Algebra and Geometry in Basic Model Theory of Fields

Notes from a short course by
Angus Macintyre

October 5, 2008

The emphasis in this course will be on a geometric formulation of the model theory of algebraically closed fields, eventually with extra structure. From this viewpoint, an abstract quantifier elimination, in which one need not mention individual algebraically closed fields and their elements, is central, and uncountable categoricity peripheral.

From now on all rings are commutative with 1. Here we deal mainly with domains, though this distinction is quite unnatural from the viewpoint of modern algebraic geometry. Fields have $0 \neq 1$, ideals are assumed proper and homomorphisms of rings are unital. For any ring R and any subset $A \subset R$, we denote by $\langle A \rangle$ the ideal generated by A in R.

1 Basic definitions and properties

Since any homomorphism of fields is injective, the category **Fields** has fields as objects and ring monomorphisms as morphisms. Important variants restrict the morphisms to be *separable*, or *regular* (see below, 4.2 4.5 4.6). Valuation theory considers instead *places*, partially defined maps. Note that **Fields** is a disjoint union of categories of fields of different characteristics.

Remark. If R is a domain with $0 \neq 1$, there is a unique homomorphism $\mathbb{Z} \to R$ and its kernel is a prime ideal of $\mathbb{Z}$, so either (0) or (p) for a unique prime p. The *characteristic* of R is 0 in the first case, and p in the second.

2 Spectrum of rings and Noetherian spaces

2.1 Spectrum of rings

Definition 1. Let R be a ring. Then the *spectrum of* R, denoted by $\mathrm{Spec}(R)$, is the topological space specified as follows: its elements are the prime ideals P of R and its closed sets are of the form $C_A = \{P : A \subset P\}$, for $A \subset R$. Consequently, open sets are of the form $U_A = \{P : A \not\subset P\}$, for $A \subset R$.

It is useful to note that every C_A (respectively U_A) can be obtained with A

a radical ideal, i.e. $\mathrm{Rad}(A) = A$, where

$$\begin{aligned}\mathrm{Rad}(A) &= \{r : r^n \in A \text{ for some } n \in \mathbb{N}\} \\ &= \text{ (non-trivially) } \bigcap\{P : A \subset P,\ P \text{ prime}\}\end{aligned}$$

The topology of $\mathrm{Spec}(R)$ is not Hausdorff in general. We have for example that, if P a prime ideal of R, then $\{P\}$ is closed in $\mathrm{Spec}(R)$ if and only if P is maximal. $\mathrm{Spec}(\mathbb{Z})$ for instance is not Hausdorff, for (0) is not maximal, though all other prime ideals are. Both $\mathcal{P}(R)$, the power set of R, and $\mathrm{Spec}(R)$ are partially ordered by $\subset$. The map

$$\begin{aligned}\mathcal{P}(R) &\to \mathrm{Spec}(R) \\ A &\mapsto C_A\end{aligned}$$

is order-reversing, and

$$C_{\bigcup A_i} = \bigcap C_{A_i}.$$

Theorem 2. *For any ring R, $\mathrm{Spec}(R)$ is compact.*

Proof. Note first, by the fact that any proper ideal is contained in a maximal one, that for any $B \subset R$, $C_B = \emptyset$ if and only if $\langle B\rangle = R$. One has to show that if $\{C_{A_i} : i \in I\}$ has the finite intersection property, then $\bigcap C_{A_i} \neq \emptyset$, i.e. $C_{\bigcup A_i} \neq \emptyset$. Now if $C_{\bigcup A_i} = \emptyset$, then $\langle \bigcup A_i\rangle = R$ and thus $1 \in \langle \bigcup A_i\rangle$. Then $1 \in \langle \bigcup_{i\in I_0} A_i\rangle$ for some finite $I_0 \subset I$, and so $C_{\bigcup_{i\in I_0} A_i} = \emptyset$, i.e. $\bigcap_{i\in I_0} C_{A_i} \neq \emptyset$. □

Let $f : R \to S$ be a ring (homo)morphism. Define $\mathrm{Spec}(f)$, or f^*, as

$$\begin{aligned}f^* : \mathrm{Spec}(S) &\to \mathrm{Spec}(R) \\ P &\mapsto f^{-1}(P)\end{aligned}$$

It can be easily checked that f^* maps $\mathrm{Spec}(S)$ to $\mathrm{Spec}(R)$, is continuous, and is functorial, i.e. $(fg)^* = g^*f^*$ and $1_R^* = 1_{\mathrm{Spec}\, R}$.

2.2 Noetherian Rings

Definition 3. A ring R is said to be *Noetherian* if every ideal of R is finitely generated.

Lemma 4. *A ring R is Noetherian if and only if R has the Ascending Chain Condition (ACC) for ideals, i.e. any increasing chain of ideals is stationary.*

Proof. Let $(A_i)_{i<\omega}$ be an increasing chain of ideals of R, and let $A = \bigcup_{i<\omega} A_i$. Since the A_i form a chain, A is an ideal, which moreover is finitely generated by Noetherianity. Let $a_1, \ldots, a_n$ be generators of A. For any $j \leq n$, there is $m_j < \omega$ such that $a_j \in A_{m_j}$. Let m be the biggest of all the m_j. Then by the fact that the A_i are increasing, all the a_j for $j \leq n$ are in A_m, so $A \subset A_m$, and since also $A_m \subset A$, we get that $A_m = A$. Therefore for all $m' \geq m$, $A_{m'} = A$, which proves our claim. □

Example. Any Principal Ideal Domain (PID) is Noetherian, and in particular $\mathbb{Z}$ and $K[X]$, for K a field, are Noetherian.

Theorem 5. *(Hilbert's Basis Theorem) If R is Noetherian, so is $R[X]$.*

This proof can be found in [2]. The following notion will be useful in the proof and later: If $f = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in R[X]$, with $a_n \neq 0$, we define the *initial term* of f to be $a_n X^n$, the *initial coefficient* of f to be a_n and the *degree of* f to be n.

Proof. Assume towards a contradiction that there is an ideal I of $R[X]$ that is not finitely generated. Then choose a sequence of elements $f_1, f_2, \cdots \in I$ as follows: Let f_1 be a nonzero element of least degree in $I \neq 0$. For $j > 1$, since by our assumption $\langle f_1, \ldots, f_j \rangle \neq I$, choose f_{j+1} to be an element of least degree among those in I but not in $\langle f_1, \ldots, f_j \rangle$.

Let a_j be the initial coefficient of f_j. Since R is Noetherian, the ideal $J = \langle a_1, a_2, \ldots \rangle$ of all the a_j is finitely generated. We may choose a finite set of generators from among the a_j themselves. Let m be the first integer such that $a_1, \ldots, a_m$ generate J.

We claim that $I = \langle f_1, \ldots, f_m \rangle$. We may write $a_{m+1} = \Sigma_{j=1}^{m} u_j a_j$, for some $u_j \in R$. Since the degree of f_{m+1} is greater or equal to the degree of each of $f_1, \ldots, f_m$, we may define a polynomial $g \in R$ having the same degree and initial term as f_{m+1} by the formula

$$g = \Sigma_{j=1}^{m} u_j f_j X^{deg f_{m+1} - deg f_j} \in \langle f_1, \ldots, f_m \rangle.$$

The difference $f_{m+1} - g$ is then in I but not in $\langle f_1, \ldots, f_m \rangle$, and has degree strictly less than the degree of f_{m+1}. This contradicts the choice of f_{m+1} as having minimal degree. □

Corollary 6. *If R is Noetherian, so is every $R[X_1, ..., X_n]$.*

The following is easy to check

Lemma 7. *A homomorphic image of a Noetherian ring is Noetherian. Consequently, any finitely generated extension of a Noetherian ring is Noetherian.*

2.3 Noetherian spaces

Definition 8. A topological space X is called Noetherian, if it has the *Descending Chain Condition (DCC)* for closed sets.

Lemma 9. *If R is a Noetherian ring, then Spec(R) is a Noetherian Space.*

Proof. If $\{C_{A_n} : n < \omega\}$ is strictly descending, for A_n ideals, then the ideal generated by the union of the A_n cannot be finitely generated. □

Parallel to this we have:

Lemma 10. *If $f : X \to Y$ is a continuous surjection and X is Noetherian, then Y is also Noetherian.*

Proof. Given a descending chain $\{Y_n : n < \omega\}$ of closed sets in Y, the descending chain $\{f^{-1}(Y_n) : n < \omega\}$ of closed sets in X is eventually constant, and so must be the former since $Y_n = f(f^{-1}(Y_n))$. □

When using Noetherianity of spaces the usual formulation is that every non-empty collection of closed sets has a minimal element. We present to basic examples of this.

Use 1: Irreducible sets and components

A closed set C is said to be *irreducible* if there are no C_1 and C_2 proper closed subsets of C such that $C = C_1 \cup C_2$

Theorem 11. *Let X be a Noetherian space.*

1. *Each closed set C of X can be written as a finite union of closed irreducible sets.*
2. *This representation of C as $C_1 \cup \cdots \cup C_n$ is unique if we require that there are no inclusions among the C_i.*

Proof. For the first part, suppose that there exists a counterexample, then let C be a minimal such closed set. Obviously C cannot be irreducible, and then $C = C_1 \cup C_2$ for some C_1 and C_2 proper closed subsets of C. By our election of C, both C_1 and C_2 can be written as finite unions of irreducible closed sets. Putting together these representations we get one for C, and so we have a contradiction.

