1 Macintyre’s theorem

Recall from last time

**Lemma 1.1.** Let $K$ be a definable infinite field in a strongly minimal theory. Then for every $n$, the $n$th power map $K \to K$ is surjective.

**Lemma 1.2.** Let $K$ be a definable infinite field of characteristic $p > 0$. Then the Artin-Schreier map

$$
\alpha : K \to K \\
x \mapsto x^p - x
$$

is onto.

**Proof.** Similar: the map $\alpha : K \to K$ has finite fibers, so $\dim(\alpha(K)) = \dim(K)$, and therefore $|K/\alpha(K)| < \infty$. As $(K, +)^0 = (K, +)$, it follows $\alpha(K) = K$. □

We need the following purely algebraic fact:

**Fact 1.3** (Kummer, Artin-Schreier). Let $L/K$ be a Galois extension with $\text{Gal}(L/K) \cong \mathbb{Z}/p$.

1. If $\text{char}(K) \neq p$ and $K$ contains a primitive $p$th root of unity, then $L = K(\sqrt[p]{a})$ for some $a \in K$. In particular, $K \neq K^p$.

2. If $\text{char}(K) = p$, then $L = K(b)$, where $b^p - b \in K$. In particular,

$$
\alpha : K \to K \\
x \mapsto x^p - x
$$

is not surjective.

**Lemma 1.4.** Let $K$ be a field. Suppose for every finite extension $L/K$, the following maps are surjective:
• The $n$th power map $L^\times \to L^\times$ for all $n \geq 1$.

• (In characteristic $p$) the Artin-Schreier map $L \to L$.

Then $K$ is algebraically closed.

Proof. Note $K$ is perfect. If $K$ is not algebraically closed, take non-trivial $L_1/K$. Take $p$ dividing $[L_1 : K]$. Let $\zeta_p$ be a primitive $p$th root of unity. Then $p \nmid [K(\zeta_p) : K]$, so $p|[L(\zeta_p) : K(\zeta_p)]$. Replacing $K$ with $K(\zeta_p)$, we may assume $\zeta_p \in K$. Replacing $L$ with a larger field, we may assume $L/K$ is Galois. Then $p$ divides the order of $\text{Gal}(L/K)$, so $\text{Gal}(L/K)$ contains a cyclic subgroup of order $p$. Replacing $K$ with a larger field, we may assume $\text{Gal}(L/K)$ is cyclic of order $p$. Then Kummer theory or Artin-Schreier theory says that the $p$th power map or the Artin-Schreier map on $K$ is non-surjective.

Theorem 1.5. Let $K$ be a definable infinite field in a strongly minimal theory. Then $K$ is algebraically closed.

Proof. Finite extensions of $K$ are also definable fields.

2 Interpretable sets

Definition 2.1. An interpretable set in a structure $M$ is a set of the form $X/E$, where $X$ is a definable set and $E \subseteq X \times X$ is a definable equivalence relation.

Example 2.2. If $G$ is a definable group and $H$ is a definable subgroup, the quotient $G/H$ is an interpretable set.

Given a structure $M$, one can form a category $\text{Def}_M$ of definable sets and definable functions, as well as a category $\text{Int}_M$ of interpretable sets and interpretable functions. There is an embedding

$$\text{Def}_M \hookrightarrow \text{Int}_M$$

One says that $M$ has elimination of imaginaries\footnote{Technically we should work with the category of 0-definable and 0-interpretable sets (sets definable without parameters, and quotients $X/E$ where $X, E$ are 0-definable). I call the condition given here “parametric elimination of imaginaries.” It turns out to be weaker than full elimination of imaginaries. See Corollary 5.4.} if this functor is an equivalence of categories.

More concretely, this means that for any definable $X$ and $E$, there is a definable surjection $f : X \twoheadrightarrow Y$ inducing a bijection $X/E \twoheadrightarrow Y$.

Fact 2.3. If $K \models \text{ACF}$, then $K$ has elimination of imaginaries.

Fact 2.4. The following structures are strongly minimal and do not eliminate imaginaries:

• An infinite set $X$ with no structure.
• \((\mathbb{Q}, +)\).

**Theorem 2.5.** If \(M\) is any structure, there is a structure \(M^{eq}\) such that \(\text{Def}_{M^{eq}}\) is equivalent to \(\text{Int}_{M}\).

If \(M\) is strongly minimal, then rank, dimension, and degree extend to \(M^{eq}\) and satisfy all the properties of yesterday’s lecture. Elements of \(M^{eq}\) are called imaginaries.

**Example 2.6.** Macintyre’s theorem generalizes. If \(M\) is strongly minimal and \(K\) is an infinite interpretable field, then \(K \models ACF\).

### 3 Minimal groups

Let \(M\) be a strongly minimal monster. In what follows, “definable” really means “interpretable.” If you like, switch to \(M^{eq}\).

**Definition 3.1.** \(G\) is connected if \(G = G^0\).

We fix some group-theoretic notation:

- \(H \triangleleft G\) means \(H\) is a normal subgroup of \(G\)
- \(Z(a)\) denotes the centralizers of \(a\):
  \[
  Z(a) = \{g \in G \mid ag = ga\}. 
  \]
- \(Z(G)\) denotes the center of \(G\):
  \[
  Z(G) = \bigcap_{a \in G} Z(a). 
  \]
- \(a^G\) denotes the conjugacy class of \(a\):
  \[
  a^G = \{g^{-1}ag : g \in G\}. 
  \]

All these sets are definable. Note

\[
 a \in Z(G) \iff a^G = \{a\}. 
\]

Note \(G\) acts on itself by conjugation, and

- The orbit of \(a\) is \(a^G\)
- The stabilizer of \(a\) is \(Z(a)\).

Therefore,

\[
 \dim(a^G) = \dim(G) - \dim(Z(a)).
\]

Note \(Z(G) \triangleleft G\).
Lemma 3.2. If $G$ is connected, and $a \in G$ has finite conjugacy class $a^G$, then $a \in Z(G)$.

