilber is that with some natural additional assumptions the converse holds.

First one must see how model theory enters the picture. Given a Zariski geometry D, let $\mathcal{L}_D$ be language with an n-ary relation symbol for each closed subset of D^n. Let $\mathcal{D}$ be D viewed in the natural way as an $\mathcal{L}_D$-structure.

Lemma 4.1. The theory of $\mathcal{L}_D$ admits quantifier elimination and D is a strongly minimal set. Moreover, Morley rank in $\mathcal{D}$ is exactly dimension.

Zariski geometries may be locally modular. If X is an infinite set we can topologize X^n by taking the positive quantifier free definable sets in the language of equality (allowing parameters) as the closed sets. This determines a trivial Zariski geometry on X. If K is a field we could topologize K^n by taking the affine subsets (ie. cosets of subspaces). This is a non-trivial locally modular Zariski geometry. If a Zariski geometry is non-locally modular, then Zilber's conjecture holds

Theorem 4.2. Suppose D is a non-locally modular Zariski geometry, then $\mathcal{D}$ interprets an infinite algebraically closed field K. If $X \subseteq K^n$ is definable in $\mathcal{D}$, then X is definable using only the field structure of K (we say that K is a *pure* field).

Hrushovski and Zilber give a more refined version of 4.2 with additional geometric information. By a *family of plane curves in* D we mean closed sets $X \subseteq D^m$ and $C \subset D^2 \times X$ such that for all $a \in X$, if we let $C(a)$ denote $\{(x,y) \in D^2 : (x,y,a) \in C\}$, then $C(a)$ is a one dimensional irreducible closed subset of D^2. We say that a family of plane curves is *ample* whenever for p and q are independent generic points of D^2, there is a plane curve $C(a)$ with $p,q \in C(a)$. An ample family is called *very ample* if for p,q (not necessarily independent) generic points in D^2 there is a curve $C(a)$ with $p \in C(a)$ and $q \notin C(a)$. In this case, we say that the family *separates points*.

We say that a Zariski geometry D is (very) ample if there is a (very) ample family of curves on D. If D is ample, then from 2.2 we see that D is non-locally modular. Indeed the converse is also true. Very ample Zariski geometries are intimately related to algebraic curves.

Theorem 4.3. If D is a very ample Zariski geometry, then there is an interpretable field K, C a smooth quasi-projective curve defined over K and a definable bijection $f : D \to C$ such that the induced maps $f^n : D^n \to C^n$ are homeomorphisms for all n.

The proof of theorem 4.2 is a quite delicate application of both the group configuration and the field configuration. Suppose we have a rich family of plane curves through a point (p,p). If X and Y are two curves through (p,p) we define the composition $X \circ Y$ by $\{(x,z) : \exists y \ (x,y) \in Y, (y,z) \in X\}$. The key idea is to define an approximate notion of "tangency" and consider the "operation" $(X,Y) \mapsto Z$ where Z is tangent to $X \circ Y$ at (p,p). This gives rise to the group configuration. A more subtle construction, using the group we just found, allows us to find the field configuration. A similar type of construction in a much simpler setting is given in [MP].

We refer the reader to [M1] for a more detailed survey of Zariski geometries.

We conclude this section by giving one further setting where this work applies. Let K be a differentially closed field (see [S] or [M2]). There is a natural topology on K^n given by taking solutions to algebraic differential equations as the basic closed sets. The Ritt basis theorem implies that this is a Noetherian. For any $D \subseteq K^n$ we topologize D^n by taking the induced topology.

Theorem 4.4 ([HS]) Let D be a strongly minimal subset of K^n. Then there is a finite $X \subset D$ such that $D \setminus X$ is a Zariski geometry.

Using quantifier elimination in differentially closed fields it is clear that Z0, Z1 and Z2 hold. Hrushovski and Sokolovic show how to reduce dimension calculations to calculations in classical algebraic geometry and deduce Z3.

If D is a non-locally modular strongly minimal subset of K^n, then by 4.2, D interprets an algebraically closed field F. The field F must be of finite Morley rank (while K has Morley rank ω). There is one natural finite Morley rank field interpretable in K, namely the field of constants $C_K = \{x \in K : x' = 0\}$. Using quantifier elimination and stability (see [M2]) one can see that any subset of C_K^n definable in K is already definable in C_K using only the field structure. Sokolovic, building on work of Cassidy (see [P2]), showed this is the only small interpretable field.