For the uniqueness let $C_1, ..., C_n$ and $D_i, ..., D_n$ be closed irreducible sets such that

$$C = C_1 \cup \cdots \cup C_n = D_1 \cup \cdots \cup D_m,$$

and for every $i \neq j$, $C_i \not\subset C_j$ and $D_i \not\subset D_j$. Then for each i, $C_i = C_i \cap \bigcup_j D_j = \bigcup_j (C_i \cap D_j)$, and by the irreducibility of C_i this implies that, for some j, $C_i = C_i \cap D_j$, i.e. $C_i \subset D_j$. Moreover, using the irreducibility of D_j, there exist l such that $D_j \subset C_l$, and so $i = l$ and $C_i = D_j$. Finally, using an analogous argument we have that for every j, there is an i such that $D_j = C_i$, thus the two representations of C are the same. □

Use 2: Dimension

This is essentially a notion of classical set theory. It is normally given in algebra for closed irreducible sets by the recursion

$$\dim(\emptyset) = -1,\ \dim(C) = \sup\{\dim(D) + 1 : D \subsetneq C\}.$$

With this definition it can be easily proved that every non-empty closed set has an ordinal valued dimension.

Then the definition of dimension can be extended to all closed sets by

$$\dim(C) = \max\{\dim(D) : D \text{ is an irreducible component of } C\}.$$

2.4 Hilbert's Nullstellensatz

Gauss' fundamental theorem of algebra establishes the basic link between algebra and geometry: It says that a polynomial in one variable over $\mathbb{C}$, an algebraic object, is determined up to a scalar factor by the set of its roots (with multiplicities), a geometric object. Hilbert's Nullstellensatz extends this link to certain ideals of polynomials in many variables. It is a formal consequence of the fundamental theorem of algebra in the sense that it holds for any algebraically closed field.

Let k be a field, $X \subset k^n$ and $I \subset k[x_1, \ldots, x_n]$, we denote by

$$Z(I) := \{(y_1, \ldots, y_n) \in k^n; \forall g \in I, g(y_1, \ldots, y_n) = 0\}$$

and by

$$I(X) := g \in k[x_1, \ldots, x_n]; \forall (y_1, \ldots, y_n) \in X, g(y_1, \ldots, y_n) = 0.$$

It is clear that I can be replaced by the ideal it generates in $k[x_1, \ldots, x_n]$ without changing $Z(I)$, and that $I(X)$ is an ideal.

Theorem 12 (Nullstellensatz)**.** *Let k be an algebraically closed field. If $I \subset k[x_1, \ldots, x_n]$ is an ideal, then*

$$I(Z(I)) = Rad(I).$$

Thus the correspondences $I \longrightarrow Z(I)$ and $X \longrightarrow I(X)$ induce a bijection between the collection of algebraic subsets of k^n and the radical ideals of $k[x_1, \ldots, x_n]$

See [2, 4.5 Theorem 1.6] for details.

2.5 Zariski Topology

Definition 13. Let $K \to L$ be a field extension, and n a positive integer. On L^n take as closed sets all finite intersections of sets of the form

$$\{\bar{\alpha} \in L^n : f(\bar{\alpha}) = 0\}$$

with $f \in K[X_1, ..., X_n]$, the resulting topology is called the *K-Zariski topology* on L^n.

Lemma 14. *Given a field extension $K \to L$, the space L^n with the K-Zariski topology has the following properties:*

1. *It is quasi-compact,*
2. *It is Noetherian,*
3. *If $K = L$, all its points are closed,*
4. *If K infinite, it is not Hausdorff.*

Proof.

1. Let $\mathcal{F}$ be a family of closed sets of L^n such that $\bigcap_{F \in \mathcal{F}} F = \emptyset$. Let J be the ideal generated by the $I(F)$'s in $K[x_1, \ldots, x_n]$. Then, by the nullstellensatz, $Rad(J) = K[x_1, \ldots, x_n]$, and there are finitely many elements $f_i \in I(F_i), F_i \in \mathcal{F}, i \leq n$ such that $Rad\langle f_1, \ldots, f_n\rangle = K[x_1, \ldots, x_n]$, thus $Rad\langle I(F_1) \bigcup \cdots \bigcup I(F_n)\rangle = K[x_1, \ldots, x_n]$. It is clear then that $F_1 \bigcap \cdots \bigcap F_n = \emptyset$.
2. By the nullstellensatz, to a descending chain of closed sets in L^n corresponds an increasing chain of radical ideals in $K[x_1, \ldots, x_n]$. Noetherianity of L^n follows then by the Hilbert's basis theorem.
3. Clear.
4. In fact, for K infinite, if fg vanishes in every point of K^n, then by the nullstellensatz, $fg = 0$ in $K[X_1, ..., X_n]$.

□

2.6 Generic points (of spaces)

Definition 15. Let C be a closed set in a topological space X, we say that $\alpha \in C$ is *a generic point of* C, if α belongs to no proper closed subset of C, i.e. $\{\bar{\alpha}\} = C$.

Consider the question of existence and uniqueness of generic points.

Lemma 16. *If a closed set C has a generic point, then it is irreducible.*

Proof. Let α be a generic point of C and suppose that $C = C_1 \cup C_2$ for some closed sets C_1 and C_2. For some $i \in \{1, 2\}$ $\alpha \in C_i$, then $\{\bar{\alpha}\} \subset C_i$, and so $C_i = C$. □

However, in a general Noetherian space irreducible closed sets need not have generics and generics may not be unique.

Example. Consider the $\mathbb{Q}$-Zariski topology on $\mathbb{Q}^2$. The unit circle $C = \{(u, v) \in \mathbb{Q}^2 : u^2 + v^2 = 1\}$ is irreducible, but has no generic point.

Example. Now consider the $\mathbb{Q}$-Zariski topology on $\mathbb{R}^2$. The unit circle $C = \{(u, v) \in \mathbb{R}^2 : u^2 + v^2 = 1\}$ has uncountably many generic points, namely every $(t, \sqrt{1 - t^2})$ such that t is a real transcendental number with $|t| < 1$.

But for $\mathrm{Spec}(R)$, R any ring, irreducible closed sets have unique generics.

Theorem 17. *If A is an ideal in R, C_A is irreducible if and only if* $\mathrm{Rad}(A)$ *is prime. Moreover, if C_A is irreducible, then it has a unique generic point* $\mathrm{Rad}(A)$.

Proof. Recall that $C_A = C_{\mathrm{Rad}(A)}$. Suppose that $\mathrm{Rad}(A)$ is not prime, and let $f, g \in A - \mathrm{Rad}(A)$ be such that $fg \in \mathrm{Rad}(A)$. Then

$$C_{\mathrm{Rad}(A)} = C_{\mathrm{Rad}(A) \cup \{f\}} \cup C_{\mathrm{Rad}(A) \cup \{g\}}.$$

Moreover, since $f, g \notin \mathrm{Rad}(A) = \bigcap\{P : A \subset P,\ P \text{ prime}\}$, there exist prime ideals P_f and P_g containing A such that $f \notin P_f$ and $g \notin P_g$, and then $P_f \in C_{\mathrm{Rad}(A)} - C_{\mathrm{Rad}(A) \cup \{f\}}$ and $P_g \in C_{\mathrm{Rad}(A)} - C_{\mathrm{Rad}(A) \cup \{g\}}$. Thus, $C_{\mathrm{Rad}(A)}$ is not irreducible.

Conversely, if $\mathrm{Rad}(A)$ is prime, then $\mathrm{Rad}(A)$ is a generic point of $C_{\mathrm{Rad}(A)}$, so $C_{\mathrm{Rad}(A)}$ is irreducible. The uniqueness follows immediately. □

2.7 $\mathbb{Z}[X_1, ..., X_n]$ and $K[X_1, ..., X_n]$

The polynomial rings $\mathbb{Z}[X_1, ..., X_n]$ and $K[X_1, ..., X_n]$, K a field, are Noetherian, and for $n = 1$ the latter is a PID. We shall see that the quantifier elimination for algebraically closed fields can naturally be stated and proved in terms of the spaces $\mathrm{Spec}(\mathbb{Z}[X_1, ..., X_n])$ $(n = 0, 1, 2, ...)$ without ever mentioning a single algebraically closed field.

The meaning of point

Let $g : R \to S$ be a homomorphism of rings, and write g also for the induced homomorphism from $R[X_1, ..., X_n]$ to $S[X_1, ..., X_n]$. Then $\mathrm{Spec}(g)$ is a continuous map from $\mathrm{Spec}(S[X_1, ..., X_n])$ to $\mathrm{Spec}(R[X_1, ..., X_n])$. If S is a domain, $S[X_1, ..., X_n]$ is too. Then an element $\bar{\alpha} \in S^n$ determines an element of $\mathrm{Spec}(S[X_1, ..., X_n])$ by

$$\bar{\alpha} \mapsto \ J_{\bar{\alpha}} = \{h \in S[X_1, ..., X_n] : h(\bar{\alpha}) = 0\}.$$

We define $I(\bar{\alpha}|R)$, when g is understood and S is a domain, as $\mathrm{Spec}(g)(J_{\bar{\alpha}})$.

When g is an embedding, identifying R and $g(R)$, $I(\bar{\alpha}|R)$ is the ideal of polynomials over R vanishing in $\bar{\alpha}$. In fact, if R is a domain, we get all elements of $\mathrm{Spec}(R[X_1, ..., X_n])$ in this way. For if $P \in \mathrm{Spec}(R[X_1, ..., X_n])$ let $S = R[X_1, ..., X_n]/P$ and $\bar{\alpha} = (X_1 + P, ..., X_n + P)$. We can also take S to be the field of fractions of $S = R[X_1, ..., X_n]/P$ if we wish. Note that from this it follows that $I(\bar{\alpha}|R)$ need not be maximal, even if R is a field.