Proof. The size of $a^G$ is the index of $Z(a)$ in $G$, which is 1 if finite, as $G = G^0$. □

Proposition 3.3. If $G$ is connected and $H \triangleleft G$ is a finite normal subgroup, then $H \leq Z(G)$.

Proof. If $a \in H$ then $a^G \subseteq H$, so $a^G$ is finite, so $a \in Z(G)$. □

Proposition 3.4. Let $G$ be a connected definable group with $Z(G)$ finite. Then $G/Z(G)$ is centerless.

Proof. Let $[a]$ denote the image of $a$ under $G \to G/Z(G)$. Suppose $[a] \in Z(G/Z(G))$. Then for every $g \in G$,

$$g^{-1} \cdot a \cdot g \equiv a \pmod{Z(G)}.$$ 

Therefore $a^G \subseteq a \cdot Z(G)$ and $a^G$ is finite, implying $a \in Z(G)$ and $[a] = 1$. □

Definition 3.5. A definable group $(G, \cdot)$ is minimal if $G$ is infinite, but every definable proper subgroup is finite.

Remark 3.6. If $G$ is definable and infinite, there is definable minimal $H \leq G$, by DCC on definable subgroups.

Lemma 3.7. If $G$ is minimal and $H$ is a finite normal subgroup, then $G/H$ is minimal.

If $G$ is minimal, then $G = G^0$.

Proof. For the first point, note that any infinite definable proper subgroup of $G/H$ pulls back to an infinite definable proper subgroup of $G$. For the second point, note that $G^0$ is an infinite definable subgroup of $G$. □

Theorem 3.8 (Reineke). Let $G$ be a minimal group. Then $G$ is connected and abelian.

Proof. Note $G$ is connected. Suppose $G$ is non-abelian. Then $Z(G) \neq G$, so $Z(G)$ is finite. Let $H = G/Z(G)$. Then $H$ is minimal, and centerless by Proposition 3.4. So $H$ is a connected non-abelian centerless minimal group.

Claim 3.9. If $a, b \in H$ are non-trivial, then $a, b$ are conjugate. So there is only one non-trivial conjugacy class in $H$.

Proof. As $a$ is non-central, the centralizer $Z(a)$ is a definable proper subgroup of $H$, so $Z(a)$ is finite. Counting ranks,

$$\dim(a^H) = \dim(H) - \dim(Z(a)) = \dim(H).$$

Similarly, $\dim(b^H) = \dim(H)$. As $H = H^0$, the Morley degree of $H$ is 1 and so $a^H$ and $b^H$ cannot be disjoint. Thus $a$ and $b$ are conjugate. □

Take some non-trivial $a \in H$. 

4
• If \( a^2 = 1 \), then by symmetry \( b^2 = 1 \) for all \( b \) conjugate to \( a \). Thus \( b^2 = 1 \) for all \( b \in H \), and \( H \) is abelian, a contradiction.

• Suppose \( a^2 \neq 1 \). Then \( a \neq a^{-1} \). Take \( b \) such that \( b^{-1}ab = a^{-1} \). Then

\[
\begin{align*}
  b^{-1}ab &= a^{-1} \\
  b^{-2}ab^2 &= b^{-1}a^{-1}b = a
\end{align*}
\]

Therefore \( a \notin Z(b) \) but \( a \in Z(b^2) \). It follows that

\( Z(b) < Z(b^2) \).

On the other hand \( b^2 \neq 1 \) (because \( b \) and \( a \) are conjugate and \( a^2 \neq 1 \)), so \( b \) and \( b^2 \) are conjugate. By symmetry, \( |Z(b)| = |Z(b^2)| \), contradicting \( Z(b) \subsetneq Z(b^2) \).

\[\Box\]

**Corollary 3.10.** For any infinite definable \( G \) there is an infinite definable abelian subgroup \( H \leq G \).

**Corollary 3.11.** If \( G = G^0 \) and \( \dim(G) = 1 \), then \( G \) is minimal, and therefore abelian.

**Proof.** If \( G \) fails to be minimal, take an infinite definable \( H < G \). Then \( 0 < \dim(H) \leq \dim(G) = 1 \), so \( \dim(H) = \dim(G) \). But then \( \dim(G/H) = 0 \), so \( H \) has finite index, contradicting \( G = G^0 \).

\[\Box\]

It is *not* true that every group of finite Morley rank has a definable subgroup of rank 1, but the examples are hard to come by.

### 4 Zilber indecomposability

Let \( G \) be a definable group.

**Definition 4.1.** A definable set \( X \subseteq G \) is indecomposable if for any definable subgroup \( H \leq G \), the quotient \( X/H \) is infinite or size 1.

**Proposition 4.2.** If \( X \subseteq G \) is definable, then \( X \) is a disjoint union \( X_1 \sqcup \cdots \sqcup X_n \) with \( X_i \) indecomposable.

(This decomposition isn’t unique)

**Theorem 4.3** (Zilber indecomposability). If \( X \subseteq G \) is indecomposable and \( 1 \in X \), then the subgroup \( \langle X \rangle \leq G \) generated by \( X \) is definable and connected. More generally, suppose \( \mathcal{F} \) is a collection of indecomposable sets containing \( 1 \). Then \( \langle \bigcup \mathcal{F} \rangle \) is definable and connected.

\[\text{Note } Z(b) \text{ is finite because } Z(b) < H \text{ and } H \text{ is minimal.} \]
**Lemma 4.4.** Suppose $M$ acts on $G$. Suppose $X \subseteq G$ is fixed setwise by $M$. Suppose that for every $M$-invariant definable subgroup $H \leq G$ the quotient $X/H$ is a singleton or infinite. Then $X$ is indecomposable.

*Proof.* Suppose $X$ fails to be indecomposable. Take $H_0$ such that $1 < |X/H_0| < \aleph_0$. Let $H$ be the intersection of all conjugates of $H_0$ under $M$. By dcc, $H$ is a finite intersection $H_0 \cap H_1 \cap \cdots H_n$ where each $H_i$ is a conjugate under $M$ of $H_0$. As $X$ is invariant under $M$, each quotient $X/H_i$ has the same size as $X/H_0$, and is in particular finite. Therefore

$$X/H = X/(H_0 \cap \cdots \cap H_n)$$

is finite.

