INTRODUCTION TO MODEL THEORY WITH APPLICATIONS

RONNIE NAGLOO

5. Model Theory of fields I

In this lecture we take a close look at the model theory of algebraically closed fields. We show how the various tools and concepts we have developed in the first four lectures applies in this setting. This will be the first lecture devoted to looking at some model theory of fields. In Lecture 6, we will study the theory the ordered field of real numbers.

5.1. **Algebraically closed fields.** We work in the language of rings $\mathcal{L}_r = \{+, -, \times, 0, 1\}$ where $+, \times$ are binary function symbols, $-$ is a unary function symbol and $0, 1$ are constants symbols. We focus on ACF, the theory of algebraically closed fields, which is axiomatized by the following $\mathcal{L}_r$-sentences:

- $\neg(0 = 1)$
- $\forall x \forall y\, (x + y = y + x)$
- $\forall x\, (0 + x = x)$
- $\forall x\, (x + -x = 0)$
- $\forall x \forall z \forall y\, \left((x + y) + z = x + (y + z)\right)$
- $\forall x \forall y\, (x \times y = y \times x)$
- $\forall x\, (1 \times x = x)$
- $\forall x \forall z \forall y\, \left((x \times y) \times z = x \times (y \times z)\right)$
- $\forall x \forall z \forall y\, \left(x \times (y + z) = (x \times y) + (x \times z)\right)$
- $\forall x\, (x = 0 \vee \exists y\, (x \times y = 1))$
- For each degree $d \in \mathbb{N}_{d>0}$, the sentence

$$\forall a_0 \ldots \forall a_{d-1} \exists x\, (a_0 + a_1 x + \ldots + a_{d-1} x^{d-1} + x^d = 0)$$

It is not hard to see that ACF is not complete. Indeed, for each prime number p, let ϕ_p be the sentence $\phi_p := (\underbrace{1 + \ldots + 1} = 0)$. Then ϕ_p is true in some models of ACF while $\neg\phi_p$ is true in others. Let

$$ACF_p = \begin{cases} ACF \cup \{\phi_p\} & \text{if } p \text{ is prime} \\ \\ ACF \cup \{\neg\phi_p : p \text{ prime}\} & \text{if } p = 0 \end{cases}$$

It follows that for each p prime or 0 the theory ACF_p is a completion of ACF.

Theorem 5.1. *ACF_p is κ-categorical for every uncountable cardinal κ. Hence ACF_p is complete.*

Proof. We will use the fact that two algebraically closed fields of characteristic p are isomorphic if and only if they have the same transcendence degree over the prime field $\mathbb{F}$ (recall that $\mathbb{F} = \mathbb{Q}$ if $p = 0$ and $\mathbb{F} = \mathbb{F}_p$ if p is prime). So let $\mathcal{M}_1, \mathcal{M}_2 \models ACF_p$ of cardinality $\kappa > \aleph_0$. Let A_1 and A_2 be a transcendence basis for $\mathcal{M}_1$ and $\mathcal{M}_2$ respectively. So $\mathcal{M}_1 = \mathbb{F}(A_1)^{alg}$ and $\mathcal{M}_2 = \mathbb{F}(A_2)^{alg}$. Since $\mathbb{F}$ is countable and κ is uncountable we get that

$$|A_1| = |\mathbb{F}(A_1)^{alg}| = \kappa = |\mathbb{F}(A_2)^{alg}| = |A_2|.$$

and hence $\mathcal{M}_1$ and $\mathcal{M}_2$ are isomorphic. So ACF_p is κ-categorical. Notice that ACF_p has no finite models[1]. Hence, we can apply Vaught's test to conclude that ACF_p is complete. □

It follows that $(\mathbb{Q}^{alg}, +, -, \times, 0, 1) \equiv (\mathbb{C}, +, -, \times, 0, 1)$. We will later see that $(\mathbb{Q}^{alg}, +, -, \times, 0, 1)$ is an elementary substructure of $(\mathbb{C}, +, -, \times, 0, 1)$. Moreover, from the completeness of ACF_p more can be proven:

Theorem 5.2 (Lefschetz Principle). *Let ϕ be a sentence in $\mathcal{L}_r$. The following are equivalent:*

(1) $(\mathbb{C}, +, -, \times, 0, 1) \models \phi$
(2) $(\mathbb{F}_p^{alg}, +, -, \times, 0, 1) \models \phi$ *for all but finitely many primes p.*
(3) $(\mathbb{F}_p^{alg}, +, -, \times, 0, 1) \models \phi$ *for infinitely many primes p.*

Proof. (1) $\Longrightarrow$ (2) Assume $(\mathbb{C}, +, -, \times, 0, 1) \models \phi$. Since ACF_0 is complete it follows that $ACF_0 \models \phi$. We claim that there is a finite subset $\Delta \subset ACF_0$ such that $\Delta \models \phi$. Indeed, since $ACF_0 \models \phi$ we have that $ACF_0 \cup \{\neg\phi\}$ is inconsistent. By the compactness theorem, there is a finite subset $\Delta \subset ACF_0$ such that $\Delta \cup \{\neg\phi\}$ is inconsistent. So $\Delta \models \phi$. It is not hard to see that for some $N > 0$ we have that $\Delta \subset ACF \cup \{\neg\phi_p : p \text{ is prime and } p \leq N\}$. So in particular $ACF \cup \{\neg\phi_p : p \text{ is prime and } p \leq N\} \models \phi$. From this (2) is immediate.
(2) $\Longrightarrow$ (3) is clear.
$\neg$(1) $\Longrightarrow$ $\neg$(3) Assume that $(\mathbb{C}, +, -, \times, 0, 1) \not\models \phi$. Since ACF_0 is complete $(\mathbb{C}, +, -, \times, 0, 1) \models \neg\phi$. We can apply (1) $\Longrightarrow$ (2) to $\neg\phi$ and get that $(\mathbb{F}_p^{alg}, +, -, \times, 0, 1) \models \neg\phi$ for all but finitely many primes p. Since ACF_p is complete, this means that $(\mathbb{F}_p^{alg}, +, -, \times, 0, 1) \models \phi$ only for finitely many primes p. □

Notice that we can replace $\mathbb{C}$ by any model of ACF_0 and $\mathbb{F}_p^{alg}$ by any model of ACF_p. Here is an application of the Lefschetz Principle.

Theorem 5.3 (Ax's Theorem). *Every injective polynomial map from $\mathbb{C}^n$ to $\mathbb{C}^n$ is surjective.*

Proof. For $K \models ACF$, recall that a function $f : K^n \to K^n$ is a polynomial map if $f = (f_1, \ldots, f_n)$ with $f_i \in K[x_1, \ldots, x_n]$ for each $i = 1, \ldots, n$. We say that f has degree d if each f_i has degree at most d. It is not hard to see that there is an $\mathcal{L}_r$-sentence

[1] You will prove this in the problem session.

$\Phi_{n,d}$ such that for $F \models ACF$, we have that $F \models \Phi_{n,d}$ if and only if every injective polynomial map $F^n \to F^n$ of degree d is surjective. Using Theorem 5.2 (Lefschetz Principle) it suffices to show that for any n, d and any prime p, $\mathbb{F}_p^{alg} \models \Phi_{n,d}$. Indeed then we would have that $\mathbb{C} \models \phi_{n,d}$ for any n, d which is exactly what we want to show.