Theorem 4.5. (Sokolovic) If F is an infinite finite Morley rank field interpretable in a differentially closed field K, then F is definably isomorphic to C_K.

Corollary 4.6. If K is differentially closed and $D \subset K^n$ is a non-locally modular strongly minimal set, then D interprets C_K.

§5 The Mordell-Lang conjecture for function fields

In 1993 Hrushovski [H1] found an application of geometric model theory to diophantine geometry in his proof of the Mordell-Lang conjecture for function fields. What, to me, is truly remarkable about Hrushovski's proof, is that it seems to flow naturally from the stream of ideas in current model theory. In this section I will give some of the background of the Mordell-Lang conjecture and outline Hrushovski's proof in one basic case. I refer the reader to [L] for a more detailed history of the problem.

We will work inside a large algebraically closed field $\mathbf{K}$. An abelian variety A is a projective variety equipped with a rational map $\mu : A \times A \to A$ making A into a group. We usually write the group additively. The simplest example of an abelian variety is an elliptic curve. Let E be the projective plane curve given by the equation $Y^2Z = X(X - Z)(X + \lambda Z)$. We can think of E as the plane curve $y^2 = x(x - 1)(x - \lambda)$ together with one point O at infinity (this is the point with homogeneous coordinates (0,1,0)). We must define the group law on E. The zero of the group will the point O. If P and Q are distinct points on E, consider the line l through P and Q (see diagram 2). Since E is a cubic curve the line l will intersect E in exactly three points (counting multiplicity). If R is the third point of E on l, then we say $P + Q + R = O$. Note that if P has affine coordinates (x, y), then $-P$ will have coordinates (x, y). To add a point S to itself we take l to be the tangent line to E at S. Usually l will intersect E at S with multiplicity 2. In this case there is a second point T on E such that R is also on l and $S + S + T = 0$. Otherwise, l will intersect E at S with multiplicity 3 and $S + S + S = 0$. Though it is non-trivial to verify associativity, this defines a group law on E and addition is a rational map (see [Si1] or [SiT]).

One dimensional abelian varieties are isomorphic to elliptic curves. It not easy to give algebraic descriptions of higher dimensional abelian varieties. However, if we look at complex abelian varieties there is a very easy topological description. If A is a complex abelian variety of dimension d, there are $\alpha_1, \ldots, \alpha_{2d} \in \mathbf{C}^d$ linearly independent over $\mathbf{R}$ such that A is analytically isomorphic to $\mathbf{C}^d/\Lambda$ where Λ is the lattice $\mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_{2d}$ (see [R]). The next lemma summarizes some properties of abelian varieties which we will need. The first principles are easy to verify for complex analytic varieties using the topological description.

Lemma 5.1. Let A be an abelian variety of dimension d.

i) A is a divisible abelian group. If $\mathbf{K}$ has characteristic zero or n is prime to the characteristic of $\mathbf{K}$, then A has n^{2d} n-torsion points.

ii) (rigidity (see [Mi1]) If A is defined over an algebraically closed field k, then every abelian subvariety of A is also defined over k.

Definition. Suppose Γ is a subgroup of A. We say that Γ is *finite rank* if there is a finitely generated subgroup Γ_0 such that $\Gamma \subseteq \{g \in A : ng \in \Gamma_0$ for some $n = 1, 2, \ldots\}$. For example, taking $\Gamma_0 = \{0\}$, the torsion subgroup of A is of finite rank.

We can now state the full Mordell-Lang conjecture.

Mordell-Lang Conjecture (characteristic zero) Suppose $\mathbf{K}$ has characteristic zero, A is an abelian variety, Γ is a finite rank subgroup of A and X is a proper subvariety of A. Then $X \cap \Gamma$ is a finite union of cosets of subgroups of A.

This conjecture implies the Mordell Conjecture. Suppose C is a curve of genus $g > 1$ defined over a number field k. The Mordell Conjecture asserts that C has only finitely many k-rational points (i.e. points with coordinates in k).

To any curve X of genus $g \geq 1$ we can associate a g-dimensional abelian variety $J(X)$ defined over k called the Jacobian of X (see [Mi2]). The curve X is a subvariety of $J(X)$ and $J(X)$ is the smallest abelian variety in which X embeds. If C has genus 1, then X is an elliptic curve and $J(X) = X$.

