# TUTORIAL NOTES
# INTRODUCTION TO $\omega$-STABLE THEORIES
# UNIVERSITY OF MANCHESTER

INSTRUCTOR: OMAR LEÓN SÁNCHEZ

## 1. Tutorial 1 (Oct 19th)

**Ultraproducts**

**Definition 1.1.** Let $I$ be an infinite set. A filter on $I$ is a set $D \subset \mathcal{P}(I)$ such that

(1) $I \in D$ and $\emptyset \notin D$
(2) if $A$ and $B$ are in $D$, then $A \cap B$ is in $D$
(3) if $A \in D$ and $A \subset B \subseteq I$, then $B \in D$

We usually think of the elements in $D$ are "large" sets of $I$.

*Example* 1.2. Given any (infinite) set $I$ we have

(1) $D_F = \{X \subseteq I : X^c \text{ is finite}\}$ is a filter, called the Frechet filter.
(2) Given $x \in I$, let $D_x = \{X \subseteq I : x \in X\}$. Then $D_x$ is a filter on $I$ , called the principal filter at $x$.

**Definition 1.3.** A filter $D$ on $I$ is called an ultrafilter if $X \in D$ or $X^c \in D$ for all $X \subset I$.

Principal filter are examples of ultrafilters. Examples of nonprincipal ultrafilters are guaranteed by the following result.

**Lemma 1.4.** *Given a filter $D$ of $I$, there is an ultrafilter $\mathcal{U}$ of $I$ extending $D$.*

*Proof.* Let $\mathcal{F} = \{F \subset \mathcal{P}(I) : F \text{ is a filter extending } D\}$. If we order the elements of $\mathcal{F}$ by inclusion and take an increasing chain, it is easy to check that the union of the chain is a filter. Thus, by Zorn's lemma, $\mathcal{F}$ has a maximal element $\mathcal{U}$. We claim that $\mathcal{U}$ is an ultrafilter. Towards a contradiction, assume it is not. Then there is $X \subset I$ such that $X \notin \mathcal{U}$ and $X^c \notin \mathcal{U}$. Let

$$\mathcal{U}' = \{Y \subseteq I : Z \setminus X \subseteq Y \text{ for some } Z \in \mathcal{U}\}$$

Then $\mathcal{U}'$ is a filter that contains $\mathcal{U}$. Moreover, it contains $X^c$, contradicting maximality of $\mathcal{U}$. $\square$

*Remark* 1.5. Given $I$ and $D_F$ the Frechet filter on $I$, if $\mathcal{U}$ is an ultrafilter extending $D_F$ then $\mathcal{U}$ is nonprincipal.

Fix a language $\mathcal{L}$, an infinite set $I$, and an ultrafilter $\mathcal{U}$ on $I$. Suppose $\mathcal{M}_i$ is an $\mathcal{L}$-structure for each $i \in I$. The construction of the "ultraproduct" $\mathcal{L}$-structure

$$\mathcal{M} := \prod_{i \in I} \mathcal{M}_i / \mathcal{U}$$

is given as follows: On the product $\prod_{i\in I} M_i$ define the equivalence relation $f \sim g$ iff $\{i \in I : f(i) = g(i)\} \in \mathcal{U}$. Here $f(i)$ is the $i$-th component of $f$ (or simply think of $f$ as $f : I \to \cup_{i\in I} M_i$ with $f(i) \in M_i$). One can check that $\sim$ is an equivalence relation. The underlying set of the ultraproduct $\mathcal{M}$ is $M := \prod_{i\in I} M_i/\sim$ (thus the elements of the ultraproduct are equivalence classes). Now we give the interpretation of the symbols from $\mathcal{L}$ in $\mathcal{M}$.

(1) For each constant symbol $c \in \mathcal{C}$, we set $c^{\mathcal{M}} = (c^{\mathcal{M}_i})_{i\in I}/\sim$

(2) For each function symbol $(f, n) \in \mathcal{F}$, let $a_1, \ldots, a_n \in \prod M_i/\sim$ and write $a_i = g_i/\sim$ where $g_i \in \prod M_i$, then we set

$$f^{\mathcal{M}}(a_1, \ldots, a_n) = (f^{\mathcal{M}_i}(g_1(i), \ldots, g_n(i)))_{i\in I}/\sim$$

It is an exercise to show that this is well defined (i.e., independent of the choice of $g_i$'s)

(3) For each relation symbols $(R, n) \in \mathcal{R}$, let $a_1, \ldots, a_n \in \prod M_i/\sim$ and write $a_i = g_i/\sim$ where $g_i \in \prod M_i$, then we set

$$(a_1, \ldots, a_n) \in R^{\mathcal{M}} \iff \{i \in I : (g_1(i), \ldots, g_n(i)) \in R^{\mathcal{M}_i}\} \in \mathcal{U}$$

Again, this is independent of the choice of $g_i$'s.

**Theorem 1.6** (Loś's theorem)**.** *Let $\phi(x_1, \ldots, x_n)$ be an $\mathcal{L}$-formula and $a_1, \ldots, a_n \in \prod M_i/\sim$ with $a_i = g_i/\sim$ where $g_i \in \prod M_i$. Then,*

$$\prod_{i\in I} \mathcal{M}_i/\mathcal{U} \models \phi(a_1, \ldots, a_n) \iff \{i \in I : \mathcal{M}_i \models \phi(g_1(i), \ldots, g_n(i))\} \in \mathcal{U}$$

*Proof.* First, one shows that if $t(x_1, \ldots, x_n)$ is an $\mathcal{L}$-term, then

$$t^{\mathcal{M}}(a_1, \ldots, a_n) = (t^{\mathcal{M}_i(g_1(i),\ldots,g_n(i))})_{i\in I}/\sim$$

. This is done by induction on the complexity of the term. The rest of the proof goes via induction on the complexity of the formula. We leave the details to the reader. □

We conclude with a couple of exercises:

(1) Let $\mathcal{U}$ be a principal (ultra)filter on $I$ at $s \in I$. Also, let $\mathcal{M}_i$ be $\mathcal{L}$-structures for $i \in I$. Prove that the ultraproduct $\mathcal{M} := \prod_{i\in I} \mathcal{M}_i/\mathcal{U}$ is isomorphic (as an $\mathcal{L}$-structure) to $\mathcal{M}_s$. (Hint: Define the map $\varphi : \mathcal{M}_s \to \mathcal{M}$ by $a \mapsto (b_i)_{i\in I}/\sim$ where $b_s = a$ and $b_j$ are arbitrarily chosen when $j \neq s$. Prove this map is well defined and that it is an isomorphism of $\mathcal{L}$-structures.)