Let p be an arbitrary prime number and for contradiction, suppose we have an injective polynomial map $f : (\mathbb{F}_p^{alg})^n \to (\mathbb{F}_p^{alg})^n$ which is not surjective. So there is some $\bar{a} \in (\mathbb{F}_p^{alg})^n$ not in the image of f. Let $\bar{b}$ be the tuple of the coefficients (in $\mathbb{F}_p^{alg}$) of f. Let K be the subfield of $\mathbb{F}_p^{alg}$ generated over $\mathbb{F}_p$ by $\bar{a}$ and $\bar{b}$. By construction, the restriction map $f' : K^n \to K^n$ is a one-to-one but not onto. However, notice that $K \subset \mathbb{F}_p^{alg} = \bigcup_{k>0} \mathbb{F}_{p^k}$ is finite. This is a contradiction since every injective function from a finite set to itself is surjective. □

It follows that it can more generally be shown that the above result holds for polynomial maps between Zariski closed subsets of $\mathbb{C}^n$. One can also replace $\mathbb{C}$ with any model of ACF_0.

Theorem 5.4. *ACF has quantifier elimination and hence is model complete.*

Proof. We use criterion $(*)$ of Proposition 4.12 from Lecture 4. Let $\mathcal{M}, \mathcal{N} \models ACF$ and assume that $\mathcal{A}$ is a common substructure. It is not hard to see that $\mathcal{A}$ is a subring of $\mathcal{M}$ and $\mathcal{N}$. Since $\mathcal{A}$ is a subring of a field, it is an integral domain and hence has a unique field of fractions. The field of fractions in $\mathcal{M}$ is isomorphic to that in $\mathcal{N}$. So without loss of generality we may assume that $\mathcal{A}$ is a subfield of $\mathcal{M}$ and $\mathcal{N}$. Recall that the atomic $\mathcal{L}_A$-formulas in one variable x are given by $p(x) = 0$ for $p \in A[x]$. We hence have to consider $\phi(x)$ an $\mathcal{L}_A$-formula of the form

$$\bigwedge_{i=1}^{r}(p_i(x) = 0) \wedge \bigwedge_{j=1}^{s}(q_j(x) \neq 0)$$

where $p_i, q_j \in A[x]$ for $i = 1, \ldots, r$ and $j = 1, \ldots, s$. Assume $m \in M$ is such that $\mathcal{M} \models \phi(m)$. We need to show that there is $n \in N$ is such that $\mathcal{N} \models \phi(n)$. If at least one of the $p_i(x) = 0$ appears in $\phi(x)$, then m is algebraic over $\mathcal{A}$. Let $p \in A[x]$ be its minimal polynomial. Since $\mathcal{N} \models ACF$, we can find $n \in N$ so that $p(n) = 0$. It follows that the fields $\mathcal{A}(m)$ and $\mathcal{A}(n)$ are isomorphic $\mathcal{L}_A$-structures (there is an isomorphism fixing A which sends m to n). Since $\mathcal{L}_A$-isomorphisms are elementary $\mathcal{L}_A$-embeddings, we have that $\mathcal{N} \models \phi(n)$. If no $p_i(x) = 0$ appears in $\phi(x)$, then $\bigwedge_{j=1}^{s}(q_j(m) \neq 0)$ means that m is not a root of the polynomials q_j for $j = 1, \ldots, s$. Let B be the set of all roots of the polynomials $q_1, \ldots, q_s$. It follows that B is finite. Hence any $n \in N \setminus B$ is such that $\bigwedge_{j=1}^{s}(q_j(n) \neq 0)$. So there is $n \in N$ is such that $\mathcal{N} \models \phi(n)$. Finally, from Proposition 4.11 (2) we get that ACF is model complete. □

Remark 5.5. It is not hard to see, by inspecting the proof, that ACF_p has quantifier elimination and hence is model complete.