Let C have genus $g > 1$. Let Γ be the k-rational points of $J(C)$. The Mordell-Weil theorem (see [L]) asserts that Γ is a finitely generated group. Thus $\Gamma \cap C$ is a finite union of cosets of subgroups of Γ. If any of these subgroups is infinite, then the Zariski closure of that coset is also a coset and the Zariski closure must be the entire curve C. But then there would be a group structure defined on C and C would be an abelian variety contradicting the fact that $J(C) \supset C$ and $J(C)$ is the smallest abelian variety in which C embeds. Thus $C \cap \Gamma$ is finite and C contains only fintitely many k-rational points.

The Mordell conjecture was proved by Faltings who also prove the Mordell-Lang conjecture in case Γ is finitely generated. The full characteristic zero Mordell-Lang conjecture (even in the case where A is a semi-abelian variety) was proved by McQuillen ([Mc]) building on Faltings' work as well of work of Raynaud, Hindry and Vojta.

Long before Faltings, Manin [Ma] proved the function field case of the Mordell conjecture.

Theorem 5.2. (Manin) Let k be algebraically closed of characteristic zero and let $K \supset k$ be finitely generated over k. Let C be a curve of genus $g > 1$ defined over K. Then either C has only finitely many K-rational points or C is isomorphic to a curve defined over k.

So far we have only considered characteristic zero. What about characteristic $p > 0$? The obvious generalization of the Mordell-Lang conjecture to characteristic p is false. Suppose C is a curve of genus $g > 1$ defined over $\mathbf{F}_p$ and let $J(C)$ be its Jacobian. Let α be a generic point of C. Let Γ be the group of $\mathbf{F}_p(\alpha)$-rational points of $J(C)$. By the Lang-Neron theorem (the function field version of the Mordell-Weil theorem (see [Si2])) Γ is finitely generated.

If σ is the Frobenius automorphism $x \mapsto x^p$, then $\sigma^n(\alpha) \in C$ for all n. Thus $C \cap \Gamma$ is infinite, but C is not a coset of a subgroup. In this case our curve C is defined over the prime field. This leaves open the possibility that one could prove a function field version of the Mordell-Lang conjecture in all characteristics. Prior to Faltings, Buium ([Bu]) proved a characteristic zero function field version. Abramovich and Voloch [AV] had made progress in characteristic p. Finally Hrushovski proved the complete function field version (in fact Hrushovski's proof works in the more general case of "semi-abelian" varieties).

Theorem 5.3. (Mordell-Lang Conjecture for function fields) Let k be an algebraically closed field with $K \supset k$. Let A be an abelian variety defined over K , X a subvariety of A and Γ a finite rank subgroup of A. Suppose $X \cap \Gamma$ is Zariski dense in X. Then there is a subabelian variety $A_1 \subseteq A$, an abelian variety B defined over k, a surjective homomorphism $g : A_1 \to B$ and a subvariety X_0 of B defined over k, such that $g^{-1}(X_0)$ is a translate of X.

For the remainder of this section we will outline the proof of a special case of Hrushovski's theorem which illustrates the use of model theoretic ideas.

Let k be algebraically closed of characteristic zero and let $K \supset k$. Let A be an abelian variety of dimension $d > 1$ defined over K with no non-trivial subabelian varieties (such an abelian variety is called *simple*). Let Γ be the torsion points of A and let $C \subset A$ be a curve on A. We will show that either $C \cap \Gamma$ is finite or A is isomorphic to an abelian variety defined over k.

We are free to replace K by a larger field. Following Manin and Buium we see that it is useful to replace K by a rich differential field. We can find a derivation $\delta : K \to K$ such that $k = \{a \in K : \delta(a) = 0\}$, the field of constants of δ. We next replace K by the differential closure of (K, δ). Since k is already algebraically closed, passing to the differential closure of K does not add any new constants. Thus we may assume that K is differentially closed and k is the field of constants of K.

The next idea is to replace Γ by a "small" definable group $\Sigma \supseteq \Gamma$. We then have a chance of using our model theoretic tools. What do I mean by "small"? Recall that K has Morley rank ω and if V is a d-dimensional variety then V has Morley rank ωd. The next result is a compilation of work of Manin and Buium refined by Hrushovski and Sokolovic in the model theoretic setting.