But $H$ is $M$-invariant, so this contradicts the assumption. 

**Example 4.5.** If $G$ is connected, then $[G, G]$ is definable and connected. Here, $[G, G]$ denotes the derived subgroup—the subgroup generated by commutators $a^{-1}b^{-1}ab$.

*Proof.* We claim that for each $a \in G$, the set $a^G$ is indecomposable. It is closed under conjugation, so we only need to consider quotients $a^G/N$ where $N \trianglelefteq G$. Now $a^G/N$ is the conjugacy class of $a$ in $G/N$, which is either a singleton or infinite, because $G/N$ is connected. Thus $a^G$ is indecomposable. The left-translate $a^{-1} \cdot a^G$ is also indecomposable, and contains $1 = a^{-1} \cdot a$. Let $\mathcal{F}$ be

$$\{a^{-1} \cdot a^G : a \in G\}$$

Then $[G, G]$ is $\langle \bigcup \mathcal{F}\rangle$, so $[G, G]$ is definable and connected. 

**Definition 4.6.** A definable group $G$ is definably simple if $G$ has no proper non-trivial definable normal subgroup.

**Lemma 4.7.** Let $G$ be definably simple. Let $X \subseteq G$ be closed under conjugation. If $X$ is infinite, then $X$ is indecomposable.

*Proof.* By the lemma we only need to consider the quotients $X/G$ and $X/1$. The first has size 1 and the second is infinite. 

**Theorem 4.8.** Let $G$ be a non-abelian definably simple group. Then $G$ is simple.

*Proof.* Suppose $G$ is definably simple. If $G$ is finite, every subgroup is definable, so $G$ is simple. Assume $G$ infinite. Then $G = G^0$ or else $G^0$ is a proper normal non-trivial definable subgroup. By non-abelianity, $Z(G)$ is a proper subgroup, normal as always. So $Z(G) = 1$ by definable simplicity.

Given $a \in G \setminus \{1\}$, we have $a \notin Z(G)$, so $Z(a) < G$. As $G = G^0$ it follows $\dim(Z(a)) < \dim(G)$, so $\dim(a^G) = \dim(G) - \dim(Z(a)) > 0$. Thus $a^G \cup \{1\}$ is infinite. It is closed under conjugation, so $a^G \cup \{1\}$ is indecomposable. By Zilber’s indecomposability theorem,

$$H = \langle a^G \cup \{1\} \rangle$$
is a definable non-trivial subgroup. It is closed under conjugation, so $H \triangleleft G$. By definable simplicity, $H = G$. So
\[ \langle a^G \rangle = G \]
for all $a \neq 1$.

Now if $H$ is an abstract normal subgroup, take $a \in H$, and note $a^G \subseteq H$, so
\[ \langle a^G \rangle \leq H \implies H = G. \]

Therefore $G$ is simple.

\[ \square \]

**Lemma 4.9.** If $G$ is connected and non-trivial then $G$ has a definable proper normal subgroup $H$ (possibly trivial) such that $G/H$ is abelian or simple.

**Proof.** Proceed by induction on $\dim(G)$. If $\dim(G) = 0$, then $G$ is finite, and we can take $H$ a maximal proper normal subgroup. Suppose $\dim(G) > 0$. If there is an infinite proper normal subgroup $K \triangleleft G$, then $\dim(G/K) = \dim(G) - \dim(K) < \dim(G)$, and by induction there is $H/K \triangleleft G/K$ such that $(G/K)/(H/K) \cong G/H$ is simple or abelian. So we may assume every definable proper normal subgroup of $G$ is finite. In particular, $G = G^0$. If $G$ is abelian, take $H = 1$. Otherwise, $Z(G)$ is finite and every proper normal $K \triangleleft G$ satisfies $K \leq Z(G)$. Therefore $G/Z(G)$ is definably simple, so we can take $H = Z(G)$.

\[ \square \]

**Theorem 4.10.** Let $G$ be any definable group. Then there is a subnormal sequence of definable groups such that the quotients are abelian or simple.

**Proof.** Build a sequence $G = G_0 \triangleright G_1 \triangleright \cdots$ by taking $G_{i+1}$ to be a proper normal subgroup of $G_i$ with quotient $G_{i+1}/G_i$ that is abelian or simple. Eventually the process terminates, by DCC.

\[ \square \]

5 Exercises

**Exercise 5.1.** The field $\mathbb{Q}$ is not algebraically closed. Write down a formula $\phi(x)$ such that $\phi(\mathbb{Q})$ is neither finite nor cofinite.

**Exercise 5.2.** In the field $\mathbb{C}$, let $X = \mathbb{C} \times \mathbb{C}$ and let $E$ be the equivalence relation whose equivalence classes are the sets $\{(x,y), (y,x)\}$. Find a definable set $Y$ and definable function $f : X \to Y$ such that
\[ \forall a, b \in X : a Eb \iff f(a) = f(b). \]

**Exercise 5.3.**

- Let $G$ be a definable group, $X$ be a definable set, and suppose $G$ has a transitive definable group action on $X$. If $G = G^0$, show that $\deg(X) = 1$.

- Equivalently, show that if $G = G^0$ is definable and $H \leq G$ is definable, then $\deg(G/H) = 1$.  

In particular, if \( H \triangleleft G \) and \( G = G^0 \), then \((G/H)^0 = G/H\).

**Exercise 5.4.** If \((G, +)\) is minimal, then one of the following holds:
- \( G \) is an infinite \( \mathbb{F}_p \)-vector space for some prime \( p \).
- \( G \) is divisible, and for every \( n \geq 1 \) has finite \( n \)-torsion.

**Solution.** Let \( G[n] \) denote the group of \( n \)-torsion. If \( G[p] \) is infinite for any prime \( p \), then \( G[p] = G \) by minimality. So assume \( G[p] \) is finite for all \( p \). Then the map \( x \mapsto p \cdot x \) has finite fibers, and its image must be a subgroup of rank \( \dim(G) \). As \( G = G^0 \) by minimality, this implies the map is surjective. So \( G \) is divisible. For any \( n \geq 1 \) the short exact sequence
\[
0 \to G[n] \to G \xrightarrow{x \mapsto n \cdot x} G \to 0
\]
shows \( G[n] \) has rank 0, i.e., is finite.