So we finally obtain the claim that $(\mathbb{Q}^{alg}, +, -, \times, 0, 1)$ is an elementary substructure of $(\mathbb{C}, +, -, \times, 0, 1)$. There are several consequences of Theorem 5.4. First recall from Lecture 2 that if $K \models ACF$ then an *algebraic set* $V \subseteq K^n$ is the common zeroes of a set of polynomial equations with coefficient in K. More precisely, $V \subseteq K^n$ is an algebraic set if there are polynomials $P_1, \dots, P_k \in K[x_1, \dots, x_n]$ such that

$$V = \{\overline{a} \in K^n : P_1(\overline{a}) = \cdots = P_k(\overline{a}) = 0\}.$$

We have the following

Corollary 5.6. *Let $K \models ACF$. A subset $X \subseteq K^n$ is definable if and only if it is constructible*

Proof. The right to left assertion is immediate. Assume $X \subseteq K^n$ is definable. Suppose $\phi(\overline{x}, \overline{y})$ is an $\mathcal{L}_r$-formula and $\overline{a} \in K^m$ is such that $X = \{\overline{b} \in K^n : K \models \phi(\overline{b}, \overline{a})\}$. Since ACF has QE, there is a quantifier free $\mathcal{L}_r$-formula $\psi(\overline{x}, \overline{y})$ equivalent to $\phi(\overline{x}, \overline{y})$. But $\psi(\overline{x}, \overline{y})$ is a Boolean combination of atomic $\mathcal{L}_r$-formulas. So we may assume that $\psi(\overline{x}, \overline{y})$ is an atomic $\mathcal{L}_r$-formula, that is a formula of the form $p(\overline{x}, \overline{y}) = 0$ where $p \in \mathbb{Z}[\overline{x}, \overline{y}]$. Let $P \in K[\overline{x}]$ be the polynomial $p(\overline{x}, \overline{a})$. Then $X = \{\overline{b} \in K^n : P(\overline{b}) = 0\}$ is an algebraic set. □

Corollary 5.7 (Chevalley's theorem)**.** *Let $K \models ACF$. The image of a constructible set in K^n under a polynomial map is constructible.*

Proof. We write $\mathcal{L} = \mathcal{L}_r$. Let $X \subseteq K^n$ be constructible and let $F : K^n \to K^m$ be a polynomial map. By Corollary 5.6 X is definable, say by the $\mathcal{L}_K$-formula $\phi(\overline{x})$. Then the image $F(X) = \{\overline{a} \in K^m : K \models \exists \overline{x}\, (F(\overline{x}) = \overline{a} \wedge \phi(\overline{x}))\}$ is a definable set. Hence by Corollary 5.6 again, we have that $F(X)$ is constructible. □

Corollary 5.8 (Weak Hilbert's Nulstellensatz)**.** *Suppose $K \models ACF$ and I is a proper ideal in $K[x_1, \dots, x_n]$. Then there exists a tuple $\overline{a} \in K^n$ such that $P(\overline{a}) = 0$ for all $P \in I$.*

Proof. Since $K[x_1, \dots, x_n]$ is Noetherian, the ideal I is finitely generated, say by $f_1, \dots, f_k \in K[x_1, \dots, x_n]$. Let I' be a maximal ideal extending I and let us denote by F the field $F := K[x_1, \dots, x_n]/I'$. By construction $K \subseteq F \subseteq F^{alg}$. Notice that both K and F^{alg} are models of ACF and that the point $\overline{v} = \overline{x} + I' \in F^n$ is such that $f_1(\overline{v}) = \cdots = f_k(\overline{v}) = 0$. Let us write the formula $\bigwedge_{i=1}^{k}(f_i(\overline{x}) = 0)$ as $\phi(\overline{x}, \overline{b})$ with $\overline{b}$ the K-tuple of coefficients. Using model completeness of ACF we have that

$$F^{alg} \models \exists \overline{x}\, \phi(\overline{x}, \overline{b}) \implies K \models \exists \overline{x}\, \phi(\overline{x}, \overline{b}).$$

Hence, there is $\overline{a} \in K^n$ such that $f_1(\overline{a}) = \cdots = f_k(\overline{a}) = 0$. Since the f_i's generates I, the result follows.