Seen from R, $\bar{\alpha}$ and $\bar{\beta}$ in perhaps different S are *algebraically indistinguishable* if $I(\bar{\alpha}|R) = I(\bar{\beta}|R)$. What remains after we forget the *set-theoretic points* $\bar{\alpha}, \bar{\beta}, ...$ is the element of $\mathrm{Spec}(R[X_1, ..., X_n])$.

We are going to formulate the basic model theory of fields in terms of $\mathrm{Spec}\,\mathbb{Z}[X_1, ..., X_n]$, $n \in \omega$. This contrasts with the fact that neither $\mathbb{Z}[X_1, ..., X_n]$ nor its spectrum have much of a model theory in the classical sense.

Varieties

For this course and *affine variety* in n-space over R, which we assume to be $\mathbb{Z}$ or a field, is defined as an irreducible closed set in $\mathrm{Spec}(R[X_1, ..., X_n])$ (It is desirable to go further in the direction of a scheme-theoretic model theory, but the length of the course precludes this).

We have seen in the discussion of generic points that an affine variety C is of the form $C_P := C_{\{}P\}$ for a unique prime ideal P, the generic point of C. By *a point of* C we will understand an element of C_P. Such *points* correspond to the ideals $I(\bar{\alpha}|R) \supset P$, i.e. loosely to the set-theoretic points of the algebraic set defined by P (note that P is finitely generated). They may very well not be closed points of C_P.

2.8 Logic topology and Spectral topology

For a language L, first-order or propositional, let $\mathrm{Tarski}(L)$ be the set of complete L-theories. $\mathrm{Tarski}(L)$ is topologized by taking as closed sets the ones of the form $C_{T_0} = \{T : T_0 \subset T\}$ for an L-theory T_0.

The Compactness Theorem says that $\mathrm{Tarski}(L)$ is compact, and has as basis the set of clopens C_{T_0} for T_0 finite. So one says that $\mathrm{Tarski}(L)$ is a compact totally disconnected space, or a *Stone space*. Also note that $\mathrm{Tarski}(L)$ is Hausdorff.

The clopen sets form a Boolean algebra, and thus a Boolean ring $\mathrm{Ring}(L)$ under:

$$a \cdot b = a \cap b,$$
$$a + b = (a \cap b^c) \cup (a^c \cap b).$$

Note, since Ring(L) is a Boolean ring, all its prime ideals are maximal.

So, what is the connection between Tarski(L) and Spec(Ring(L))?

For $T \in \text{Tarski}(L)$ define

$$P_T = \{r \in \text{Ring}(L) : T \notin r\}.$$

It is an easy exercise to check that P_T is a prime ideal of Ring(R).

Conversely, for $P \in \text{Spec}(\text{Ring}(L))$ define

$$T_P = \{\phi : C_{\{\phi\}} \in P\}.$$

Again, it can be checked that $T_P \in \text{Tarski}(L)$, $P_{T_P} = P$ and $T_{P_T} = T$. Thus $T \mapsto P_T$ is a bijection.

Moreover, if A is a set of clopens, the inverse image of $C_A \subset \text{Spec}(\text{Ring}(L))$ is the set of theories T meeting all the complements of elements of A, and so is closed. Thus the map $T \mapsto P_T$ is continuous.

Now note that Spec(R) is Hausdorff for any Boolean ring R. For if P_1 and P_2 are distinct elements, there is $r \in R$ with $r \in P_1$ and $1 - r \in P_2$. Finally, since a continuous bijection of compact Hausdorff spaces need to be a homeomorphism, we have that Tarski(L) and Spec(Ring(L)) are homeomorphic.

2.9 The Characteristic Revisited

Let L be the language of ring theory, and let Tarski(Fields) be the closed subset of Tarski(L) consisting of the complete theories of fields.

The *characteristic* of a field is a first crude first-order invariant of fields: For a field K, and p a prime number,

$$\text{ch}(K) = p \iff K \vDash \underbrace{1 + 1 + ... + 1}_{p \text{ times}} = 1$$

$$\text{ch}(K) = 0 \iff K \vDash \underbrace{1 + 1 + ... + 1}_{p \text{ times}} \neq 1, \text{ for any prime } p$$

Exercise 1. Show that no first-order sentence expresses that a field has characteristic 0.

Exercise 2. Let Φ be a set of sentences in the language of ring theory. Prove that if Φ holds in some fields of arbitrarily large characteristic, then Φ holds in some field of characteristic 0.

Exercise 3. Give an example of a sentence ψ which holds in some field of characteristic 0, but does not hold in any field of finite characteristic. [Hint: Think of $\mathbb{R}$]

For p a prime number or zero, consider Tarski(ch(K) = p) the closed subset of Tarski(Fields). If p is a prime this set is a clopen, but if $p = 0$ it is not.

Exercise 4. The map

$$\begin{aligned} \text{Tarski(Fields)} &\to \text{Spec}(R) \\ T &\mapsto \text{ch}(K), \text{ for } K \vDash T \end{aligned}$$

is continuous but is not a homeomorphism.

3 Chevalley-Tarski

3.1

This is the basic quantifier elimination for algebraically closed fields. We give it as a *direct image theorem* for the system of spaces $\mathrm{Spec}(\mathbb{Z}[X_i : i < n])$ with no reference to quantifiers.

3.2

Consider the natural monomorphism

$$j_n : \mathbb{Z}[X_i : i < n] \to \mathbb{Z}[X_i : i < n+1]$$

and its dual map

$$\begin{aligned} \mathrm{Spec}(j_n) : \mathrm{Spec}(\mathbb{Z}[X_i : i < n+1]) &\to \mathrm{Spec}(\mathbb{Z}[X_i : i < n]) \\ P &\mapsto P \cap \mathbb{Z}[X_i : i < n] \end{aligned}$$

$\mathrm{Spec}(j_n)$ is not in general a *proper* map, i.e. the image of a closed set need not be closed. This corresponds to the fact that in the quantifier elimination for algebraically closed fields negations of atomic formulas are needed.

The standard example of a non-proper $\mathrm{Spec}(j_n)$ is obtained by taking $n = 2$ and considering the closed set $C_{\{X_0X_1-1\}}$ whose image is the complement of C_{X_0} in $\mathbb{Z}[X_0]$ which is not closed.

Exercise 5. Show that indeed C_{X_0} is not open in $\mathbb{Z}[X_0]$.

3.3

To get the right theorem one works with *constructible sets*.

Definition 18. A subset Y of a topological space X is called *locally closed* if for each $y \in Y$ there is an open subset U_y and a closed set C_y such that $y \in U_y$ and $Y \cap U_y = C_y \cap U_y$.

Lemma 19. *Let X be a space. $Y \subset X$ is locally closed if and only if it can be written as $Y = U \cap C$ for some open set U and some closed set C.*

Proof. ($\Leftarrow$) Clear. ($\Rightarrow$) Suppose that Y is locally closed and, for each $y \in Y$, let U_y and C_y as in the definition. Since $Y \cap U_y = C_y \cap U_y$, we have that $Y^c \cap U_y = C_y^c \cap U_y$, and so

$$Y^c \cap U = \bigcup_{y \in Y} (C_y^c \cap U_y),$$

where $U = \bigcap_{y \in Y} U_y$. The set in the right hand side of the equality above is obviously open, let us call it V. Finally note that $Y = V^c \cap U$. □

Definition 20. A subset Y of a topological space X is called *constructible* if it is a finite union of locally closed sets.

Note that the constructible sets of a space X form the smallest Boolean subalgebra of $\mathcal{P}(X)$ containing all open and closed sets of X.

Theorem 21 (Abstract Chevalley-Tarski)**.** *The image under* $\mathrm{Spec}(j_n)$ *of a constructible set is constructible.*

Remark. The most specific item used in the proof of the theorem is the fact that $K[X]$ is a Principal Ideal Domain, for K a field. In some way or another this is used in all proofs of quantifier elimination in basic field theory.

Proof. Note that, since image commutes with finite unions, it is enough to show that the image of every $Y = U \cap C \subset \mathbb{Z}[X_i : i < n+1]$, with U an open set and C an irreducible closed set, is constructible.

Suppose for the sake of a contradiction that $\mathrm{Spec}(j_n)(Y)$ is not constructible for some such Y. Given that $\mathbb{Z}[X_i : i < n+1]$ is Noetherian, we may also assume that Y is a counterexample with minimal C, i.e. for every $C' \subsetneq C$ closed, and every U' open, $\mathrm{Spec}(j_n)(U' \cap C')$ is constructible.

Let P_0 be the generic point of C and let $g_0, ..., g_m$ be generators for P_0. Then $P_0 \in U$, since otherwise Y would be empty, contradicting our initial assumption. Let $U = U_B$ for B an ideal and note that if $f_0, ..., f_r$ are generators of B, then $U = U_{\{f_0\}} \cup ... \cup U_{\{f_r\}}$ and so $Y = (U_{\{f_0\}} \cap C) \cup ... \cup (U_{\{f_r\}} \cap C)$. Thus we may assume that $U = U_{\{f\}}$ for some $f \in \mathbb{Z}[X_i : i < n+1]$.