6  **Appendix: imaginaries and interpretable sets**

In mathematics, we often need to be able to take the quotient of a set \( X \) by an equivalence relation \( E \subseteq X \times X \).

**Definition 6.1.** If \( A \subseteq M \), an \( A \)-interpretable set is a set of the form \( X/E \) where \( X \) is \( A \)-definable and \( E \subseteq X \times X \) is an \( A \)-definable equivalence relation. An interpretable set is an \( A \)-interpretable set for some \( A \).

**Definition 6.2.** A structure \( M \) has elimination of imaginaries if for every 0-interpretable set \( X/E \), there is a 0-definable set \( Y \) and a bijection \( X/E \to Y \) such that the composition
\[
X \to X/E \to Y
\]
is 0-definable.

Another way of saying this is that given 0-definable \( X/E \), there is a 0-definable surjection \( f : X \to Y \) such that
\[
\forall x_1, x_2 \in X : (f(x_1) = f(x_2) \iff x_1 E x_2).
\]

**Proposition 6.3.** Let \( M \) have elimination of imaginaries.

1. If \( M' \equiv M \) then \( M' \) has elimination of imaginaries.

2. Any expansion of \( M \) by constants has elimination of imaginaries.

**Proof.** 1. Given a 0-interpretable set \( X'/E' \) in \( M' \), take formulas \( \phi(x) \) and \( \psi(x_1, x_2) \) such that \( X' = \phi(M') \) and \( E' = \psi(M') \). Let \( X = \phi(M) \) and \( E = \psi(M) \). Using the fact that \( M \equiv M' \), one sees easily that \( E \) is an equivalence relation on \( X \). Take a 0-definable set \( Y \) and a 0-definable surjection \( f : X \to Y \) eliminating \( X/E \). The one can transfer \( Y \) and \( f \) back to \( M' \) in the same fashion. We leave the details as an exercise.
2. Suppose $X/E$ is interpretable, where $X = \phi(M; b_0)$ and $E = \psi(M; b_0)$ for some tuple of new constants $b_0$. Let $B$ be the set of $b$ such that $\psi(M; b)$ is an equivalence relation on $\phi(M; b)$. The set $B$ is definable and contains $b_0$. Consider the 0-definable sets

$$\tilde{X} := \{(a, b) : b \in B, \ M \models \phi(a, b)\}$$

$$\tilde{E} := \{(a_1, b; a_2, b) : b \in B, \ M \models \psi(a_1, a_2, b)\}.$$  

Then $\tilde{E}$ is an equivalence relation on $\tilde{X}$. By elimination of imaginaries there is a 0-definable bijection $\tilde{f} : \tilde{X}/\tilde{E} \to \tilde{Y}$ with

$$\tilde{f}(a_1, b_1) = f(a_2, b_2) \iff b_1 = b_2 \land M \models \psi(a_1, a_2, b_1).$$

Let $f(a) = \tilde{f}(b_0)$. Then $f : X \to \tilde{Y}$ is $b_0$-definable, and

$$f(a_1) = f(a_2) \iff (M \models \psi(a_1, a_2, b_0)) \iff a_1 E a_2.$$  

Thus the quotient $X/E$ is eliminated.

\[ \square \]

**Corollary 6.4.** If $M$ has elimination of imaginaries, for every interpretable set $X/E$ there is a definable set $Y$ and a bijection $X/E \to Y$ such that the composition

$$X \to X/E \to Y$$

is definable.

**Definition 6.5.** Let $X$ be a definable set in a monster model $\mathbb{M}$. A finite tuple $c$ is a code for $X$ if for every $\sigma \in \text{Aut}(\mathbb{M})$, the following are equivalent:

- $\sigma$ fixes $X$ setwise.
- $\sigma$ fixes $c$ pointwise.

**Proposition 6.6.** Suppose $X$ has a code $c$.

- $X$ is $c$-definable.
- More generally, $X$ is $A$-definable iff $c \in \text{dcl}(A)$.
- If $c'$ is another code, then $\text{dcl}(c) = \text{dcl}(c')$ (c and $c'$ are “interdefinable.”).

**Proof.** The second point implies the first and third points. For the second point, we may assume $A$ is small. Then

- $X$ is $A$-definable iff $X$ is fixed setwise by $\text{Aut}(\mathbb{M}/A)$.
- $c \in \text{dcl}(A)$ iff $c$ is fixed pointwise by $\text{Aut}(\mathbb{M}/A)$,
so the two are equivalent by definition of codes.

Because the code is unique up to interdefinability, we often talk about “the” code for \(X\), denoted \(⌜X⌝\).

**Proposition 6.7.** If \(\mathcal{M}\) eliminates imaginaries, then every definable set has a code.

Proof. Let \(X = \phi(\mathcal{M}; b_0)\) be a definable set. Let \(k = |b_0|\) and let \(E\) be the 0-definable equivalence relation on \(\mathcal{M}^k\) given by

\[
bEb' \iff \phi(\mathcal{M}; b) = \phi(\mathcal{M}; b').
\]

Take 0-definable \(f : \mathcal{M}^k \to Y\) such that

\[
f(b) = f(b') \iff bEb' \iff \phi(\mathcal{M}; b) = \phi(\mathcal{M}; b').
\]

Then for any \(\sigma \in \text{Aut}(\mathcal{M})\),

\[
\sigma(f(b_0)) = f(b_0) \iff f(\sigma(b_0)) = f(b_0) \iff \phi(\mathcal{M}; \sigma(b_0)) = \phi(\mathcal{M}; b_0) \iff \sigma(\phi(\mathcal{M}; b_0)) = \phi(\mathcal{M}; b_0) \iff \sigma(X) = X.
\]

Later we will see a converse.

**Lemma 6.8.** If \(\mathcal{M} \models ACF\) and \(V \subseteq \mathcal{M}^n\) is an \(\mathcal{M}\)-linear subspace, then \(V\) has a code \(c\).