(2) Fix a ultrafilter $\mathcal{U}$ on $\omega$ (the natural numbers), an $\mathcal{L}$-structure $\mathcal{M}$ and set $\mathcal{M}_i = \mathcal{M}$ for $i \in \omega$. The ultraproduct $\mathcal{M}^* = \prod_{i\in\omega} \mathcal{M}_i/\mathcal{U}$ is called the ultrapower of $\mathcal{M}$ with respect to $\mathcal{U}$. Consider the diagonal map $d : \mathcal{M} \to \mathcal{M}^*$ given by $a \mapsto (a)_{i\in I}/\sim$. Show that $d$ is an elementary $\mathcal{L}$-embedding. Now assume that $\mathcal{U}$ is nonprincipal, show that

$$d \text{ is an isomorphism} \iff \mathcal{M} \text{ is finite}$$

## 2. Tutorial 2 (Ot 26th)

We will do some basic exercises using compactness and ultrapoducts.

**(1)** Suppose $T$ is a complete theory with a finite model of size $n < \omega$. Prove that all models of $T$ has size $n$.

**<u>Solution.</u>** Let $\mathcal{M} \models T$ with $|M| = n$. Now consider the $\mathcal{L}$-sentence $\sigma_n$ saying that there are exactly $n$ many elements, that is

$$\sigma_n : \quad \exists x_1 \dots \exists x_n \wedge_{i<j} (x_i < x_j) \wedge (\forall y \vee_i (y = x_i))$$

Clearly $\mathcal{M} \models \sigma_n$. Thus $T \not\models \neg\sigma_n$, and so, since $T$ is complete, we get $T \models \sigma_n$. Hence, any model of $T$ satisfies $\sigma_n$.

*Remark* 2.1. Note that the above is also an easy consequence of the fact that a theory is complete if and only any two of its models are elementary equivalent (this fact is an easy exercise).

**(2)** Let $T$ be an $\mathcal{L}$-theory. Suppose that for every $n < \omega$ there is $m > n$ such that $T$ has a model of size $m$ (i.e., $T$ has arbitrarily large models). Prove that has an infinite model.

**<u>Solution.</u>** Let $\theta_n$ be the sentence saying that there are at least $n$ many elements. Consider the $\mathcal{L}$-theory $T^* := T \cup \{\theta_n :< \omega\}$. It follows from the assumption that $T^*$ is finitely satisfiable. Thus, by compactness, $T^*$ has a model $\mathcal{M}$. Clearly $\mathcal{M}$ is an infinite model of $T$.

**(3)** (Amalgamation) Suppose $\mathcal{M}_0, \mathcal{M}_1, \mathcal{M}_2$ are $\mathcal{L}$-structures with $\mathcal{M}_0 \preceq \mathcal{M}_i$ for $i = 1, 2$. Prove that there is an $\mathcal{L}$-structure $\mathcal{N}$ and elementary $\mathcal{L}$-embeddings $f_i : \mathcal{M}_i \to \mathcal{N}$ such that $f_1|_{M_0} = f_2|_{M_0}$.

For this exercise we will need ways to construct elementary embeddings. This can generally be done as follows. Let $\mathcal{M}$ be an $\mathcal{L}$-structure. Let $\mathcal{L}_M$ be the new language where we expand $\mathcal{L}$ by adding constant symbols for each element of $\mathcal{M}$, that is

$$\mathcal{L}_M = \mathcal{L} \cup \{c_m : m \in M\}$$

Then $\mathcal{M}$ is naturally an $\mathcal{L}_M$-structure (by setting $c_n^{\mathcal{M}} = m$ for $m \in M$). The diagram of $\mathcal{M}$, $Diag(\mathcal{M})$, is defined as the $\mathcal{L}_M$-theory

$$\{\phi(c_{m_1}, \dots, c_{m_n}) : \phi(x_1, \dots, x_n) \text{ is a q.f. } \mathcal{L}\text{-formula and } \mathcal{M} \models \phi(m_1, \dots, m_n)\}$$

The elementary diagram of $\mathcal{M}$, $Diag_{el}(\mathcal{M})$, is defined as the diagram of $\mathcal{M}$ but where we allow $\phi$ to range over all $\mathcal{L}$-formulas (not necessarily q.f.). Now, if we have an $\mathcal{L}_M$-structure which happens to be a model of $Diag(\mathcal{M})$ then we have an injective map $\alpha : M \to N$ given by $m \mapsto c_m^{\mathcal{N}}$. Moreover, we have the following fact (that we leave as an exercise to the interested reader):

**Fact 2.2.** *If $\mathcal{N} \models Diag(\mathcal{M})$ then the map $\alpha : M \to N$ is an $\mathcal{L}$-embedding. Furthermore, if $\mathcal{N} \models Diag_{el}(\mathcal{M})$ then $\alpha$ is an elementary embedding.*

**<u>Solution to (3).</u>** Let

$$\mathcal{L}^* = \mathcal{L}_{M_0} \cup \{c_m : m \in M \setminus M_0\} \cup \{d_\mu : \mu \in M_2 \setminus M_0\}$$