To simplify the notation let $R = \mathbb{Z}[X_i : i < n]$. Notice that $\mathrm{Spec}(j_n)$ has a section given by

$$\begin{aligned} \mathrm{Spec}(R) &\to \mathrm{Spec}(R[X_n]) \\ p &\mapsto \langle p \rangle \end{aligned}$$

For $p \in \mathrm{Spec}\, R$. We have a natural isomorphism

$$R[X_n]/\langle p \rangle \cong R/p[X_n].$$

Also note that this induces a natural isomorphism:

$$((R-p)/\langle p \rangle)^{-1} R[X_n]/\langle p \rangle \cong F_p[X_n],$$

where F_p is the field of fractions of R/p. In what follows we identify this two rings.

Consider the natural projection $R[X_n] \to R[X_n]/\langle p \rangle$, clearly $P_0/\langle p \rangle = \langle g_0 + \langle p \rangle, ..., g_m + \langle p \rangle \rangle$. Furthermore, consider $\langle P_0/\langle p \rangle \rangle$, the ideal generated by $P_0/\langle p \rangle$ in $F_p[X_n]$. We know that $\langle P_0/\langle p \rangle \rangle$ is principal, with generator $\gcd(g_0 + \langle p \rangle, ..., g_m + \langle p \rangle)$.

Let $p_0 = Spec(j_n)(P_0)$, i.e. $p_0 = P_0 \cap R$. Using the Euclidean algorithm $g + \langle p_0 \rangle := \gcd(g_0 + \langle p_0 \rangle, ..., g_m + \langle p_0 \rangle)$ can be written as a linear combination of $g_0 + \langle p_0 \rangle, ..., g_m + \langle p_0 \rangle$ in $F_{p_0}[X_n]$, fix one such linear combination and let $h_0, ..., h_m \in R - p_0$ be representatives for the $\langle p_0 \rangle$-classes which appear as denominators of its coefficients. Let $U' = U_{\{\prod h_i\}} \subset \mathrm{Spec}(R)$, open neighborhood of p_0. In fact, for every $p \in U' \cap C_{p_0}$, $g + \langle p \rangle$ generates $\langle P_0/\langle p \rangle \rangle$.

Given that P_0 is a prime ideal in $R[X_n]$ containing $\langle p_0 \rangle$, $P_0/\langle p_0 \rangle$ is a prime ideal in $R[X_n]/\langle p_0 \rangle$. Also, since $P_0/\langle p_0 \rangle$ is disjoint from the multiplicative set $R - p_0/\langle p_0 \rangle$, $\langle P_0/\langle p_0 \rangle \rangle$ is a prime ideal in $F_{p_0}[X_n]$. We conclude that $g + \langle p_0 \rangle$ is irreducible in $F_{p_0}[X_n]$.

The irreducibility of $g + \langle p_0 \rangle$ gives us that, in the same polynomial ring, $\gcd(g + \langle p_0 \rangle, f + \langle p_0 \rangle) = 1 + \langle p_0 \rangle$. To check this note that otherwise we would have

$$g + \langle p_0 \rangle (G + \langle p_0 \rangle / H + \langle p_0 \rangle) = f + \langle p_0 \rangle$$

for some $G \in R[X_n]$, $H \in R - p_0$. And then, writing $g + \langle p_0 \rangle$ as a linear combination of the $g_i + \langle p_0 \rangle$ and eliminating the denominators, we would have that for some $G_0, ..., G_m \in R[X_n]$ and some $H' \in R - p_0$

$$G_0 g_0 + \cdots + G_m g_m + \langle p_0 \rangle = H' f + \langle p_0 \rangle,$$

and it would follow that $f \in P_0$.

Now, using the Euclidean algorithm in $F_{p_0}[X_n]$ write $1 + \langle p_0 \rangle$ as a linear combination of $g + \langle p_0 \rangle$ and $f + \langle p_0 \rangle$, and let $h_0', h_1' \in R - p_0$ be representatives for the denominators of the coefficients of the linear combination. Let $W = U_{\{\prod h_i \prod h_i'\}} \subset \operatorname{Spec} R$, open neighbourhood of p_0, then we have that, for every $p \in W \cap C_{p_0}$, $g + \langle p \rangle$ and $f + \langle p \rangle$ generate $F_p[X_n]$.

Claim:

$$W \cap C_{p_0} \subset \operatorname{Spec}(j_n)(U \cap C)$$

Proof of Claim:

We show that for $p \in W \cap C_p 0$, $\langle p \rangle + P_0 \in U \cap C$ and $\operatorname{Spec}(j_n)(\langle p \rangle + P_0) = p$.

It is clear that $\langle p \rangle + P_0$ contains P_0, so it belongs to C. Further we have the following:

$$\operatorname{Spec}(j_n)(\langle p \rangle + P_0) = (\langle p \rangle + P_0) \cap R = (\langle p \rangle \cap R) + (P_0 \cap R) = p + p_0 = p.$$

It is left to see that $\langle p \rangle + P_0$ is in U, i.e. that it does not contain f.

Suppose towards a contradiction that $f \in \langle p \rangle + P_0$. Since

$$(\frac{H_0 + \langle p \rangle}{h_0' + \langle p \rangle})(g + \langle p \rangle) + (\frac{H_1 + \langle p \rangle}{h_1' + \langle p \rangle})(f + \langle p \rangle) = 1 + \langle p \rangle,$$

for some H_0, H_1 in $R[X_n]$ and h_0', h_1' as above, our assumption implies that $f + \langle p \rangle \in P_0$. Thus

$$f + \langle p \rangle = \sum_j (G_j + \langle p \rangle)(g_j + \langle p \rangle)$$

for some $G_0, dots, G_m \in \mathbb{R}[X_n]$. In the last equation, using the expression for $g + \langle p \rangle$ in terms of the $g_j + \langle p \rangle$ in $F_p[X_n]$ and multiplying both sides by $\prod h_i \prod h_j$, we get that $\prod h_i \prod h_j$ as a linear combination of $g_0, \ldots, g_m$ with coefficients in $R[X_n]/\langle p \rangle$. This implies that the equivalence class of $\prod h_i \prod h_j$ modulo $\langle p \rangle$ is the same as the equivalence class of an element of P_0 modulo $\langle p \rangle$, which in turn means that $\prod h_i \prod h_j$ belongs to the ideal $P_0 + \langle p \rangle$ of $R[X_n]$. Since $\prod h_i \prod h_j$ belongs to R, it follows that it lies in $(P_0 \cap R) + (\langle p \rangle \cap R) = p_0 + p = p$, contradicting the hypothesis that $p \in W$. This proves the claim.

To finish the proof finish the proof write $\operatorname{Spec}(j_n)(U \cap C)$ as

$$\operatorname{Spec}(j_n)(U \cap C) = [\operatorname{Spec}(j_n)(U \cap C) \cap W] \cup [\operatorname{Spec}(j_n)(U \cap C) \cap W^c].$$

The first part of the union is a constructible set since $\operatorname{Spec}(j_n)(U \cap C) \cap W = C_{\operatorname{Spec}(j_n)(P_0)} \cap W$. For the second part notice that $\operatorname{Spec}(j_n)(U \cap C) \cap W^c = \operatorname{Spec}(j_n)(U \cap C \cap \operatorname{Spec}(j_n)^{-1}(W^c))$ and $P_0 \in C - \operatorname{Spec}(j_n)^{-1}(W^c)$, then, by our minimality assumption on C, $\operatorname{Spec}(j_n)(U \cap C) \cap W^c$ is constructible. $\square$

3.4 The generality of the result

Inspection of the proof above shows that the result is true, not just for $\mathbb{Z}[X_0, \ldots, X_n]$, but for $R[X_0, \ldots, X_n]$ where R is Noetherian. The case $R = K$, a field, is directly connected to logic.

3.5 Constructible sets as functors

Let C be a closed set in $\operatorname{Spec} \mathbb{Z}[X_0, \ldots, X_n]$, and L a field. Suppose $C = C_A$. Define $C(L) = \{\bar{\alpha} \in L^{n+1} : g(\bar{\alpha}) = 0, \forall g \in A\}$.

Lemma 22. *This does not depend on the choice of A, for $C(L) = \{\bar{\alpha} \in L^{n+1} : I(\bar{\alpha}|\mathbb{Z}) \in C\}$.*

Proof. Clear. □

C is to be construed as a syntax-free version of a finite conjunction of atomic formulas.

If U is the complement of C, define $U(L)$ as $L^{n+1} \setminus C(L)$, and in general, for Y constructible, define $Y(L)$ in the obvious way.

Lemma 23. *For fixed L, $Y \mapsto Y(L)$ is a homomorphism from the Boolean algebra of constructible subsets of $\operatorname{Spec} \mathbb{Z}[X_0, \ldots, X_n]$ to the Boolean algebra of constructible sets of L^{n+1} for the Zariski topology.*

Proof. Clear. □

Functoriality Each Y defines a functor from the category of fields to the category of sets. Most important is the cylindric aspect:

Let Y be constructible in $\operatorname{Spec} \mathbb{Z}[X_0, \ldots, X_n]$ and $\operatorname{Spec}(j_n)(Y)$ its constructible image in $\operatorname{Spec} \mathbb{Z}[X_0, \ldots, X_{n-1}]$. What is the connection between $Y(L) \subset L^{n+1}$, and $\operatorname{Spec}(j_n)(Y)(L) \subset L^n$?

Let $\pi_n : L^{n+1} \to L^n$ be the natural projection onto the first n coordinates.

Warning. $\pi_n(Y(L)) \neq \operatorname{Spec}(j_n)(Y)(L)$ in general.