Proof sketch. Let \(k = \dim(V)\). There is some coordinate projection \(\pi : \mathcal{M}^n \to \mathcal{M}^k\) such that \(\pi(V) = \mathcal{M}^k\) and the induced map

\[
V \to \pi(V) = \mathcal{M}^k
\]

is an isomorphism. The inverse of this isomorphism is an \(\mathcal{M}\)-linear map

\[
\mathcal{M}^k \to V \hookrightarrow \mathcal{M}^n.
\]

This map is coded by an \(n \times k\) matrix. The entries of this matrix are a code for \(V\). (Exercise: fill in the details.)

**Lemma 6.9.** If \(\mathcal{M} \models ACF\) and \(S \subseteq \mathcal{M}^n\) is finite, then \(S\) has a code.

Proof. For each \(\bar{a} \in \mathcal{M}^n\), let \(p_{\bar{a}}\) be the ideal in \(\mathcal{M}[X_1, \ldots, X_n]\) consisting of polynomials \(P(X_1, \ldots, X_n)\) vanishing at \(\bar{a}\). Each \(p_{\bar{a}}\) is a maximal ideal of \(\mathcal{M}[X_1, \ldots, X_n]\). Let

\[
I = \bigcap_{\bar{a} \in S} p_{\bar{a}}.
\]
By commutative algebra, one can recover $S$ from $I$ as follows:

$$S = \{ \bar{a} : p\bar{a} \supseteq I \}.$$ 

There is an action of $\text{Aut}(\mathbb{M})$ on $\mathbb{M}[X_1, \ldots, X_n]$, and we see that $\sigma \in \text{Aut}(\mathbb{M})$ fixes $S$ setwise iff $\sigma$ fixes $I$ setwise.

For each $d$, let $V_d$ be the $\mathbb{M}$-vector space of polynomials of degree $\leq d$. Then $V_d \cap I$ has a code $c_d$ for each $d$. Then for any $\sigma \in \text{Aut}(\mathbb{M})$, the following are equivalent:

- $\sigma$ fixes $S$ setwise
- $\sigma$ fixes $I$ setwise
- $\sigma$ fixes $C := \{c_1, c_2, \ldots\}$ pointwise.

Therefore $S$ is $C$-definable, hence $\bar{d}$-definable for some finite tuple $\bar{d}$ from $C$. But then the following are equivalent for $\sigma \in \text{Aut}(\mathbb{M})$:

1. $\sigma$ fixes $S$ setwise
2. $\sigma$ fixes $C$ pointwise
3. $\sigma$ fixes $\bar{d}$ pointwise,

because $1 \implies 2 \implies 3 \implies 1$. So $\bar{d}$ is a code for $S$. \hfill \Box

In the next section, we will use strong minimality to show that ACF eliminates imaginaries.

Given a complete theory $T$, we can form a (multi-sorted) theory $T^\text{eq}$ which has a sort for each 0-interpretable set $X/E$. Every model $M \models T$ yields a model $M^\text{eq} \models T^\text{eq}$. The theory $T^\text{eq}$ eliminates imaginaries. In a certain sense, $T$ and $T^\text{eq}$ are “the same thing.” For example:

- The category of models of $T$ is equivalent to the category of models of $T^\text{eq}$. In particular, $\text{Aut}(M) \cong \text{Aut}(M^\text{eq})$.

- The category of 0-interpretable sets in $T$ is equivalent to the category of 0-interpretable sets in $T^\text{eq}$, or the category of 0-definable sets in $T^\text{eq}$.

- In particular, if $X \subseteq \mathbb{M}^n$ is definable in $\mathbb{M}^\text{eq}$, it is definable in $\mathbb{M}$.

**Exercise 6.10.** $\mathbb{M}$ is $\kappa$-saturated and $\kappa$-homogeneous iff $\mathbb{M}^\text{eq}$ is $\kappa$-saturated and $\kappa$-homogeneous.

Elements of $\mathbb{M}^\text{eq}$ are called “imaginaries.”

**Theorem 6.11.** Suppose $\mathbb{M}$ is a monster model. Then the following Suppose $\mathbb{M}$ and $\mathbb{M}^\text{eq}$ are monster models. Then the following are equivalent:

1. For every 0-definable set $X$ in $\mathbb{M}$ and definable equivalence relation $E$ in $\mathbb{M}$, the set $X/E$ in $\mathbb{M}^\text{eq}$ is in 0-definable bijection with a definable set in $\mathbb{M}$. 

11
2. \( M \) has elimination of imaginaries.

3. Every definable set \( X \subseteq M^n \) has a code in \( M \).

4. For every imaginary \( e \in M^{eq} \), there is an interdefinable real tuple \( a \in M^n \).

Technically, we need to assume that if \( D_1, D_2 \) are definable sets, then the disjoint union \( D_1 \sqcup D_2 \) also is a definable set. This holds if there are two distinct constant symbols (like \( 0, 1 \) in ACF), or if we had set up the category of definable sets “correctly.”

**Proof.** The implication \( 1 \implies 2 \) is easy. The implication \( 2 \implies 3 \) was proven earlier.

For \( 3 \implies 4 \), if \( e \in M^{eq} \) then \( e \in X/E \) for some 0-definable set \( X \subseteq M^n \) and 0-definable equivalence relation \( E \subseteq X \times X \). Let \([a]_E\) denote the \( E \)-equivalence class of \( a \in X \). Then \( e \) is some set \([a]_E\), so \( e \) is a code for \([a]_E\). On the other hand, \( e \) has a real code \( b \in M^k \), so \( e \) and \( b \) are interdefinable.

It remains to show \( 4 \implies 1 \). Let \( X/E \) be 0-interpretable in \( M \). Then \( X/E \) is a 0-definable set in \( M^{eq} \).

**Claim 6.12.** For every \( e \in X/E \) there is \( n \geq 0 \) and \( a \in M^n \) and an \( L^{eq} \)-formula \( \phi(x,y) \) such that

\[
\begin{align*}
\phi(e, M^{eq}) &= \{a\} \\
\phi(M^{eq}, a) &= \{e\}
\end{align*}
\]

**Proof.** By assumption (4), there is some real tuple \( a \in M^n \) interdefinable with \( e \). Then

\[
\begin{align*}
\psi(e, M^{eq}) &= \{a\} \\
\chi(M^{eq}, a) &= \{e\}
\end{align*}
\]

for some formulas \( \psi \) and \( \chi \). Take \( \phi = \psi \land \chi \).