Also, let

$$T^* = Diag_{el}(\mathcal{M}_1) \cup Diag_{el}(\mathcal{M}_2)$$

By Fact 2.2, it suffices to show that $T^*$ has a model. So, by compactness, it suffices to show that $T^*$ is finitely satisfiable. Let $\Sigma$ be a finite subset of $T^*$. Then $\Sigma = \{\sigma_1, \dots, \sigma_s\} \cup \{\eta_1, \dots, \eta_t\}$ where the $\sigma_i$'s are $\mathcal{L}_{M_1}$-sentences and the $\eta_i$'s are $\mathcal{L}_{M_2}$-sentences. Let $\sigma = \sigma_1 \wedge \cdots \wedge \sigma_s$ and $\eta = \eta_1 \wedge \cdots \wedge \eta_t$. We can write $\sigma$ as $\sigma'(\bar{c}_{\bar{m}})$ where $\sigma'(\bar{x})$ is an $\mathcal{L}_{M_0}$-formula and $\bar{c}_{\bar{m}}$ is a tuple from $\mathcal{L}_{M_1} \setminus \mathcal{L}_{M_0}$. Similarly, we can write $\eta$ as $\eta'(\bar{d}_{\bar{\mu}})$. Since $\mathcal{M}_0 \preceq \mathcal{M}_1$, from the fact that $\mathcal{M}_1 \models \sigma'(\bar{m})$ we get that there is a tuple $\bar{a}$ from $\mathcal{M}_0$ such that $\mathcal{M}_0 \models \sigma'(\bar{a})$. Similarly, from the fact that $\mathcal{M}_0 \preceq \mathcal{M}_2$, we can find a tuple $\bar{b}$ from $\mathcal{M}_0$ such that $\mathcal{M}_0 \models \eta'(\bar{b})$.

Now make the $\mathcal{L}_{M_0}$-structure $\mathcal{M}_0$ into an $\mathcal{L}^*$-structure, call it $\mathcal{M}_0^*$, by interpreting the constants as follows: $\bar{c}_{\bar{m}}$ as $\bar{a}$, $\bar{d}_{\bar{\mu}}$ as $\bar{b}$, and interpret the rest arbitrarily. It is now easy to check that $\mathcal{M}_0^*$ is a model of $\Sigma$. We are done!

*Remark* 2.3. The previous "amalgamation" result does not generally hold if we remove the assumption that $\mathcal{M}_0$ is an **elementary** substructure. In general, an $\mathcal{L}$-theory $T$ is said to have the *amalgamation property* if given any models $\mathcal{M}_0, \mathcal{M}_1, \mathcal{M}_2$ with $\mathcal{M}_0 \subseteq \mathcal{M}_i$, for $i = 1, 2$, there exists $\mathcal{N} \models T$ and $\mathcal{L}$-embeddings $f_i : \mathcal{M}_i \to \mathcal{N}$ such that $f_1|_{M_0} = f_2|_{M_0}$. The theory of fields has the amalgamation property. We leave as an exercise (to the interested reader) to find an example showing that the theory of rings does **not** have the amalgamation property.

**(4)** Recall that the class of torsion-free groups is axiomatized by the theory

$$T_{tf} = GROUPS \cup \{\sigma_n : n < \omega\}$$

where $\sigma$ is the sentence saying that every nontrivial element does not have order $n$. Prove that this class of groups does not have a finite axiomatization.

**Solution.** Towards a contradiction suppose there is such an axiomatization. By taking conjunctions, we may assume it is given by a single sentence $\sigma$. Then $T_{tf} \models \sigma$ and so, by compactness, there must a finite $\Sigma \subset T_{tf}$ such that $\Sigma \models \sigma$. There is $N < \omega$ such that $\Sigma \subseteq GROUPS \cup \{\sigma_n : n \leq N\}$. Now consider the structure $\mathcal{G} = (\mathbb{Z}/(p), +)$ where $p$ is a prime larger than $N$. Then $\mathcal{G} \models \Sigma$. However, $\mathcal{G} \not\models \sigma$ which contradicts the fact that $\Sigma \models \sigma$.

**(5)** Recall that a group is said to be a torsion group if each element has torsion (i.e., finite order). Prove that the class of torsion groups is not elementary.

**Solution.** Towards a contradiction suppose it is, say by $T$. Let

$$G_n = (\mathbb{Z}/(n+2), +)$$

for $n \in \omega$. Let $\mathcal{U}$ be a nonprincipal ultrafilter of $\omega$. Consider the ultraproduct

$$G = \prod_{n<\omega} G_n/\mathcal{U}$$

By Loś's theorem, $G \models T$. However, the element $\alpha = (1, 1, \dots)/\sim \in G$ has no torsion. Indeed, if it did there would be $N < \omega$ such that $\alpha^N = (0, 0, \dots)/\sim$. That is,

$$\{n < \omega : N \equiv 0 \bmod n+2\} \in \mathcal{U}.$$

But since $\mathcal{U}$ is nonprincipal all of its elements are infinite. So the above set would be infinite, this is clearly impossible (its size is at most $N$).

We finish with some additional exercises (which we leave to the reader):

(1) Prove that the theory $ACF$ (algebraically closed fields) is not finitely axiomatizable.
(2) Prove that the class of finite fields is not elementary.

## 3. Tutorial 3 (Nov 9th)

**Real closed fields.** The goal is to give an idea of why the theory $RCF$ in the language $\mathcal{L}_{ord}$ (of ordered rings) has quantifier elimination.

**Definition 3.1.** An ordered field $(K, <)$ is a field equipped with a linear order such that for all $a, b, c \in K$ we have

$$a < b \implies a + c < b + c$$

and

$$a < b \text{ and } c > 0 \implies ac < bc$$

*Example* 3.2. $\mathbb{R}$ and $\mathbb{Q}$ are ordered fields. Moreover, there is a unique way to order them. On the other hand, $\mathbb{Q}[t]$ is also orderable but this has many orders (uncountably many).

*Remark* 3.3. Let $K$ be an ordered field. It can easily be seen that $K$ must have characteristic zero. Also, note that for nonzero $a \in K$ we have $a^2 > 0$ (since $a^2 = aa = (-a)(-a)$). Also, $-1 < 0$. This yields that $-1$ is not a sum of squares.

**Definition 3.4.**

(1) A field $K$ is (formally) real if $-1$ is not a sum of squares.
(2) A real field $K$ is real closed if it has no formally real algebraic extensions.

The above remark shows that any ordered field is real. Turns out that the converse is also true, but this requires some work.

The following theorem is the key to the axiomatization of $RCF$.