Example. Let $n = 1$ and $Y = C\{X_0^2 + X_1^2 + 1\}$. Then $\operatorname{Spec}(j_1)(Y) = \operatorname{Spec} \mathbb{Z}[X_0]$. So, for $L = \mathbb{R}$, $\operatorname{Spec}(j_1)(L) = \mathbb{R}$. But $Y(L) = \emptyset \subset \mathbb{R}^2$.

Quantifier elimination is true for algebraically closed fields L, in the strong sense that

$$\pi_n(Y(L)) \neq \operatorname{Spec}(j_n)(Y)(L).$$

We still have to prove this. Our earlier theorem has no reference to *any* field.

Mild generalisation. In the preceding replace $\mathbb{Z}$ by a field K. Then you get functors from fields *extending* K to sets, in essentially the same way.

4 The important kinds of field extensions

4.1 Generalities

Fix $K \to L$. $\alpha \in L$ is *algebraic* over K if $I(\alpha|K) \neq 0$. In this case, $I(\alpha|K)$ is principal, generated by a unique monic polynomial. The elements of L algebraic over K form a subfield of L, the *relative algebraic closure* of K in L. If this is

L, $K \to L$ is said to be an *algebraic* extension. If α is algebraic over K, then $K(\alpha) = K[\alpha]$. If α is not algebraic over K, α is *transcendental*.

If $P \neq \{0\}$, $P \in \operatorname{Spec} K[X]$, then $K \to K[X]/P$ gives an algebraic extension with a zero of P (equivalently of its monic generator). An algebraic extension of an algebraic extension is algebraic, i.e. the algebraic extension of K form a category in an obvious way. The existence of algebraic L over K, with no proper algebraic extension, is clear by a limit argument. Again, a Zorn argument gives uniqueness up to isomorphism of this K^{alg}, the *algebraic closure* of K. K^{alg} satisfies the infinite list of axioms, one for each $n \geq 1$, which says that each monic polynomial of degree n has a root. Let ACF be the class of fields satisfying these axioms. $\mathbb{C}$ is of course the most visible example.

4.2 Separable algebraic extensions

Over K^{alg}, every monic element of $K[X]$ splits into linear factors, with the usual uniqueness. The inseparability phenomenon occurring only in nonzero characteristic, has to do with $f(X)$ irreducible over K but having a root of multiplicity grater than one in K^{alg}. In this case, f and its derivative f'_x have nontrivial gcd, unless $f'_x = 0$. But for f irreducible and $f'_x \neq 0$, there can be no nontrivial gcd on degree grounds. Thus $f'_x = 0$ and easily, $f(X) = g(X^p)$ for some irreducible $g \in K[X]$ and p the characteristic of K. An irreducible polynomial f is *separable* if f has no multiple roots. If f is not separable, then $f = g(X^{p^m})$ for a unique $m \geq 1$, and separable g.

$\alpha \in K^{\text{alg}}$ is *separable* over K if its minimal polynomial over K is separable. In characteristic 0, α is automatically separable. In characteristic p, if $\beta \in K$ is not a p power in K, $X^p - \beta$ is not separable. The elements of K^{alg} separable over K form a subfield K^{sep} containing K; we call it the *separable closure* of K. No element of $K^{\text{alg}} \setminus K^{\text{sep}}$ is separable over K^{sep}, indeed, each such element has a minimal polynomial of the form $X^{p^m} - \beta$.

Definition 24. An algebraic $K \to L$ is separable if every $\alpha \in L$ is separable over K.

The separable algebraic extensions of a fixed K form a category, with a distinguished extension $K \to K^{\text{sep}}$, unique up to isomorphism over K.

4.3 Tensor products and linear disjointness

Suppose $K \to L_1$ and $K \to L_2$ are field extensions. Each naturally gives L_i the structure of a K-algebra, and one has the tensor product $L_1 \otimes_K L_2$ of K-algebras. This may or may not be a domain. If it is, we say that the extensions are *linearly disjoint* over K. In that case, we have a natural field M in which the tensor product embeds, its field of fractions, and one easily sees that elements of L_1 linearly independent over K remain so over L_2(and the same with the roles of L_1 and L_2 reversed). Conversely, if we merely have some M where the natural $L_1 \otimes_K L_2$ embeds, then the $K \to L_i$ are linearly disjoint over K. Quite generally, in a commuting diagram, we say L_1 is linearly disjoint from L_2 over K if every set of elements of L_1 linearly independent over K remains so over L_2. This turns out to be symmetric ([3, page 360]).

4.4 K^{1/p^n} and K^{1/p^∞}

Suppose K has characteristic p. Then $x \to x^p$ is an embedding from K to itself. Inside K^{alg}, one has the subfield of all elements α such that $\alpha^{p^n} \in K$. This is K^{1/p^n}, and $K^{1/p^\infty} = \bigcup_{n \in N} K^{1/p^n}$. K is said to be *perfect* if and only if $K = K^{1/p}$, or equivalently, $K = K^p = \{\beta^p, \beta \in K\}$.

$\text{Aut}(K^{\text{alg}}|K)$ is the group of all automorphisms σ of K^{alg} fixing the elements of K. We have that K^{1/p^∞} is fixed pointwise by any such σ, and any element of $K^{\text{sep}} \setminus K$ can be moved by some σ. So, $\text{Aut}(K^{\text{alg}}|K) = \text{Aut}(K^{\text{sep}}|K)$.

4.5 General separability

Lemma 25. *Let $K \to L$ be an algebraic extension, where K and L are fields of characteristic p. Then the following are equivalent:*

1. *$K \to L$ is separable*
2. *$K \to L$ is linearly disjoint from $K \to K^{1/p}$ over K*
3. *$K \to L$ is linearly disjoint from $K \to K^{1/p^\infty}$ over K.*

Proof. Suppose that $K \to L$ is a separable extension, but not linearly disjoint from K^{1/p^∞}. Choose n minimal, and elements $\beta_0, \ldots, \beta_{n-1}$ in K^{1/p^∞} linearly independent over K but linearly dependent over L via $\sum \alpha_i \beta_i = 0$. Let $\sigma \in \text{Aut}(K^{\text{alg}}|K)$, then $\sum \sigma(\alpha_i)\beta_i = 0$. By minimality, $\alpha_i/\sigma(\alpha_i)$ is constant, so $\sigma(\alpha_i/\alpha_1) = \alpha_i/\alpha_1$ for any σ, so $\alpha_i/\alpha_1 \in K$, giving a linear dependence over K. Suppose $K \to L$ not separable, so get $\alpha \in L, \alpha \notin K, \alpha^p \in K$. So 1 and α are linearly independent over K but clearly linearly dependent over $K^{1/p}$. □

Definition 26. An extension $K \to L$, not necessarily algebraic, is called *separable* if and only if $K \to L$ and $K \to K^{1/p^\infty}$ are linearly disjoint over K.

We have then that $K \to L$ is separable if and only if $K \to L$ and $K \to K^{1/p}$ are linearly disjoint over K, and if K is perfect, then $K \to L$ is separable.

Exercise 6. Show that the definition does not depend on the $K \to K^{1/p^\infty}$.

Show that the composition of separable maps is separable.

4.6 Regular extensions

$K \to L$ is *regular* if it is linearly disjoint from $K \to K^{\text{alg}}$ over K.

Lemma 27. *If $K \to L$ is regular, then $K \to L$ is separable and K is relatively algebraically closed in L.*

Proof. Separability is clear since $K^{1/p^\infty} \subset K^{\text{alg}}$. Suppose that $\alpha \in L$ is algebraic over K, then $\dim_{K^{\text{alg}}}\{\alpha\} = 1$, so $\dim_K\{\alpha\} = 1$, so $\alpha \in K$. □

Theorem 28. *Suppose that $K \to L$ is separable, and $K \to L$ is relatively algebraically closed. Then $K \to L$ is regular.*

Proof. Since $K \to K^{1/p^\infty}$ is algebraic, $L \otimes_K K^{1/p^\infty}$ is a field by separability. Suppose that we have a minimal relation $\alpha_0 l_0 + \cdots + \alpha_{n-1} l_{n-1} = 0$, $\alpha_i \in K^{\text{alg}}$, $l_i \in L$, contradicting linear disjointness. By the usual Galois argument, the α_i can be chosen in $(L \otimes_K K^{1/p^\infty})^{1/p^\infty}$. Thus some power of each α_i is in L, but since K is relatively algebraically closed in L, this implies that each $\alpha_i \in K^{1/p^\infty}$, and this contradicts separability. □

Corollary 29. *A composition of regular maps is regular.*

4.7 Some logical points

1. An extension $K \to L$ is relatively algebraically closed if it preserves all the predicates $\text{Sol}_n(x_0, \ldots, x_{n-1})$, defined by: $\exists y(x_0 + x_1 y + \cdots + x_{n-1} y^{n-1} + y^n = 0)$.

2. An extension $K \to L$ is separable if it preserves all $D_{n,p}(x_0, \ldots, x_{n-1})$ where $p = \text{ch}(K)$ and $D_{n,p}$ is defined by $\exists y_0, \ldots, \exists y_{n-1} \neq 0(\sum y_j^p x_j = 0)$. This is easy, because, after taking p^{th} roots, this is what linear disjointness of $K \to L$ and $K \to K^{1/p}$ says.

We will look now at the basic Robinsonian model theory for the category of fields

1. for embeddings;

2. for regular maps;

3. for separable maps.

4.8

One basic idea is to characterise the various $K \to L$ in terms of the $I(\bar{\alpha}|K)$, where $\bar{\alpha} \in L^n$.

Exercise 7. 1. $K \to L$ is separable if and only if each such $I(\bar{\alpha}|K)$ remains prime over K^{1/p^∞}, i.e. $I(\bar{\alpha}|K) \cdot K^{1/p^\infty}$ is prime.