□

Let $K \models ACF$. Given $f_1, \dots, f_k \in K[x_1, \dots, x_m]$, we denote by $V(f_1, \dots, f_m)$ set of common zeroes in K^n of the f_i's. By definition $V(f_1, \dots, f_m)$ is an algebraic set. It turns out that the Weak Nulstellensatz also tells us that if $V(f_1, \dots, f_m) = \emptyset$, then the ideal $I = (f_1, \dots, f_m)$ is such that $1 \in I$. So in particular, there are $g_1, \dots, g_m \in K[x_1, \dots, x_n]$ such that $1 = f_1 g_1 + ... + f_m g_m$. A natural question is whether there is an effective way to compute the g_i's or to prove that they do not exist. It is not hard to see that this can be achieved by providing an upper bound on the degree of the g_i's. Model theory gives an easy proof that such bounds do exists.

Proposition 5.9. *Let $m, n, d \in \mathbb{N}$. There is $\delta \in \mathbb{N}$ such that if $K \models ACF$ and $f_1, \dots, f_m \in K[x_1, \dots, x_n]$ have degree at most d and $V(f_1, \dots, f_m) = \emptyset$, then there are $g_1, \dots, g_m \in K[x_1, ..., x_n]$ of degree at most δ such that $1 = f_1g_1 + ... + f_mg_m$.*

Proof. Let $m, n, d \in \mathbb{N}$ be fixed. We will proceed by contradiction. However, observe first if $K \models ACF$, then any polynomial $P \in K[x_1, \dots, x_n]$ of degree at most e, is of the form $P(\overline{x}) = P_e(\overline{x}, \overline{a})$ for some canonical polynomial $P_e \in \mathbb{Z}[x_1, \dots, x_n, \overline{y}]$ and $\overline{a}$ some K-tuple of coefficients. So for each degree e, we also have fixed the canonical polynomial $P_e \in \mathbb{Z}[\overline{x}, \overline{y}]$.

For contradiction assume that no such $\delta \in \mathbb{N}$ exists. So for any $e \in \mathbb{N}$, there is $K \models ACF$ and $f_1, \dots, f_m \in K[x_1, \dots, x_n]$ of degree at most d with $V(f_1, \dots, f_m) = \emptyset$ such that, for any $g_1, \dots, g_m \in K[x_1, ..., x_n]$ if the degree of the g_i's is $\leq e$ then $1 \neq f_1g_1 + ... + f_mg_m$. Let $\overline{a}_1, \dots, \overline{a}_m$ be new constant symbols (we think of the $P_d(\overline{x}, \overline{a}_i)$'s as the $f_i(\overline{x})$'s) and let Φ_e be the sentence asserting that

$$\text{for all } \overline{x}, \overline{b}_1, \dots, \overline{b}_m, \qquad 1 \neq \textstyle\sum_{i=1}^m P_d(\overline{x}, \overline{a}_i) P_e(\overline{x}, \overline{b}_i).$$

So if we interpret $P_d(\overline{x}, \overline{a}_i)$ as $f_i(\overline{x})$ the sentence Φ_e is a step towards saying that e is not a bound. Consider now T the theory

$$ACF \cup \{\neg \exists \overline{x} \bigwedge_{i=1}^m (P_d(\overline{x}, \overline{a}_i) = 0)\} \cup \{\Phi_e : e \in \mathbb{N}_{>0}\}.$$

Let Δ be a finite subset of T. Then for some $N > 0$, we have that

$$\Delta \subset ACF \cup \{\neg \exists \overline{x} \bigwedge_{i=1}^m (P_d(\overline{x}, \overline{a}_i) = 0)\} \cup \{\Phi_e : e \leq N\}.$$

Using our assumption we see that Δ is consistent. Hence using the compactness theorem, T is consistent. Let $F \models T$. Then F is a model of ACF in which the Weak Hilbert's Nulstellensatz fails. $\square$

5.2. **Complete Theories revisited.** So far we have used Vaught's test to prove that a given consistent theory T is complete. However, in the next lecture we will look at $Th(\mathbb{R}, +, -, \times, 0, 1, <)$ and in this case Vaught's test will not apply. For example the following is true.