**Theorem 3.5.** *Let $K$ be a real field. TFAE*

(1) *$K$ is real closed*
(2) *$K(i)$ is algebraically closed (where $i^2 = -1$)*
(3) *for $a \in K$ either $a$ or $-a$ is a square, and every polynomial over $K$ in one variable of odd degree has a root in $K$*

As a consequence of (3) in the theorem we get:

**Corollary 3.6.** *In the language of rings, $\mathcal{L}_{rings}$, the class of real closed fields is axiomatizable.*

One can not get q.e. in the language of rings (if it had q.e. the positive elements would either be finite or cofinite). But it turns out that the order $<$ is all we need to add to the language to get q.e. So, we now work in the language $\mathcal{L}_{ord}$. We let $RCF$ be the theory of ordered fields together with the axioms for real closed fields (i.e., (2) from the above theorem).

Note that in a model of $RCF$ the order is unique; indeed, the positive elements are the squares. We also have the following "intermediate value theorem":

**Corollary 3.7.** *Let $K \models RCF$. Then for any $p \in K[x]$ and $a < b$ with $p(a)p(b) < 0$, there is $a < c < b$ such that $p(c) = 0$.*

*Proof.* Since $F(i)$ is algebraically closed, $p$ factors over $K$ into linear and quadratic irreducible polynomials. One of the linear factors must change sign between $a$ and $b$. Thus this linear factor must have a root in between. ☐

A *real closure* of a real field $K$ is a real closed algebraic extension of $K$. Real closures are not generally isomorphic. However, if $K$ is ordered and $K_1$ and $K_2$ are real closures of $K$ such that their unique orderings extend that of $K$, then they are isomorphic over $K$. Now the question is: can we find a real closure extending the order?

**Proposition 3.8.** *Suppose $K$ is an ordered field. Then $K$ has a real closure that extends its ordering. Moreover, if $L$ is a real closed field extension of $K$ extending the ordering, then there is a real closure of $K$ in $L$.*

**Theorem 3.9.** *$RCF$ has q.e.*

*Proof.* We use the criterion for q.e. that we discussed in lectures. So, let $K, L \models RCF$ with a common substructure $R$, $\phi(\bar{x}, y)$ a quantifier free $\mathcal{L}_{ord}$-formula, $\bar{a}$ from $R$ and $b \in K$ such that $K \models \phi(\bar{a}, b)$. We must find $c \in L$ such that $L \models \phi(\bar{a}, c)$. Note that $R$ is an integral domain, then $Frac(R)$ is an ordered field, by Proposition 3.8 it has a real closure in $K$ and a real closure in $L$. Since these real closures are isomorphic (over $Frac(R)$), we may assume that $K$ and $L$ contain a common real closure $F$ of $Frac(R)$. Thus, it suffices to find the desired $c$ in $F$. Since $\phi$ is q.f., we may assume that it has the form

$$\wedge_i(p_i = 0) \wedge \wedge_j(q_j > 0)$$

for $p_i$ and $q_j$ polynomials in one variable over $F$. If one of the $p_i$'s is not zero, then $b$ is algebraic over $F$ and hence in $F$. Thus we may assume that $\phi$ is of the form $\wedge_j(q_j > 0)$. As in the proof of Corollary 3.7, each $q_i$ factors over $F$ into irreducible linear and quadratic terms. Thus, from the linear terms and the fact that $q_i(b) > 0$ for all $i$, we can find two lists $d_1, \dots, d_n$ and $e_1, \dots, e_n$ of elements from $F$ with $\max_i(d_i) < \max_i(e_i)$ such that for all $d_i < u < e_i$ we have $q_i(u) > 0$. Letting $c = \frac{d+e}{2} \in F$, where $d = \max_i(d_i)$ and $e = \max_i(e_i)$, we get $q_i(c) > 0$ for all $i$ as desired. □

Let $\mathcal{L}$ be a language containing $<$ (i.e., a binary relation symbol). We recall that an $\mathcal{L}$-structure $\mathcal{M}$ is *o-minimal* if every definable subset of $M$ is a finite union of intervals (equivalently, definable using only $<$) . A consequence of q.e. for $RCF$ is that every model if $RCF$ is *o*-minimal.

## 4. Tutorial 4 (Nov 16th)

**Elimination of imaginaries.** Let $\mathcal{M}$ be an $\mathcal{L}$-structure. Suppose $E$ is an equivalence relation on $M^n$. We say that $E$ is a definable equivalence relation if the set $E \subseteq M^n \times M^n$ is definable. We can consider the quotient space

$$M^n/E = \{\bar{a}/E : \bar{a} \in M^n\}.$$

Can we view this as a "definable set"? For instance, can we find a definable set of representatives? That is, can we find a definable set $X \subseteq M^n$ such that $X$ is a set of representatives for $M^n/E$? This turns out to be true in any model of $RCF$ (using Skolem functions). However, it is not true in $ACF_0$. For example, the relation on $K \models ACF_0$ given by $xEy$ iff $x^2 = y^2$ cannot a have a definable set of representatives (since such set would a infinite and coinfinite definable set, but this is impossible by strong minimality of $ACF_0$).

The next best thing that one could ask for (to somehow view $M^n/E$ as a definable set) is to ask about the existence of a definable function $f : M^n \to M^m$, for some $m$, such that $f(\bar{x}) = f(\bar{y})$ iff $\bar{x}E\bar{y}$. Note that if this is the case we can identify $M^n/E$ with the definable set $f(Y)$ as these two set are in "definable" bijection $\bar{a}/E \mapsto f(\bar{a})$.

We will see that the existence of such functions is guaranteed in the theories $ACF_0$ and $DCF_0$. Before doing so, we need some preliminary results.

**Definition 4.1.** Let $\kappa$ be an infinite cardinal and $\mathcal{M}$ an $\mathcal{L}$-structure.

(1) $\mathcal{M}$ is said to be $\kappa$-strongly homogeneous if for every $A \subseteq M$ with $|A| < \kappa$ and $f : A \to M$ a pem, there is an extension of $f$ to an automorphism of $\mathcal{M}$.
(2) $\mathcal{M}$ is said to be $\kappa$-saturated if for every $A \subseteq M$ with $|A| < \kappa$ all types over $A$ (with respect to the complete theory $Th_A(\mathcal{M})$) are realized in $\mathcal{M}$.