2. $K \to L$ is regular if and only if each $I(\bar{\alpha}|K)$ is absolutely prime, i.e. remains prime over K^{alg}.

5 *ACF* and *ECF*

5.1

We already defined *ACF*.

Definition 30. K is an *existentially closed field*, *ECF*, if, whenever a system of polynomial equalities and inequalities $g_1 = \cdots = g_k = 0$, $f_1 \neq 0, \ldots, f_l \neq 0$ over K has a solution in some $K \to L$ it has a solution in K.

Rabinovich trick At the cost of going to an extra variable t, and for solvability *in fields*, you can replace $f \neq 0$ by $tf = 1$. So in definition of ECF, one needs only positive conditions, and then we see:

Lemma 31. *K is ECF if and only if every element of* $\mathrm{Spec}(K[X])$ *has a point in K.*

Note that this characterisation leaves it not obvious whether ECF is an elementary condition.

Lemma 32. *$ECF \Rightarrow ACF$.*

Proof. If g is an irreducible polynomial in $K[X]$, then g has a root in $K[X]/(g)$, which is an extension of K. □

Conversely,

Theorem 33. *$ACF \Rightarrow ECF$.*

Proof. Suppose K is in ACF, consider a system $g_1 = \cdots = g_k = 0$; $f_1 \neq 0, \ldots, f_l \neq 0$. This defines a locally closed set X in $\mathrm{Spec}(K[x_0, \ldots, x_{n-1}])$, and $X \neq \emptyset$ if we assume as we now do, that the system can be solved in some $K \to L$. Now, without loss of generality, assume that $X = C \cap U$, where C is irreducible with generic P and $U = \{Q : f \notin Q\}$ for some fixed f.

Note the following: If $Q \in X$ is maximal in X, then Q is actually a maximal ideal. For if all proper $Q_1 \supsetneq Q$ contains f, then $f \in RadQ$, so $f \in Q$.

If $n = 1$, ACF clearly gives a K-point. So proceed by induction.

Let $j : K[x_0, \ldots, x_{n-2}] \to K[x_0, \ldots, x_{n-1}]$ as usual. Now $\mathrm{Spec}(j)(C \cap U) = \bigcup_{0 \leq j < m} C_j \cap U_j$ where the C_j are distinct irreducible closed sets, and U_j open. Now $\mathrm{Spec}(j)(P)$ is in exactly one C_j, say C_0, and is C_0-generic. By induction, $C_0 \cap U_0$ has a K-point $\bar{\beta} = (\beta_0, \ldots, \beta_{n-2})$. Let $I = I(\bar{\beta}|K)$. I is maximal, $\mathrm{Spec}(j)(P) \subset I$, $I \in U_0$. Now choose $J \in C \cap U$, $I = \mathrm{Spec}(j)(J)$, J maximal (by what we said above). So $P \subset J$. Consider $\Gamma = \{h(\bar{\beta}, x_{n-1}) : h \in J\} \subset K[x_{n-1}]$. Clearly, $1 \notin \Gamma$ since $1 \notin J$. Also, Γ is an ideal. It is even prime. For if $h_1(\bar{\beta}, x_{n-1})h_2(\bar{\beta}, x_{n-1}) = h(\bar{\beta}, x_{n-1})$, $h \in J$, then $(h - h_1)h_2 \in I[x_{n-1}] \subset J$, so $h_1 \in J$ or $h_2 \in J$. So, Γ is either $\{0\}$ (easy), or generated by an irreducible $g(x_{n-1}) = h(\bar{\beta}, x_{n-1})$, $h \in J$. Let β_{n-1} be a root of g in K and let $J_1 = I((b_0, \ldots, b_{n-1})|K)$. Suppose $h \in J$, then $h(\beta_0, \ldots, \beta_{n-2}, x_{n-1}) \in \Gamma$, so $h(\beta_0, \ldots, \beta_{n-1}) = 0$. By maximality, $J_1 = J$. Since $J \in C \cap U$, we are done. □

Corollary 34. *ECF is first order.*

Proof. Clear. □

Corollary 35. *Maximal ideals in $K[x_0, \ldots, x_{n-1}]$, where $K \in ACF$, are of the form $I(\bar{\beta}|K)$, $\bar{\beta} \in K^n$.*

Proof. We have already showed this in the proof of our last theorem. Again: if M is a maximal ideal of $K[x_0, \ldots, x_{n-1}]$, then M has a zero in $K[x_0, \ldots, x_{n-1}]/M$, so it has a K-point $\bar{\beta}$, since K is ECF. Let $M' = I(\bar{\beta}|K)$. $M \subset M'$, and it's the same ideal by maximality of M. So M is of the wanted form. □

Theorem 36. *ACF has quantifier elimination.*

Proof. It suffices to show the following: Let C be closed irreducible and U open in $\operatorname{Spec}\mathbb{Z}[x_0,\ldots,x_{n-1}]$, and $\bigcup_{0\leq j<m}(C_j\cap U_j)=\operatorname{Spec}(j)(C\cap U)$, with C_j closed and U_j open as usual. Let π be the projection from K^n onto K^{n-1} (to the first $n-1$ coordinates). Then $\pi((C\cap U)(K))=\bigcup_{0\leq j<m}(C_i\cap U_j)(K)$.

We have to prove that $\pi((C\cap U)(K))\supset\bigcup_{0\leq j<m}(C_i\cap U_j)(K)$, since the other inclusion is trivial. And for that, consider a j for which $C_j\cap U_j$ defines a nonempty set of $\operatorname{Spec}[x_0,\ldots,x_{n-2}]$. Let $\bar{\beta}\in C_j\cap U_j(K)$, and let $I=I(\bar{\beta}|\mathbb{Z})$. Now lift I to maximal $J\in C\cap U$. The argument in the preceding proof gives β_{n-1}, so $J=I((\beta_0,\ldots,\beta_{n-1})|\mathbb{Z})$, and $\bar{\beta}\in\pi((C\cap U)(K))$. □

Corollary 37. *If K,L are two algebraically closed fields, then $K\equiv L$ if and only if $\operatorname{ch}(K)=\operatorname{ch}(L)$.*

Proof. A sentence corresponds to a constructible set of $\operatorname{Spec}(\mathbb{Z})$. But basic open sets of $\operatorname{Spec}(\mathbb{Z})$ are defined by formulas of the form $n\cdot 1\neq 0$, which say that the characteristic is not n. □

Corollary 38. *ACF is strongly minimal.*

Proof. Suppose that $C\cap U$ is a locally closed set in $\operatorname{Spec}\mathbb{Z}[x_0,\ldots,x_{n-2},x_{n-1}]$, where C is closed irreducible and U an open set of the form $\{Q:f\notin Q\}$.

Let $K\models ACF$, and $\lambda_0,\ldots,\lambda_{n-2}\in K$. Let d_1 be the maximal x_{n-1}-degree of a generating set for the generic P of C, and d_2 be the x_{n-1}-degree of f. Then, either:

$$|(C\cap U)(K)\cap(\{(\lambda_0,\ldots,\lambda_{n-2})\}\times K)|\leq d_1$$

or

$$|K\setminus((C\cap U)(K)\cap(\{(\lambda_0,\ldots,\lambda_{n-2})\}\times K))|\leq d_2.$$

□

One can go on from here by pure model theory to get uncountable categoricity and other related properties.

We have not used the notion of transcendence degree. What is most important is to relate it to topological dimension.

Exercise 8.
1. Any individual finite field has quantifier elimination (this isn't trivial).
2. 1 and ACF exhaust the fields with quantifier elimination.

5.2 Lefschetz Principle

This concerns the set

$$\{P\in\operatorname{Spec}(\mathbb{Z}):\phi\text{ holds in all }K\in ACF\text{ with }\operatorname{ch}(K)=P\},$$

where ϕ is a first-order sentence. The Chevalley-Tarski result shows that this is a constructible in $\operatorname{Spec}(\mathbb{Z})$. More is true:

Lemma 39. *A constructible subset X of $\operatorname{Spec}(\mathbb{Z})$ is either:*

1. *a finite set of closed points, or,*
2. *a cofinite set containing (0).*

Proof. The point (0) belongs to every nonempty open set and the only closed set to which (0) belongs is Spec($\mathbb{Z}$). So (0) is generic. If C is closed and irreducible in Spec($\mathbb{Z}$) and contains more than one element then $C = \text{Spec}(\mathbb{Z})$. This is because the Krull dimension of Spec($\mathbb{Z}$) is one, so the generic point of C must be (0) if C contains more than one element. Since every nonempty open set is cofinite, for any set X of the form $C \cap U$, with C closed irreducible and U open, X is cofinite, if $C = \text{Spec}(\mathbb{Z})$, or, in the other case, X contains at most one element. Thus any constructible set, being a finite union of such sets, is finite or cofinite. □

Corollary 40. *A sentence ϕ holds in an algebraically closed field of characteristic 0 if and only if it holds in all algebraically closed fields of sufficiently large characteristic.*

5.3 More on absolute irreducibility

Theorem 41. *Suppose $K \to L$ and $K, L \in ACF$. Let P be a prime ideal in $K[x_0, \ldots, x_{n-1}]$. Then $P \cdot L[x_0, \ldots, x_{n-1}]$ is a prime ideal in $L[x_0, \ldots, x_{n-1}]$.*

Proof. Let $\bar{\alpha} \in K^n$ be a zero of P. Then $\bar{\alpha}$ is also a zero of $P.L[x_0, \ldots, x_{n-1}]$. If $g \in L[x_0, \ldots, x_{n-1}]$, $g(\bar{x}) - g(\bar{\alpha}) \in P.L[x_0, \ldots, x_{n-1}]$ (for if we write $g(\bar{x}) - g(\bar{\alpha})$ as a sum of monomials of the form $c_i.M_i$, where $c_i \in L$ and $M_i \in K[\bar{x}]$, we will have that $M_i \in P$ since $M_i(\bar{\alpha}) = 0$). So, if $g(\bar{\alpha}) = 0$, we will have that $g(\bar{x}) \in P.L[x_0, \ldots, x_{n-1}]$. Thus, $P.L[x_0, \ldots, x_{n-1}] = I(\bar{\alpha}|L)$, so it's prime. □

Corollary 42. *Let K be a field and $P \in \text{Spec}\, K[\bar{x}]$, then P is absolutely prime if and only if for any $K \to L$, $P \cdot L[\bar{x}]$ is prime.*

5.4 Definable sets and maps for ACF

Let $K \in ACF$. The definable subsets of K^n are the constructible subsets of subsets of K^n for the Zariski topology.