Let \( Q = X/E \). For each formula \( \phi(x,y) \), let \( Q_\phi \) be the 0-definable set of \( e \in Q \) such that there is \( a \) such that

\[
\begin{align*}
\phi(e, M^{eq}) &= \{a\} \\
\phi(M^{eq}, a) &= \{e\}.
\end{align*}
\]

Then \( \phi \) determines a bijection \( f_\phi \) from \( Q_\phi \) to some definable set \( Y_\phi \). The collection of \( Q_\phi \) covers \( Q \) (by the claim), so by compactness

\[
Q = Q_{\phi_1} \cup \cdots \cup Q_{\phi_m}
\]

for some \( \phi_1, \ldots, \phi_m \). One can find 0-definable subsets \( Q'_i \subseteq Q_{\phi_i} \) such that the \( Q'_i \) form a partition:

\[
Q = Q'_1 \cup \cdots \cup Q'_m.
\]

(For example, take \( Q'_i = Q_i \setminus \bigcup_{j<i} Q_j \).) Then \( f_\phi|Q'_i \) is a bijection \( Q'_i \to Y'_i \) for some 0-definable \( Y'_i \subseteq Y_\phi \). These can be glued to yield a definable bijection

\[
Q'_1 \sqcup \cdots \sqcup Q'_m \cong Y'_1 \sqcup \cdots \sqcup Y'_m.
\]

Because we are cheating, the right hand side is a definable set in \( M \). \( \Box \)
7 Appendix: interpretable sets in strongly minimal theories

Fix $\mathbb{M}$ a strongly minimal monster.

**Lemma 7.1.** If $M \preceq \mathbb{M}$ and $X \subseteq \mathbb{M}^n$ is definable and non-empty, there is $a \in X$ such that
\[ a \in \text{acl}(\langle X \rangle S) \]

*Proof.* By induction on $n$. If $n = 1$, then $X$ is finite or cofinite. In the finite case, the finite set $X$ is $\langle X \rangle$-definable, so we can take any $a \in X$. In the cofinite case, $X \cap M \neq \emptyset$ so we can take any $a \in M$. Next suppose $n > 1$. Let $Y = \pi(X)$ where $\pi : \mathbb{M}^n \to \mathbb{M}^{n-1}$ is a coordinate projection. By induction there is $b \in Y \cap \text{acl}(\langle Y \rangle)$. Now $\langle Y \rangle \in \text{dcl}(\langle X \rangle)$, so
\[ b \in \text{acl}(\langle X \rangle) \]

Next let $Z = \{ c \in \mathbb{M} : (b, c) \in X \}$. Then $Z$ is non-empty because $b \in Y = \pi(X)$. By induction, there is $c \in Z$ such that
\[ c \in \text{acl}(\langle Z \rangle) \subseteq \text{acl}(\langle Y \rangle), \]
using the fact that $Z$ is defined from $b$ and $\langle X \rangle$. Now $(b, c) \in X$ and
\[ (b, c) \in \text{acl}(\langle Y \rangle) = \text{acl}(\langle X \rangle), \]

because $b \in \text{acl}(\langle X \rangle)$.

**Lemma 7.2.** If $M \preceq \mathbb{M}$ and $e \in \mathbb{M}^{eq}$ is any imaginary, then there is a real tuple $a$ from $\mathbb{M}$ such that
\[ a \in \text{acl}(\langle e \rangle) \]
\[ e \in \text{dcl}(\langle a \rangle). \]

*Proof.* Write $e$ as an element of $X/E$ for some 0-definable set $X \subseteq \mathbb{M}^n$ and some 0-definable $E \subseteq X \times X$. Let $Y$ be the equivalence class represented by $e$. Then $e = \langle Y \rangle$. Take $a \in Y$ such that $a \in \text{acl}(\langle e \rangle)$. Then $e \in \text{dcl}(\langle a \rangle)$ because $a \mapsto e$ under $X \rightarrow X/E$.

**Proposition 7.3.** If $\text{acl}(\emptyset)$ is infinite, then every imaginary $e \in \mathbb{M}^{eq}$ is interdefinable with an imaginary of the form $\langle Y \rangle$ for $Y \subseteq \mathbb{M}^n$ a finite set.

*Proof.* Let $M = \text{acl}(\emptyset)$. Choose a real tuple $a \in \mathbb{M}^n$ such that
\[ a \in \text{acl}(\langle e \rangle) \]
\[ e \in \text{dcl}(\langle a \rangle). \]

Let $Y$ be the finite orbit of $a$ under $\text{Aut}(\mathbb{M}^{eq}/e)$. Then $\text{Aut}(\mathbb{M}^{eq}/e)$ fixes $Y$ setwise, so
\[ \langle Y \rangle \in \text{dcl}(\langle e \rangle). \]

Pick some 0-definable function $f$ such that $e = f(a)$. Then by symmetry, $e = f(a')$ for any $a' \in Y$. Therefore $e \in \text{dcl}(\langle Y \rangle)$. So $e$ is interdefinable with $\langle Y \rangle$.
Corollary 7.4. ACF has elimination of imaginaries.

Definition 7.5. A small subset $S \subseteq M^{eq}$ is a “good base” if $acl(S) \cap M$ is infinite.

Remark 7.6. If $S$ is a good base, then $acl^{eq}(S) = dcl^{eq}(M)$ for some small $M \leq M$, namely $M = acl^{eq}(S) \cap M$. (To see this, given $e \in acl^{eq}(S)$ find $a \in acl(Me)$ such that $e \in dcl^{eq}(a)$.)

Definition 7.7. If $e \in M^{eq}$ and $S$ is a good base, then the rank $R(e/S)$ is for any/every real tuple a such that $acl(eS) = acl(aS)$.

One can define $R(e/S)$ when $S$ is bad, but it takes a little more work and we won’t need it.