It turns out that a theory always has a $\kappa$-strongly homogeneous and $\kappa$-saturated model for any $\kappa$. The following is easy to check:

**Fact 4.2.** *Suppose $\mathcal{M}$ is $\kappa$-strongly homogeneous and $\kappa$-saturated.*

(1) *Let $\bar{a}, \bar{b}$ be $n$-tuples from $M$ and $A \subseteq M$ with $|A| < \kappa$. If $tp^{\mathcal{M}}(\bar{a}/A) = tp^{\mathcal{M}}(\bar{b}/A)$ then there is an automorphism $\sigma$ of $\mathcal{M}$ fixing $A$ such that $\sigma(a) = b$.*
(2) *Suppose $A \subseteq M$ with $|A| < \kappa$. Then, $a \in dcl(A)$ iff for all $\sigma \in Aut(\mathcal{M}/A)$ we have $\sigma(a) = a$.*

**Proposition 4.3.** *Suppose $\mathcal{M}$ is $\kappa$-strongly homogeneous and $\kappa$-saturated. Let $A \subseteq M$ with $|A| < \kappa$. A definable set $X \subseteq M^n$ is $A$-definable iff for all $\sigma \in Aut(\mathcal{M}/A)$ we have $\sigma(X) = X$.*

*Proof.* We have seen in lectures that $(\Rightarrow)$. Let us show $(\Leftarrow)$. Let $X = \phi^{\mathcal{M}}(\bar{x}, \bar{b})$. Consider

$$\Gamma = \{\psi(\bar{x}) : \psi(\bar{x}) \text{ is an } \mathcal{L}_A\text{-formula and } \mathcal{M} \models \forall \bar{x}\ \phi(\bar{x}, \bar{b}) \to \psi(\bar{x})\}$$

We claim that $Th_A(\mathcal{M}) \cup \Gamma \models \phi(\bar{x}, \bar{b})$. If not, by $\kappa$-saturation, we can find $\bar{c}$ in $M$ realizing $\Gamma$ but not $\phi(\bar{x}, \bar{b})$. Now, by strong homogeneity, for every $\bar{c}'$ in $M$ with $tp^{\mathcal{M}}(\bar{c}/A) = tp^{\mathcal{M}}(\bar{c}'/A)$ there is $\sigma \in Aut(\mathcal{M}/A)$ such that $\sigma(\bar{c}) = \bar{c}'$. By our assumption, $\sigma(X) = X$, so $\bar{c}'$ cannot be in $X$. In other words, $tp^{\mathcal{M}}(\bar{c}/A) \models \neg\phi(\bar{x}, \bar{b})$. Thus, we can find an $\mathcal{L}_A$-formula $\theta$ from $tp^{\mathcal{M}}(\bar{c}/A)$ such that

$$\mathcal{M} \models \forall \bar{x}\; \theta(\bar{x}) \rightarrow \neg\phi(\bar{x}, \bar{b}).$$

It follows that $\neg\theta \in \Gamma$ but this is impossible since $\mathcal{M} \models \theta(\bar{c})$. We have thus shown that $Th_A(\mathcal{M}) \cup \Gamma \models \phi(\bar{x}, \bar{b})$. By compactness, there is a formula $\psi \in \Gamma$ such that

$$\mathcal{M} \models \forall \bar{x}\, \psi(\bar{x}) \rightarrow \phi(\bar{x}, \bar{b}).$$

It follows that $X = \phi^{\mathcal{M}}(\bar{x}, \bar{b}) = \psi^{\mathcal{M}}(\bar{x})$ as desired (since $\psi$ is an $\mathcal{L}_A$-formula). $\square$

## 5. Tutorial 5 (Nov 23rd)

We fix $\mathcal{M}$ a $\kappa$-saturated and $\kappa$-strongly homogeneous $\mathcal{L}$-structure for large $\kappa$. Also, $B$ will be a subset of $M$ with $|B| < \kappa$.

Recall that last time we proved that given a definable set $X$, we have that $X$ is $B$-definable iff all $\sigma \in Aut(\mathcal{M})$ fixes $X$ setwise. We can now ask, given a definable $X$ is there a *smallest* $dcl$-closed $B$ over which $X$ is defined. Here $dcl$-closed means $B = dcl(B)$ and by "smallest" we mean that if $X$ is $A$-definable then $B \subseteq dcl(A)$. This motivates the following definition:

**Definition 5.1.** Let $p$ be a (possibly incomplete) type over $A \subset M$. We say that $B$ is a canonical base for $p$ if $B$ is $dcl$-closed and for each $\sigma \in Aut(\mathcal{M})$ we have

$$\sigma(p^{\mathcal{M}}) = p^{\mathcal{M}} \text{ setwise} \iff \sigma(B) = B \text{ pointwise}$$

Recall that $p^{\mathcal{M}}$ denotes the set of realization of $p$ in $\mathcal{M}$. Note that $p$ could be a single formula, and so we can talk about the canonical base of a formula (in fact we will mostly focus on this case).

*Remark* 5.2. Let $X$ be a definable set with canonical base $B$. Note that $B$ is the smallest $dcl$-closed set over which $X$ is defined. Indeed, if $X$ is $A$-definable, then any $\sigma \in Aut(\mathcal{M}/A)$ fixes $X$ pointwise and thus fixes $B$ setwise; by saturation $B \subseteq dcl(A)$. This also shows that canonical basis are unique (if they exist). We also have that $B$ is of the form $dcl(\bar{b})$ for finite tuple $\bar{b}$ (we'll see this in Lemma 5.3 below). Finally, if $X$ is $A$-definable and also $C$-definable, then it is $dcl(A) \cap dcl(C)$-definable.