Proposition 5.10. *There is a $\mathcal{R} \models Th(\mathbb{R}, +, -, \times, 0, 1, <)$ which has cardinality $\mathfrak{c} = |\mathbb{R}|$ but which is not isomorphic to $(\mathbb{R}, +, -, \times, 0, 1, <)$.*

Proof. Let us write $\mathcal{M} = (\mathbb{R}, +, -, \times, 0, 1, <)$ and $T = Th(\mathbb{R}, +, -, \times, 0, 1, <)$. Also let $\mathcal{U}$ be an ultrafilter on $\mathbb{N}$ that extends the Fréchet filter. Consider the ultraproduct $\mathcal{R} := \prod \mathcal{M}/U$ (so here $\mathcal{M}_i = \mathcal{M}$ for all $i \in \mathbb{N}$). Such a product is called an ultrapower of $\mathcal{M}$. It is not hard to see that $\mathcal{R}$ has the same cardinality as $\mathbb{R}$ since we have considered a countable direct product of $\mathbb{R}$. It is also not hard to see that $\mathcal{R} \models T$. Indeed if $\phi \in T$, then $\{i \in \mathbb{N} : \mathcal{M}_i \models \phi\} = \mathbb{N} \subset \mathcal{U}$. Hence by Loś' Theorem, $\mathcal{R} \models \phi$. Let $f \in \prod_{i \in \mathbb{N}} \mathcal{M}$ be the function defined as $f(i) = \frac{1}{i+1}$ and let us write $\epsilon := \underline{f}$. Then ϵ

is an infinitesimal: $\mathcal{R} \models (0 < \epsilon)$ and $\mathcal{R} \models (\epsilon < r)$ for any $r \in \mathbb{R}$. This follows from Loś' Theorem since the set $\{i \in \mathbb{N} : \mathcal{M} \models \frac{1}{i+1} < r\}$ is cofinite and hence in $\mathcal{U}$. So in particular $\mathcal{R}$ is not isomorphic to $(\mathbb{R}, +, -, \times, 0, 1, <)$. $\square$

We will need the following alternate "test".

Proposition 5.11. *Suppose T is a consistent $\mathcal{L}$-theory that has quantifier elimination. Suppose that there is a $\mathcal{L}$-structure $\mathcal{A}$ such that for any $\mathcal{M} \models T$, there is an embedding $\rho : \mathcal{A} \to \mathcal{M}$. Then T is complete.*

Proof. Let ϕ be an $\mathcal{L}$-sentence. We need to show that either $T \models \phi$ or $T \models \neg\phi$. Since T is consistent, there is $\mathcal{M} \models T$. Since ϕ is an $\mathcal{L}$-sentence we have that either $\mathcal{M} \models \phi$ or $\mathcal{M} \models \neg\phi$. Without loss of generality let us assume that $\mathcal{M} \models \phi$. Let $\mathcal{N} \models T$ be arbitrary. We need to show that $\mathcal{N} \models \phi$. Since T has QE and $\mathcal{A}$ embeds in both $\mathcal{M}$ and $\mathcal{N}$, from Proposition 4.11[2] we have that

$$\mathcal{M} \models \phi \iff \mathcal{N} \models \phi.$$

Hence $T \models \phi$. $\square$

As a corollary, we give a different proof that ACF_p is complete

Corollary 5.12. *ACF_p is complete*

Proof. We have already seen from Theorem 5.4 (see Remark 5.1) that ACF_p has QE. Recall that the prime field $\mathbb{F}$ is such that $\mathbb{F} = \mathbb{Q}$ if $p = 0$ and $\mathbb{F} = \mathbb{F}_p$ if p is prime. Then $\mathbb{F}$ embeds in any model of ACF_p. Hence using Proposition 5.11, ACF_p is complete. $\square$

[2]Proposition 4.11 can be easily modified to work for common embedding rather than common substructure.