Theorem 5.4. Let K be a differentially closed field and let A be an abelian variety defined over K. There is a definable group homomorphism $\mu : A \to K^n$ for some n such that $\Sigma = \ker(\mu)$ has finite Morley rank. Moreover, if A is simple we can choose μ so that $\ker(\mu)$ has no proper infinite definable subgroups.

Since K^n has no torsion, $\Gamma \subseteq \Sigma = \ker(\mu)$. We will argue that either $\Sigma \cap C$ is finite or A is isomorphic to an abelian variety defined over k. Replacing Γ by Σ allows us to use all of the tools from finite Morley rank group theory.

Let $X \subseteq \Sigma$ be a strongly minimal set containing 0. By Zilber's indecomposability theorem (see [Po2] 2.b). the subgroup of Σ generated by X is definable and for some fixed n every element of that group is a sum of n elements of X. By 5.4, since A is simple, X generates Σ. Thus Σ is in the definable closure of X and, if we consider X with all of its induced structure, Σ is interpretable in X.

We now break into cases depending on whether or not X is locally modular.

Case 1. X is locally modular.

In this case Σ is a one-based group. By the theorem 3.4, every definable subset of Σ is a Boolean combination of cosets of definable subgroups. Since Σ has no infinite definable subgroups, X must differ from Σ by a finite set. Thus Σ itself is strongly minimal.

Consider $\Sigma \cap C$. If $\Sigma \cap C$ is infinite it differs from Σ by a finite set. Thus the Zariski closure of Σ is C plus a finite set. But the torsion points of A are Zariski dense in A, thus the Zariski closure of $\Sigma = A$. Since $C \subset A$ we have a contradiction. Thus $\Sigma \cap C$ is finite.

Case 2. X is non-locally modular.

As we pointed out in 4.6, in a differentially closed field any non-locally modular strongly minimal set interprets the field of constants. So we have a strongly minimal set X which interprets the field of constants k and the group Σ. Using Hrushovski's analysis of non-orthogonality in groups (see [Po2] 2.e), it follows that there is a group G interpretable in k, and a definable homomorphism h from Σ onto G. Since Σ is minimal h has finite kernel.

Using quantifier elimination and stability one sees that k is a pure algebraically closed field. That is: any subset of k^n defined in the differentially closed field k is already definable using the field structure of k. Thus the group G is interpreted in the pure algebraically closed field k. But then there is an algebraic group G_0 defined over k such that G is isomorphic to $G_0(k)$, the k-rational points of G_0 ([Po2] 4.e).

Using the fact that Σ has only finitely many $|\ker(h)|$-torsion point, one constructs a dual homomorphism $g : G_0(k) \to \Sigma$ with finite kernel. Modding out by the kernel we may assume that g is an isomorphism. Since the derivation is trivial on k, g must be a rational map. Since $g : G_0(k) \to A$ and $G_0(k)$ is Zariski dense in $G_0(K)$, $g : G_0(K) \to A$. Since Γ is Zariski dense in A, g is surjective.

Let $N \subset G_0$ be a maximal linear algebraic subgroup. By a theorem of Chevalley ([Sh]) G_0/N is an abelian variety. Since there are no nontrivial homomorphisms from a linear group into an abelian variety, $N \subseteq \ker g$. Thus we can replace G_0 by the abelian variety G_0/N. Since N is defined over k, we may assume that G_0 is abelian variety defined over K. The rigidity of abelian varieties implies that every abelian subvariety of G_0 is definable over k. In particular $\ker(g)$ is defined over k. Thus A is isomorphic to the abelian variety $G_0/\ker(g)$ which is defined over k.

We conclude with a few words on what is needed to prove the full theorem. The proof of Hrushvoski's theorem when A is not simple or Γ is a more general finite rank group requires a slightly more subtle analysis of the finite Morley rank groups that arise. We refer the reader to [Bo2] for a detailed account of the proof in this case. In characteristic p we work with separably closed fields rather than differentially closed fields. Separably closed fields are stable but, unlike differentially closed fields, are not ω-stable. This leads to a number of complications because we must now consider types rather than definable sets. We must also use more general geometric model theory (see [Pi1]). On the other hand rather than the complicated group $\ker(\mu)$ from Lemma 4.4, one uses $\bigcap_{m=1}^{\infty} mA$.