**Lemma 5.3.** *Let $X$ be definable. Then, $B$ is a canonical base for $X$ iff there is a formula $\psi(\bar{x}, \bar{y})$ and $\bar{b}$ from $B$ such that $X = \psi^{\mathcal{M}}(\bar{x}, \bar{b})$ and for all $\bar{c}$ from $M$ with $\bar{c} \neq \bar{b}$ we have $X \neq \phi^{\mathcal{M}}(\bar{x}, \bar{c})$. In this case, $B = dcl(\bar{b})$.*

*Proof.* By Proposition 4.3, $X$ is $B$-definable. Say $X = \phi^{\mathcal{M}}(\bar{x}, \bar{b})$ for some $\bar{b} \in B$. We claim that

$$tp(\bar{b}) \models (\bar{y} \neq \bar{b}) \to (\forall \bar{x}\, \phi(\bar{x}, \bar{y}) \not\leftrightarrow \phi(\bar{x}, \bar{b})) \tag{5.1}$$

If not, by saturation, there is $\bar{b}'$ from $M$ with $tp(\bar{b}') = tp(\bar{b})$, $\bar{b}' \neq \bar{b}$, and $\phi^{\mathcal{M}}(\bar{x}, \bar{b}') = \phi^{\mathcal{M}}(\bar{x}, \bar{b})$. But then, by homogeneity, there is $\sigma \in Aut(\mathcal{M})$ with $\sigma(\bar{b}) = \bar{b}'$, so that $\sigma$ does not fix $B$ pointwise, and so (by definition of canonical base) $\sigma$ does not fix $X$ setwise, that is $\phi^{\mathcal{M}}(\bar{x}, \sigma(\bar{b})) = \phi^{\mathcal{M}}(\bar{x}, \bar{b})$, a contradiction. Thus (5.1) holds, and so, by compactness, there is $\theta(\bar{y}) \in tp(\bar{b})$ such that

$$\theta(\bar{y}) \models (\bar{y} \neq \bar{b}) \to (\forall \bar{x}\, \phi(\bar{x}, \bar{y}) \not\leftrightarrow \phi(\bar{x}, \bar{b}))$$

The desired formula is $\psi(\bar{x}, \bar{y}) = \phi(\bar{x}, \bar{y}) \wedge \theta(\bar{y})$.

For the converse, let $\sigma \in Aut(\mathcal{M})$ then $\sigma(X) = X$ iff $\psi^{\mathcal{M}}(\bar{x}, \sigma(\bar{b})) = \psi^{\mathcal{M}}(\bar{x}, \sigma(\bar{b}))$ iff $\sigma(\bar{b}) = \bar{b}$. Hence, $dcl(\bar{b})$ will be a canonical base for $X$. $\square$

Do canonical basis always exist? Not generally. This motivate the following

**Definition 5.4.** A theory $T$ eliminates imaginaries if every definable set has a canonical base.

**Lemma 5.5.** *Suppose $T$ eliminates imaginaries and that the language has at least two constant symbols (call them 0 and 1). If $X \subseteq M^n$ is a $A$-definable set and $E$ is an $A$-definable equivalence relation on $X$, then there is an $A$-definable function $f : X \to M^m$, for some $m$, such that $xEy$ iff $f(x) = f(y)$.*

*Proof.* By Lemma 5.3, for each formula $\phi(\bar{x},\bar{y})$ and tuple $\bar{a}$ there is a formula $\psi_{\bar{a}}(\bar{x},\bar{y})$ and a unique $\bar{b}$ such that $\phi^{\mathcal{M}}(\bar{x},\bar{a})=\psi^{\mathcal{M}}(\bar{x},\bar{b})$. By a standard compactness argument, there are formulas $\psi_0(\bar{x},\bar{y}),\dots,\psi_s(\bar{x},\bar{y})$ such that for a given $\bar{a}$ there is $i$ and unique $\bar{b}$ such that $\phi^{\mathcal{M}}(\bar{x},\bar{a})=\psi_i^{\mathcal{M}}(\bar{x},\bar{b})$. By a standard coding trick we can reduce to a single $\psi$ (the fact that our language has two constant symbols guarantees that this $\psi$ has not additional parameters). For instance, let me demonstrate the coding trick in the case $s=2$; i.e., we have only $\psi_0,\psi_1$. We set $\psi(\bar{x},\bar{y},z)$ to be

$$((\psi_0(\bar{x},\bar{y})\wedge(z=0))\vee(\psi_1(\bar{x},\bar{y})\wedge(z=1)))\wedge((\exists_{\text{unique}}\bar{v}\forall\bar{w}\ \phi_0(\bar{w},\bar{v})\leftrightarrow\psi_1(\bar{w},\bar{y}))\leftrightarrow(z=0))$$

This formula does the job since, given $\bar{a}$, if $\exists_{\text{unique}}\bar{b}$ such that $\phi^{\mathcal{M}}(\bar{x},\bar{a})=\psi_0^{\mathcal{M}}(\bar{x},\bar{b})$ then $(\bar{b},0)$ is the unique such that $\phi^{\mathcal{M}}(\bar{x},\bar{a})=\psi^{\mathcal{M}}(\bar{x},\bar{b},0)$; otherwise, $(\bar{b},1)$ is the unique such that $\phi^{\mathcal{M}}(\bar{x},\bar{a})=\psi^{\mathcal{M}}(\bar{x},\bar{b},1)$. A similar idea works for more than than two $\psi_i$'s.

We have shown that for any $\phi(\bar{x},\bar{y})$ there is $\psi(\bar{x},\bar{y})$ such that for any $\bar{a}$ there is unique $\bar{b}$ with $\phi^{\mathcal{M}}(\bar{x},\bar{a})=\psi^{\mathcal{M}}(\bar{x},\bar{b})$. If $\phi$ is the formula defining our equivalence relation $E$, then the function $f$ is given by $\bar{a}\mapsto\bar{b}$. To finish let us check that $\bar{a}E\bar{c}$ iff $f(\bar{a})=f(\bar{c})$. Indeed, if $\bar{a}E\bar{c}$ then

$$\phi^{\mathcal{M}}(\bar{x},\bar{c})=c/E=a/E=\phi\mathcal{M}(\bar{x},\bar{a})=\psi(\bar{x},\bar{b}),$$

and so $f(\bar{c})=\bar{b}$, as desired. □

*Remark* 5.6. The converse of the lemma is also true. More precisely, if in $\mathcal{M}\models T$ for every a definable equivalence relation $E$ on $M^n$ there is a definable $f:M^n\to M^m$ such that $xEy$ iff $f(x)=f(y)$, then $T$ eliminates imaginaries. Indeed, let $X$ be a definable set given by $\phi(x,a)$, consider the definable equivalence relation on $M^n$ given by $yEz$ iff $\forall x\phi(x,y)\leftrightarrow\phi(x,z)$. Then, there is a definable $f:M^n\to M^m$ such that $yEz$ iff $f(y)=f(z)$. Consider the formula $\psi(x,y)$ given by

$$\exists w\ \phi(x,w)\wedge(f(w)=y)$$

Then $b:=f(a)$ is the unique tuple such that $X=\psi^{\mathcal{M}}(x,b)$. By Lemma 5.3, $dcl(b)$ is a canonical base for $X$, and so $T$ eliminates imaginaries.