Lemma 7.8 (Lascar equality). $R(e_1 e_2 / S) = R(e_1 / S e_2) + R(e_2 / S)$.

Proof. Replace $S$ with a set of reals, and $e_1$ and $e_2$ with equivalent reals.

Lemma 7.9 (Extension). If $S \subseteq S'$ is an inclusion of good bases and $e$ is an imaginary, there is $e'$ such that

$$R(e'/S') = R(e/S).$$

Proof. Replacing $S$ and $S'$ with $acl(S) \cap M$ and $acl(S') \cap M$, we may assume $S$ and $S'$ are sets of reals. Take a lifting $e$, so $e \in dcl^{eq}(a)$ and $a \in acl(Se)$. By our earlier extension lemma, there is $\sigma \in Aut(M/S)$ such that

$$R(\sigma(a)/S') = R(\sigma(a)/S) = R(a/S).$$

But then $\sigma(e) \equiv_S e$, and $\sigma(e)$ is interalgebraic with $\sigma(a)$ over $S$. Therefore

$$R(\sigma(e)/S') = R(\sigma(a)/S') = R(a/S) = R(e/S).$$

Definition 7.10. If $X$ is an interpretable set, define $dim(X)$ to be $\max\{R(e/S) : e \in X\}$ for any good base $S$ over which $X$ is defined.

Corollary 7.11. The number $dim(X)$ is well-defined, independent of the choice of $S$.

Theorem 7.12. Dimension has the following properties:

1. $dim(X \cup Y) = \max(dim(X), dim(Y))$.
2. $dim(X \times Y) = dim(X) + dim(Y)$.
3. If $f : X \to Y$ is an interpretable bijection, then $dim(X) = dim(Y)$.
4. If \( f : X \to Y \) is an interpretable surjection, and \( \dim(f^{-1}(y)) = k \) for all \( y \in Y \), then 
\[ \dim(X) = k + \dim(Y) \]

5. Dimension varies definably in families: if \( R \subseteq X \times Y \) are interpretable, and \( R_y = \{ x \in X : (x, y) \in R \} \) for \( y \in Y \), then the sets 
\[ Y_k := \{ y \in Y : \dim(R_y) = k \} \]
are interpretable, for each \( k \).

Proof. All the properties are proved analogously to the ones for definable sets, except the last one. Pick some interpretable surjection \( f : \tilde{X} \to X \) with \( \tilde{X} \) definable. First suppose that \( \dim(f^{-1}(x)) \) is a constant \( j \) across all \( x \in X \). Then 
\[ \dim(R_y) = \dim(f^{-1}(R_y)) - j \]
which varies definably in \( y \) by the case of definable sets. If \( \dim(f^{-1}(x)) \) depends on \( x \), we can partition \( x \) into pieces on which \( \dim(f^{-1}(x)) \) is constant and reduce to the constant case.

\[ \square \]

**Proposition 7.13.** Let \( X \) be an interpretable set.

1. \( \dim(X) > 0 \) iff \( X \) is infinite.

2. There is an upper bound on \( n \) such that \( X \) can be partitioned into \( n \) disjoint interpretable subsets \( X_1, \ldots, X_n \) with \( \dim(X_i) = \dim(X) \) for \( 1 \leq i \leq n \).

Proof. Take an interpretable surjection \( f : \tilde{X} \to X \) with \( \tilde{X} \) definable. Partitioning \( X \), we may assume the fibers have constant dimension \( j = \dim(\tilde{X}) - \dim(X) \).

1. If \( \dim(X) = 0 \), every fiber has dimension \( j = \dim(\tilde{X}) \), so there can be at most \( \deg(\tilde{X}) \) fibers, and \( X \) is finite. Conversely, if \( X \) is finite then \( X \) is in interpretable bijection with a finite definable set \( X' \), so \( \dim(X) = \dim(X') = 0 \).

2. Any partition \( X = X_1 \sqcup \cdots \sqcup X_n \) would pull back to a partition \( \tilde{X} = \tilde{X}_1 \sqcup \cdots \sqcup \tilde{X}_n \), and 
\[ \dim(\tilde{X}_i) = \dim(f^{-1}(X_i)) = j + \dim(X_i) = j + \dim(X) = \dim(\tilde{X}). \]
So \( n \) is bounded by \( \deg(\tilde{X}) \).

\[ \square \]

We define the **Morley degree** \( \deg(X) \) to be the maximum \( n \) such that \( X \) can be written as a union of \( n \) disjoint interpretable subsets \( X_1 \sqcup \cdots \sqcup X_n \) with \( \dim(X_i) = \dim(X) \) for each \( i \).

So we have more or less transferred all the facts concerning strongly minimal \( \mathbb{M} \) to its expansion \( \mathbb{M}^{eq} \). We now change terminology: “definable” will always mean “interpretable,” or equivalently, “definable in \( \mathbb{M}^{eq} \).”
**Fact 7.14.** The following are equivalent for a definable set $X$:

- $\dim(X) = 1$ and $\deg(X) = 1$.
- $X$ is infinite, but cannot be written as a disjoint union of two definable sets.

We call such sets strongly minimal sets.

*Proof sketch.* More generally, show that $X$ has Morley rank $>1$ iff $X$ contains $d$ pairwise disjoint infinite definable subsets for arbitrarily high $d$. Reduce to the case where $X \subseteq M^2$ and $\dim(X) = 2$. I guess you can argue this by looking at the complement $M^2 \setminus X$, and using the fact that it has Morley rank 1 and finite Morley degree. \(\square\)

---

**8 Appendix: two lemmas that will help with Zilber’s theorem**

**Lemma 8.1.** Let $G = G^0$ be a definable group. Let $X, Y \subseteq G$ have $\dim(X) = \dim(Y) = \dim(G)$. Then $G = X \cdot Y$, i.e.,

$$G = \{x \cdot y : x \in X \text{ and } y \in Y\}.$$  

*Proof.* Given any $g \in G$, the sets $X$ and $g \cdot Y^{-1}$ are full-rank definable subsets. Because $\deg(G) = |G/G^0| = 1$, these two sets must intersect. Therefore there are $x \in X$ and $y \in Y$ such that

$$x = g \cdot y^{-1},$$

or equivalently $g = x \cdot y$. \(\square\)

If $X,Y$ are two definable sets of dimension $k$ and degree 1, let $X \sim_k Y$ indicate that $\dim(X \cap Y) = k$. This is an equivalence relation.