The definable maps $Y \to K^m$, where $Y \subset K^n$, are those whose graphs are definable subsets of K^{n+m}. Obviously, the case $m = 1$ is basic and other cases easily follow. Again obviously, the case to understand is that of a graph defined by $C \cap U$, C irreducible, U open in Spec $K[x_0, \ldots, x_{n-1}]$.

Let P be the generic of C, and consider the domain $D = K[x_0, \ldots, x_{n-1}]/P$, and the subdomain $D_0 = K[x_0, \ldots, x_{n-2}]/\text{Spec}(j)(P)$. There are two cases:

Case 1: $x_{n-1} + P$ is transcendental over D_0. $(x_0 + P, \ldots, x_{n-1} + P)$ and $(x_0 + P, \ldots, 1 + x_{n-1} + P)$ are distinct and in $C \cap U(D)$: it's clear for the first, and for the second let's take $P \in P$ and write $P(x_0, \ldots, x_{n-2}, x_{n-1}))$ as a polynomial in x_{n-1} with coefficients in Spec$(j)(P)$. Since this $x_{n-1} + P$ is a zero of this polynomial in D, and since x_{n-1} is transcendental over D_0, this polynomial has to be the zero polynomial. Now let K_1 be the algebraic closure of the field of fractions of D. Then, $K_1 \models C \cap U$ is not a graph, so $K \models C \cap U$ is not a graph. So Case 1 is impossible.

Case 2: $x_{n-1} + P$ **is algebraic over** D_0**.** There are three subcases:

1. If $x_{n-1} + P$ is in the fraction fields of D_0: we treat this subcase later.

2. Not subcase 1, but $x_{n-1} + P$ is algebraic and separable over the fraction field of D_0. This cannot happen, as we see by Galois Theory, if we take a conjugate of $x_{n-1} + P$ over the fraction field of D_0 and proceed as in case1, we'll see that $C \cap U$ can't be the graph of a function.

3. $x_{n-1} + P$ is not separable, unless it is purely inseparable. An argument like the one of subcase 2 gives a contradiction.

   So for some m, $x_{n-1}^{p^m} + P$ is an element of the fraction field of D_0.

Now the common feature of the subcases 1 and 3 is that for some $m \geq 0$ and $f(x_1, \ldots, x_{n-1})$ and $g(x_1, \ldots, x_{n-1}) \in K(x_1, \ldots, x_{n-1}), g \notin P$, $g.x_{n-1}^{p^m} - f \in P$ (where, if $p = 0, m = 0$ and $0^0 = 1$). Now let $C_1 \subset C$ consist of the Q with $g \in Q$. Clearly, on $C \cap U \cap (C \setminus C_1)$, our graph is the graph of $(f/g)^{-p^m}$. We can then handle $C_1 \cap U$ by induction.

This proves:

Theorem 43. *Let K be in ACF. A definable function on a subset of K^n is a finite union of functions which on definable sets are of the form $(f/g)^{(1/p^m)}$ with f and g polynomials.*

5.5 "Ax" theorem

Theorem 44. *Let K be in ACF. Let X be a definable subset of K^n, and $f : X \to X$ a definable map. If f is injective, f is surjective.*

Proof. If not, consider any counterexample (X, f), X defined by a formula $\phi(v_0, \ldots, v_{n-1}, k_0, \ldots, k_{m-1})$, where ϕ is constructible over $\mathbb{Z}$ and $k_j \in K$, and suppose that the graph of f is defined by $\psi(v_0, \ldots, v_{n-1}, w_0, \ldots, w_{n-1}, l_0, \ldots, l_{r-1})$ with ψ constructible over $\mathbb{Z}$ and $l_j \in K$. Consider any $\bar{k}, \bar{l}$, such that ψ defines the graph of an injective non-surjective function f on the corresponding X. There must be a prime p so that there are such $\bar{k}, \bar{l}$ in $\mathbb{F}_p^{\text{alg}}$. But then, $\bar{k}, \bar{l}$ lie in some $\mathbb{F}_{p^{s_0}}$. Since each finite field is perfect, the preceding theorem shows that for some $s_1 \geq s_0$ and all $s \geq s_1$, f maps $X(\mathbb{F}_{p^s})$ to $X(\mathbb{F}_{p^s})$. But it is clearly surjective on these finite sets, so also on $X(\mathbb{F}_p^{\text{alg}})$, and we get the desired contradiction. □

6 Separably Closed Fields

6.1

A field K is *separably closed* if it has no separable extensions, i.e $K = K^{\text{sep}}$. Let us fix a prime p, and for now consider only K of characteristic p (but our discussion will be uniform in p). The class of separably closed fields is a first order class: K is separably closed if and only if every irreducible polynomial in $K[x]$ is not prime with its derivative.

6.2 p-dependence, p-basis, Ershov invariants

In 4.7, we observed that $K \to L$ is a separable extension if and only if it preserves the predicates $D_{n,p}(x_0, \ldots, x_{n-1})$, where $p = \mathrm{ch}(K)$, expressing that $x_0, \ldots, x_{n-1}$ are linearly independent over the field of p^{th} powers. The (linear) dimension of K over K^p is a basic invariant, algebraically and model theoretically.

Lemma 45. *If* $\dim(K/K^p)$ *is finite, it is of the form* p^m.

Proof. Suppose $K \neq K^p$. Choose $\alpha \notin K^p$. Then, $1, \alpha, \alpha^2, \ldots, \alpha^{p-1}$ are linearly independent over K^p. For if not, say $c_0^p + c_1^p.\alpha + \cdots + c_{p-1}^p.\alpha^{p-1} = 0$. So, $c_0 + c_1^p.\beta + \cdots + c_{p-1}.\beta^{p-1} = 0$ where $\beta^p = \alpha, \beta \notin K$. But $X^p - \alpha$ is irreducible (because this polynomial is equal to $(X - \beta)^p$, which does not have any non trivial divisor in $K[X]$). Thus, $X^p - \alpha$ is the minimal polynomial of β over K, so all the c_i are zero. Then, $\dim(\alpha|K^p) \geq p$, but $\alpha^p \in K^p$, so $\dim(\alpha|K^p) = p$ (we mean by $\dim(\alpha|K^p)$, the linear dimension of the field $K[\alpha]$ over K^p).

Now if $\alpha_1 \notin K^p[\alpha] = K_1$, and suppose for a contradiction that $\dim(\alpha_1|K_1) = q < p$. Then, $\alpha_1^q \in K_1$, and since $\alpha_1^p \in K_1$ and p and q are relatively prime, we obtain by Bezout's theorem in arithmetic, that $\alpha_1 \in K_1$, which is not possible. We have then by basic linear algebra that $\dim(K^p[\alpha, \alpha_1]|K^p) = \dim(K_1^p[\alpha_1]|K_1) \cdot \dim(K_1|K^p) = p^2$. And so on, we may continue to prove that if our process needs at least m steps to have $K^p[\alpha_1, \ldots, \alpha_n] = K$, then $\dim(K|K^p) = p^m$. □

If the $(\alpha_i)_{i \in I}$ are, as above, elements of K linearly independent modulo K^p, and such that $K_p[(\alpha_i)_{i \in I}] = K$, we call *p-basis* of K, the family of monomials in $(\alpha_i)_{i \in I}$ of degree $< p$. The cardinality of this family is $p^{card(I)}$. p-bases always exist, by a Zorn argument. Note that the cardinal of a p-basis of K is the linear dimension of K over K^p. So if $\dim(K|K^p)$ is finite, then all the p-basis have the same cardinal. Suppose that $\dim(K|K^p)$ is infinite, and let X be a p-basis. So X is infinite, and $|X|$ is the dimension of the vector space K over K^p. So, by the properties of the dimension on vector spaces, two infinite p-bases of K have the same cardinal.

This leaves the existence problem for *p-dimensions*: which occur?

Lemma 46. *Let* X *be a set of algebraically independent elements over* $\mathbb{F}_p$. *Let* $K = \mathbb{F}_p(X)$. *Then the p-dimension of* K *is* $p^{card(X)}$ *if* $card(X)$ *is finite, and* $card(X)$ *if* $card(X)$ *is infinite.*

Proof. $K^p = \mathbb{F}_p(Y)$ where Y consists of the p^α powers of elements of X. Thus it is clear that the reduced monomials in X of degree $\leq p - 1$ span K over K^p (observe that if $g \in \mathbb{F}_p[X], g \neq 0$, then $\frac{1}{g} = (\frac{1}{g})^p.g^{p-1}$, and so, one gets a spanning set from inside $\mathbb{F}_p[X]$). It is obvious that a linear dependence of the reduced monomials in X, over $\mathbb{F}_p(Y)$ would give an algebraic dependence between the X over $\mathbb{F}_p$. □

Now ask: Which p-dimensions occur for K separably closed? In fact, all of those in the preceding lemma.