**Theorem 5.7.** *The theories $ACF_0$ and $DCF_0$ eliminate imaginaries.*

*Sketch of the proof.*

<u>$ACF_0$</u>: We use minimal fields of definition from algebraic geometry. That is, given a Zariski-closed set $V\subseteq K^n$ with $K\models ACF_0$ sufficiently saturated, it is an algebraic fact that there is $k<K$ such that for any $\sigma\in Aut(K)$ fixes $V$ setwise iff it fixes $k$ pointwise. I will only consider the case of a definable set $X$ of the form $V\setminus W$ where $V$ is irreducible and $W\subseteq V$ (the general case follows from this using quantifier elimination). Let $k_V$ be the minimal field of definition of $V$ and $k_W$ that of $W$. We claim that $k=\langle k_V,k_W\rangle$ (the compositum of $k_V$ and $k_W$ in $K$) is a canonical base for $X$. It is $dcl$-closed since it is a field. Now let $\sigma\in Aut(K)$. If $\sigma$ fixes $X$ setwise, then it fixes a dense open set of $V$ (denseness comes from irreducibility of $V$). But the image $\sigma(V)$ is another irreducible Zariski closed set and so, since $V$ and $\sigma(V)$ are Zariski-closed whose intersection is dense in both, we have $V=\sigma(V)$ (setwise). It follows from this that $\sigma$ also fixes $W$ setwise. Hence, $\sigma$ fixes $k_V$ and $k_W$ pointwise. Consequently, $\sigma$ fixes $k$ pointwise. On the other hand, suppose $\sigma$ fixes $k$ pointwise, then it fixes $k_V$ and $k_W$ pointwise, and so it fixes $V$ and $W$ pointwise; and hence also $X$, as desired.

$\underline{DCF_0}$: In differential-alegebraic we also have minimal differential field of definitions for Kolchin-closed sets. The proof in this case is analogous to the $ACF_0$ case. □

## 6. Tutorial 6 (Nov 30th)

A $\omega$-stable group is a structure $G$ in a language expanding the language of groups such that $(G, e, \cdot)$ is a group and $Th(G)$ is $\omega$-stable.

Let us recall the notion of interpretability. We say that an $\mathcal{L}'$-structure $\mathcal{N}$ is interpretable in an $\mathcal{L}$-structure $\mathcal{M}$ is there is a definable $X \subseteq M^n$, a definable equivalence relation $E$ on $X$, and for each symbol in $\mathcal{L}'$ we can find an $E$-invariant set on some $X^m$ (where by definable we mean with respect to $\mathcal{L}$) such that $X/E$ with the induced $\mathcal{L}'$-structure is isomorphic to $\mathcal{N}$.

**Fact 6.1.** *Let $\mathcal{M}$ be a structure with a $\omega$-stable theory. If a group $G$ is interpretable in $\mathcal{M}$, then $G$ is $\omega$-stable.*

For example, any definable group in an algebraically closed (or differentially closed) field $K$ is $\omega$-stable. In particular, algebraic groups over $K$ are $\omega$-stable; in fact, such groups have finite Morley rank. The following conjecture is one of the main open problems in the subject of $\omega$-stable groups.

**Conjecture 6.2** (Cherlin-Zilber conjecture)**.** If $G$ is an infinite simple group of finite Morley rank, then $G$ interprets an algebraically closed field $K$ and $G$ is definably isomorphic to a simple algebraic group over $K$.

**Theorem 6.3.** *If $G$ is a $\omega$-stable group then there is no infinite descending chain of definable subgroups.*

*Proof.* Note that for any $H \leq G$ the translates of $H$ in $G$ have the same Morley rank as $H$. Hence, if $[G : H]$ is infinite we get $RM(H) < RM(G)$; otherwise, $RM(G) = RM(H)$ and $\deg G = [G : H] \deg H$. Now, let $\alpha = RM(G)$. Suppose we have an infinite descending chain $G > G_1 > G_2 > \cdots$. Let $s_i = (RM(G_i), \deg G_i)$. Then, by the comments above, the $s_i$'s are infinite descending sequence of $(\alpha+1)\times\omega$ with respect to lexicographic order. But this is impossible as the latter is well ordered. $\square$

## 7. Tutorial 7 (Dec 7th)

Let $G$ be a $\omega$-stable group. We have the following easy corollary of Theorem 6.3 above.

**Corollary 7.1.** *If $(H_i)_{i\in I}$ is a collection of definable subgroups of $G$, then there is a finite subcollection $H_{i_1}, \dots, H_{i_s}$ such that*

$$\bigcap_{i\in I} H_i = H_{i_1} \cap \cdots \cap H_{i_s}$$

We also get the following

**Proposition 7.2.** *$G$ has a smallest definable subgroup of finite index, call it $G_0$. Moreover, $G_0$ is 0-definable and normal in $G$*

We call the above $G_0$ the connected component of $G$, and we say that $G$ is connected if $G = G_0$.