There are a number of very good discussions of Hrushovski's proof. I suggest that the interested reader consult [Bo2], [P3], [Po2] or [H4] in addition to the original article [H1].

References

[AV] D. Abramovich and J. Voloch, Towards a proof of the Mordell-Lang conjecture in positive characteristic, Duke Math. J. 5 (1992).

[BL] J. Baldwin and A. Lachlan, On strongly minimal sets, J. Symbolic Logic 36 (1971).

[Bo1] E. Bouscaren, The group configuration-after E. Hrushovski, *The Model Theory of Groups*, A. Nesin and A. Pillay ed., Notre Dame Press, 1989.

[Bo2] E. Bouscaren, The proof of the Mordell-Lang conjecture, in [BoL], to appear.

[BoL] E. Bouscaren and D. Lascar, *Stability Theory and Algebraic Geometry: an introduction*, Springer Lecture Notes, to appear.

[Bu] A. Buium, Intersections in jet spaces and a conjecture of S. Lang, Annals of Math. 136 (1992).

[CK] C.C. Chang and H. J. Keisler, *Model Theory*, North Holland, 1977.

[CS] G. Cornell and J. Silverman, *Arithmetic Geometry*, Springer, 1986.

[H1] E. Hrushovski, The Mordell-Lang conjecture, J. AMS 9 (1996).

[H2] E. Hrushovski, A new strongly minimal set, Ann. Pure and Applied Logic 62 (1993).

[H3] E. Hrushovski, Strongly minimal expansions of algebraically closed fields, Israel J. Math. 79 (1992).

[H4] E. Hrushovski, Stability and its uses, Ĉurrent Developments in Mathematics, R. Bott et. al. ed., International Press Inc., 1996.

[HP] E. Hrushovski and A. Pillay, Weakly normal groups, *Logic Colloquium '85*, North Holland, 1987.

[HS] E. Hrushovski and Z. Sokolovic, Minimal sets in differentially closed set, Trans. AMS, to appear.

[HZ1] E. Hrushovski and B. Zilber, Zariski geometries, J. AMS 9 (1996).

[HZ2] E. Hrushovski and B. Zilber, Zariski geometries, Bull. AMS 28 (1993).

[L] S. Lang, *Number Theory III*, Springer Verlag, 1991.

[Ma] J. Manin, Rational points of algebraic curves over function fields, AMS Translations ser. II 59 (1966).

[M1] D. Marker, Zariski Geometries, to appear in [BoL].

[M2] D. Marker, Model Theory of Differential Fields, in [MMP].

[MMP] D. Marker, M. Messmer and A. Pillay, *Model Theory of Fields*, Lecture Notes in Logic 5, Springer Verlag, 1996.

[MP] D. Marker and A. Pillay, Reducts of $(\mathbf{C}, +, \cdot)$ which contain $+$, J. Symbolic Logic 55 (1990).

[Mc] M. McQuillen, Division points on semi-abelian varieties, Inventiones Math., 120 (1995), 143-159.

[Mi1] J. Milne, Abelian varieties, in [CS].

[Mi2] J . Milne, Jacobian varieties, in [CS]

[P1] A. Pillay, *Geometric Stability Theory*, Oxford University Press, 1996.

[P2] A. Pillay, Differential algebraic groups and the number of countable differentially closed fields, in [MMP].

[P3] A. Pillay, Model theory and diophantine geometry, Bull. Symbolic Logic, to appear.

[Po1] B. Poizat, *Groupes Stables*, Nur Al-Maniq wal-Ma'rifah, 1987.

[Po2] B. Poizat, H. L. M. (Hrushovski-Lang-Mordell), *Seminare Boubaki*, to appear.

[R] M. Rosen, Abelian varieties over $\mathbf{C}$, in [CS]

[S] G. Sacks, *Saturated Model Theory*, Benjamin, 1972.

[Sh] I. Shafarevich, *Basic Algebraic Geometry*, Springer, 1977.

[Si1] J. Silverman, *The arithmetic of elliptic curves*, Springer 1986.

[Si2] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer 1994.

[SiT] J. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer, 1992

[Z] B. Zilber, Zariski type structures, unpublished lecture notes, University of Illinois Chicago, 1991.