Lemma 47. *Suppose* $K \to L$ *separable.*

1. *If* $X \subset K$ *is p-independent in* K, *it remains p-independent in* L.

2. If in addition L is algebraic over K, then $p-\dim(K) = p-\dim(L)$

Proof. 1. Direct from 4.7

2. Obviously, it is sufficient to prove this when $[L : K] < \omega$. Consider the extensions $K^p \to K \to L$ and $K^p \to L^p \to L$, and compute dimensions. Clearly, $[L : K] = [L^p : K^p]$, so $[L : L^p] = [K : K^p]$.

□

So if K is a field of p-dimension n and if L is the separable closure of K, then K and L satisfy the conditions of the second part of the preceding lemma, so, $[L : L^p] = n$. Which proves that all the described p-dimensions can occur for separably closed fields.

Definition 48 (Ershov invariant)**.** Suppose K is separably closed. The *Ershov invariant* of K is the p-dimension of K if this is finite, and ∞ otherwise. The Ershov invariant is of the form p^ν, where p is the characteristic. ν will be called the *imperfection degree* of K.

Theorem 49 (Ershov, 1960's)**.** *Two separably closed fields are elementarily equivalent if and only if they have the same characteristic and the same Ershov invariant.*

This requires preparation.

Lemma 50. *1. The property of having a specific finite Ershov invariant is axiomatisable by a single sentence of field theory.*

2. The property of having infinite Ershov invariant is axiomatisable by a set of sentences, but not by a single sentence.

Proof. 1. We just have to know how to say with a first order sentence that the imperfection degree of a field K is ν. It is axiomatised by:

$$\exists b_1, \ldots, \exists b_\nu \forall x (\exists! x_j)_{j \in p^\nu} x = \sum x_j^p m_j(b_1, \ldots, b_\nu),$$

where the m_j are the monomials in ν variables with leading coefficient 1.

2. Clear by compactness and the fact that there are fields of finite and arbitrarily large Ershov invariant.

□

Now recall from 4.7 that separable extensions are exactly those preserving the $D_{n,p}$. In particular, an extension $K \to L$ of fields cannot be elementary unless it is separable. Ershov showed that separable extensions $K \to L$ of fields with the same Ershov invariant are elementary. We shall now prove this.

6.3 Transcendence Bases

Consider any $K \to L$ extension, and $\bar{\alpha} \in L^n$, $\bar{\alpha} = (\alpha_1, \ldots, \alpha_n)$. The α_i are *K-independent* if $I(\bar{\alpha}|K) = (0)$, otherwise they are *K-dependent*. A subset X of L is *K-independent* if all its finite subsets are independent. Similarly for K-dependence.

A *transcendence base* for L over K is a K-independent X such that $K(X) \to L$ is algebraic. Transcendence bases exist by Zorn, and they have the same cardinality by the exchange principle, which holds in algebraically closed fields. In fact, all this follows by strong minimality of ACF, purely model-theoretically.

The uncountable categoricity of ACF comes from the uniqueness of cardinality of transcendence base, and uniqueness of algebraic closure.

We now assess the situation for separably closed fields.

6.4 Separating Transcendence Bases

Definition 51. $X \subset L$ is a *separating transcendence base* for $K \to L$ if X is a transcendence base and $K(X) \to L$ is separable algebraic.

Note that separating transcendence bases exist only for separable extensions, but not all separable extensions have a separating transcendence base: For any prime number p, take the field extension $\mathbb{F}_p^{\text{alg}} \to \mathbb{F}_p^{\text{alg}}((X^{1/p^n})_{n\in\mathbb{N}})$, where X is transcendental over $\mathbb{F}_p^{\text{alg}}$. It is clear that it is a separable extension, since it is purely transcendental, but one can easily see that it doesn't have any separating transcendence base.

Theorem 52 (McLane)**.** *If L is a separable extension of K, and is finitely generated, then a separating transcendence base can be selected from any given set of generators.*

Proof. Assume that L is finitely generated over K, say $L = K(x) = K(x_1, \ldots, x_n)$. Let the transcendence degree of this extension be r. If $r = n$, the proof is complete. Otherwise, say $x_1, \ldots, x_r$ is a transcendence base. Then x_{r+1} is algebraic over $K(x_1, \ldots, x_r)$. Let $f(X_1, \ldots, X_{r+1})$ be a polynomial of lowest degree such that $f(x_1, \ldots, x_{r+1}) = 0$. Then f is irreducible. We contend that not all $x_i (i = 1, \ldots, r+1)$ appear to the p^{th}-power throughout. If they did, we could write $f(X) = \sum c_\alpha M_\alpha(X)^p$ where $M_\alpha(X)$ are monomials in $X_1, \ldots, X_{r+1}$ and $c_\alpha \in K$. This would imply that $M_\alpha(x)$ are linearly dependent over $K^{1/p}$ (taking the p^{th}-root of the equation $\sum c_\alpha M_\alpha(x)^p) = 0$). However the $M_\alpha x$ are linearly independent over K (otherwise we could get an equation for $x_1, \ldots, x_{r+1}$ of lower degree) and we thus get a contradiction to the linear disjointness of L and $K^{1/p}$ (which we have by the separability of the extension $K \to L$). Say X_1 does not appear to the p^{th}-power throughout but actually appears in $f(X)$. We know that $f(X)$ is irreducible in $K[X_1, \ldots, X_{r+1}]$ and hence $f(x) = 0$ is an irreducible equation for x_1 over $x_2, \ldots, x_{r+1}$. Since X_1 does not appear through the p^{th}-power throughout, this equation is a separable equation for x_1 over $K(x_2, \ldots, x_{r+1})$, in other words, x_1 is separable algebraic over $K(x_2, \ldots, x_{r+1})$. From this it follows that is is separable algebraic over $K(x_2, \ldots, x_n)$. If $(x_2, \ldots, x_n)$ is a transcendence base, the proof is complete. If not, say x_2 is separable over $K(x_3, \ldots, x_n)$. Then L is separable over $K(x_3, \ldots, x_n)$. Proceeding inductively, we see that the procedure can be continued until we get down to a transcendence base. This proves our theorem. □

Theorem 53 (McLane)**.** *$K \to L$ is separable if and only if every finitely generated subfield of L has a separating transcendence base.*

Proof. If $K \to L$ is separable, then every finite subextension of $K \to L$ is separable and by the preceding theorem, it has a separating transcendence base. Reciprocally, suppose that $K \to L$ is not separable, then there is a finite subextension $K \to L'$ of $K \to L$ which is not separable, and easily cannot have a separating transcendence base (since separating transcendence bases exist only for separable extensions, by transitivity of separable extensions). □

Let SCF be the theory of separably closed fields. Its completions are:

- $ACF_0 = SCF + (char = 0)$, and
- $SCF_{p,\nu} = SCF + (\text{ch} = p) + (\text{imperfection degree} = \nu)$,

for each prime p and $\nu \in \mathbb{N} \cup \{\infty\}$. We will prove below the completeness of $SCF_{p,\nu}$ for finite $\nu > 0$ and $p > 0$, and ACF_0 and $SCF_{p,0}$ are theories of algebraically closed fields of given characteristic, and are known to be complete.

From now on, we fix $p > 0$ and ν finite $\neq 0$.

Theorem 54. *Each theory $SCF_{p,\nu}$ is complete.*

Proof. When studying inclusion of one model in another, we are interested in elementary extensions, hence in our case separable extensions. Because ν is finite, a p-basis of K is still a p-basis of any $L \succeq K$. This justifies adding to the language constants for the elements of a p-basis. Let us prove that in the language $\{0, 1, +, -, .\} \cup \{b_1, \ldots, b_\nu\}$, the theory $SCF_{p,\nu}$+" the reduced monomial in $\{b_1, \ldots, b_\nu\}$ form a p-basis", axiomatised as $\forall x(\exists! x_j)_{j \in p^\nu} x = \sum x_j^p m_j(b_1, \ldots, b_\nu)$, is model complete and has a prime model. This will prove the completeness ([1, 3.1.9]).

Since $b_1, \ldots, b_\nu$ are algebraically independent over $\mathbb{F}_p$, the field $\mathbb{F}_p(b_1, \ldots, b_\nu)^s$ is uniquely determined and embeds in every model. Now by the claim below, any model is existentially closed in any model extension, this proves the model completeness ([1, 3.1.7]).

□

Claim. Let $K \models SCF_{p,\nu}$ and let L be a separable extension of K. Then L K-embeds in some elementary extension of K.

Proof. It is enough to prove it for L finitely generated over K. By McLane's theorem, such an L admits a separating transcendence basis $l_1, \ldots, l_n$ over K. But any $|K|^+$-saturated elementary extension K^* of K has infinite transcendence degree over K, therefore $K(l_1, \ldots, l_n)$ K-embeds in K^*, and $K(l_1, \ldots, l_n)^s$ also since K^* is a model, hence so does L. □

References

[1] C. C. Chang and H. J. Keisler. *Model theory*, volume 73 of *Studies in Logic and the Foundations of Mathematics*. North-Holland Publishing Co., Amsterdam, third edition, 1990.

[2] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[3] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.