*Proof.* Let

$$\mathcal{H} = \{H \leq G : H \text{ is a definable subgroup of finite index}\}$$

By Corollary 7.1, there are $H_{i_1}, \dots, H_{i_s} \in \mathcal{H}$ such that

$$\bigcap \mathcal{H} = H_{i_1} \cap \cdots \cap H_{i_s}$$

Let $G_0 = H_{i_1} \cap \cdots \cap H_{i_s}$. Clearly, $G_0$ is definable and of finite of index, and it is the smallest such. We now argue why it is 0-definable. Let $n = [G : G_0]$. Note that if $H \neq G_0$ is a definable subgroup of index $\leq n$, then $H \cap G_0$ would be a definable proper subgroup of $G_0$ of finite index, which is impossible. Thus, $G_0$ is the only definable subgroup of index $\leq n$. Now, let $\phi(x, b)$ be an $\mathcal{L}$-formula defining $G_0$. Consider the 0-definable set

$$W = \{c \in G : \phi(x, c) \text{ defines a subgroup of index} \leq n\}$$

Then the $\mathcal{L}$-formula $\exists y\, \phi(x, y) \wedge (y \in W)$ defines $G_0$. Finally, to see that $G_0$ is normal in $G$, note that for any definable group automorphism $\sigma$ of $G$ we have that $\sigma(G_0)$ is a definable subgroup of index $n$. But we have seen that then $\sigma(G_0) = G_0$. Hence, for any $g \in G$ we get $gG_0g^{-1} = G_0$, showing that $G_0 \trianglelefteq G$. □

Let $\mathcal{U}$ be a sufficiently saturated elementary of $G$. We say that a type $p \in S_1(G)$ is *generic* if $RM(p) = RM(G)$. We say that $g \in \mathcal{U}$ is *generic over* $G$ if $RM(g/G) = RM(G)$.

We have the following:

**Fact 7.3.**

(1) *Let $g$ be generic over $G$ and $h \in G$. Then $hg$ and $g^{-1}$ are generic over $G$.*
(2) *$G$ has a unique generic type iff it is connected.*

*Proof.* We prove (1). Suppose $hg$ is not generic over $G$. Then there is some definable set $X$ containing $hg$ such that $RM(X) < RM(G)$. Consider the map $f : X \to \mathcal{U}$ given by $x \mapsto h^{-1}x$. Then $f$ is a definable injective map whose image contains $g$, and so, since $RM(f(X)) = RM(X)$, we get $RM(g/G)$ contradicting genericity of $g$. To show that $g^{-1}$ is generic over $G$, we argue as before but now using the map $x \mapsto x^{-1}$. □

We now aim to prove Macintyre's theorem (in characteristic zero) that any infinite $\omega$-stable field is algebraically closed. We will use the following result from Galois theory:

**Fact 7.4.** *Let $p \in \mathbb{N}$ be a prime. If $L/K$ is a Galois extension of degree $p$ and $K$ contains all $p$-th roots of unity, then the minimal polynomial of $L/K$ is of the form $x^p - a$ for some $a \in K$.*

**Theorem 7.5** (Macintyre's theorem)**.** *If $K$ is an infinite $\omega$-stable field, then it is algebraically closed.*

*Proof.* We prove the case when $char(K) = 0$. The positive characteristic case requires a bit more work.

First, note that for every $a \in K^*$ the map $x \mapsto ax$ is a definable group automorphism of $(K, 0, +)$, then $aK_0 = K_0$ where $K_0$ is the connected component of $(K, 0, +)$. This implies that $K_0$ is an ideal of $K$, and so, since $K$ is an infinite field, we must have $K_0 = K$. By Fact 7.3(2), $K$ has a unique generic type, and so the multiplicative group $(K^*, 1, *)$ also has a unique generic type and hence it is connected. Now, for every positive integer $n$, the map $\bar{x} \mapsto x^n$ has finite fibres and so the image of this map (which is $K^n$) has the same Morley rank as $K$. So $K^n \setminus \{0\}$ is a definable subgroup of the multiplicative group of $K$ of the same Morley rank. Since the latter is connected, we get $K = K^n$, and so every element of $K$ has an $n$-th root for all $n > 0$.

We now prove that $K$ has no proper Galois extensions (since $char(K) = 0$ this will imply that $K$ is algebraically closed, in fact this is true for any perfect field). Suppose this not the case. Let $n > 0$ be minimal such that there is an infinite $\omega$-stable field $K$ with a Galois extension $L$ of degree $n$. Let us argue that $n$ must be prime. There is prime $p$ such that the group $Aut(L/K)$ has a subgroup of order $p$, but then, by the Galois correspondence, there is an intermediate field $K < F < L$ such that $L/F$ has degree $p$. Since $F$ is a finite extension of $K$, it is interpretable in $K$, and so also $\omega$-stable. By the choice of $n$, we must have $n = p$.

Now, to apply Fact 7.4, we must argue that $K$ contains all $p$-th roots of unity. But this is easy: the splitting field of $x^p - 1$ is a Galois extension of $K$ of degree $\leq p - 1$. By choice of $p$, this extension must be trivial, and so $K$ contains all $p$-th roots of unity. So, by Fact 7.4, the minimal polynomial of $L/K$ is of the form $x^p - a$. But this is impossible since above we argued that every element of $K$ has a $p$-th root, and so this polynomial would not be irreducible. This is the desired contradiction, and so $K$ has no proper Galois extensions. □

**Corollary 7.6.** *If $K$ is an infinite field with with quantifier elimination, then it is algebraically closed.*

*Proof.* We may assume that $K$ is sufficiently saturated. Note that, since $K$ has q.e., it is strongly minimal. We now argue that if $F \preceq K$ is countable then $S_1(F)$ is countable. To see this it suffices to show that any two $a, b \in K$ that are not in $F^{alg}$ have the same type over $F$. If their types were different there would be a formula $\phi(x)$ (over $F$) such that $K \models \phi(a) \wedge \neg\phi(b)$. But then $\phi^K$ is an infinite definable set (otherwise $a$ would in $F^{alg}$) and it is also coinfinite (otherwise $b$ would be in $F^{alg}$). This would contradict strong minimality of $K$. Thus, indeed, $tp(a/F) = tp(b/F)$.

I leave as an exercise to show that if $S_1(F)$ is countable for all countable $F$, then $S_n(F)$ is also countable for all $n$ (do induction on $n$). This, of course, now implies that $K$ is $\omega$-stable, and so, by Macintyre's theorem, it is algebraically closed. □