**Lemma 8.2.** Let $G$ be a definable group. Let $X \subseteq G$ be a definable subset of Morley degree 1.

- The “stabilizer”

$$\{g \in G : \dim(X \cap (g \cdot X)) = \dim(X)\}$$

is a definable subgroup of $G$.

- If the “stabilizer” is $G$, then $\dim(X) = \dim(G)$ and $G = G^0$.

*Proof.* Let $k = \dim(X)$. Let $F_k$ be the collection of definable subsets of $G$ of dimension $k$ and degree 1. As in yesterday’s notes, there is an action of $G$ on $F_k$ that respects the equivalence relation $\sim_k$. Therefore the “stabilizer” is the actual stabilizer of the equivalence class $[X]_{\sim_k}$. So it is a subgroup. It is definable because dimension is definable in families.
Now suppose the stabilizer is all of $G$. Take a small set $C$ defining $G$ and $X$. Take $g \in G$ and $a \in X$ such that $R((a, g)/C) = \dim(G \times X) = \dim(G) + \dim(X)$. As an exercise with the Lascar equality, one can verify that

$$\dim(G) \geq R(g \cdot a/C) \geq R(g \cdot a/a, C) = R(g/a, C) = \dim(G),$$

so $R(g \cdot a/C) = \dim(G)$. Also, $R(g \cdot a/g, C) = R(a/g, C) = \dim(X)$. Now $g \cdot a \in g \cdot X$, and if $g \cdot a \notin X$ then $g \cdot a$ is in the $gC$-definable set $(g \cdot X) \setminus X$, so that

$$R(g \cdot a/g, C) \leq \dim((g \cdot X) \setminus X) < k,$$

because $g \cdot X \sim_k X$, by the assumption on the stabilizer. This is a contradiction, so $g \cdot a \in X$. But $X$ is $C$-definable, so

$$\dim(G) = R(g \cdot a/C) \leq \dim(X).$$

Thus $k = \dim(G)$. Then the cosets of $G^0$ form a class of representatives for $\mathcal{F}_k/\sim_k$, and the action of $G$ on $\mathcal{F}_k/\sim_k$ is the action of $G$ on $G/G^0$. The stabilizer cannot be $G$ unless $G = G^0$.\[\square\]

Lemma 8.3. If $X_1, \ldots, X_d$ are sets of dimension $k$ and degree 1, and if $X_i \not\sim_k X_j$ for $i \neq j$, then the union $\bigcup_{i=1}^d X_i$ has degree at least $d$.

Proof. An exercise in additivity of dimension and degree.\[\square\]

9 Appendix: Zilber indecomposability

Let $G$ be a definable group.

Definition 9.1. A definable set $X \subseteq G$ is indecomposable if for any definable subgroup $H \leq G$, the quotient $X/H$ is infinite or size 1.

Proposition 9.2. If $X \subseteq G$ is definable, then $X$ can be written as a finite union of indecomposable definable sets.

Proof. Suppose not. Then recursively build a sequence $X_0, X_1, X_2, \ldots$ and $G_1, G_2, \ldots$, where

- $X_0$ is $X$.
- $G_{i+1}$ is a definable subgroup such that $X_i/G_{i+1}$ has size strictly between 1 and $\aleph_0$.
- $X_{i+1}$ is one of the equivalence classes that’s not a finite union of indecomposables.

By dcc on definable groups, there must be some $n$ such that

$$G_1 \cap \cdots \cap G_n = G_1 \cap \cdots \cap G_{n+1}.$$

Then any two elements of $X_n$ are congruent modulo $G_{n+1}$, contradicting the choice of $G_{n+1}$.\[\square\]
The decomposition isn’t unique at all. As a consequence, infinite indecomposable sets exist.

**Theorem 9.3** (Zilber). *Let $\mathcal{F}$ be any collection of indecomposable definable sets. Suppose $1 \in X$ for all $X \in \mathcal{F}$. Then the group $H$ generated by $\bigcup \mathcal{F}$ is definable and connected.*

**Proof.** Take $X_1, \ldots, X_n$ maximizing $\dim(Y)$ where $Y = X_1 \cdots X_n$. Let $Z$ be some degree-1 definable subset of $Y$.

**Claim 9.4.** $H \leq \text{Stab}(Z)$, where the stabilizer is as in Lemma 8.2

**Proof.** Otherwise there is some $X_{n+1} \in \mathcal{F}$ such that $X_{n+1} \not\subseteq \text{Stab}(Z)$. Now $\text{Stab}(Z)$ is a definable subgroup, so $X_{n+1}$ intersects infinitely many cosets of $\text{Stab}(Z)$, by indecomposability. Take $a_1, a_2, a_3, \ldots$ in $X_{n+1}$ lying in pairwise distinct cosets of $\text{Stab}(Z)$. Then the translates $Z \cdot a_1, Z \cdot a_2, \ldots$ are basically pairwise disjoint, and all contained in $Z \cdot X_{n+1}$. By choice of $X_1, \ldots, X_n$, we have $\dim(Z \cdot X_{n+1}) = \dim(Z)$. By Lemma 8.3 it follows that $\deg(Z \cdot X_{n+1}) = \infty$, which is impossible. 

In particular $Z \subseteq Y \subseteq \text{Stab}(Z)$. So in the definable group $\text{Stab}(Z)$ there is a set $Z$ that is fully stabilized by the group. By Lemma 8.2 it follows that $\text{Stab}(Z)$ is connected and $\dim(Z) = \dim(\text{Stab}(Z))$. By Lemma 8.1 $Z \cdot Z = \text{Stab}(Z)$. It follows that $\text{Stab}(Z) \leq Z \cdot Z \leq Y \cdot Y \leq H$, so $H = \text{Stab}(Z)$. Thus $H$ is definable and connected. 

---

18