# NOTES ON APPLIED STABILITY THEORY

L. VAN DEN DRIES

## 1. Introduction

The possibility of applying model theory outside logic was pioneered by Tarski, Mal'cev, and A. Robinson in the forties and fifties. This involved just the most basic ideas and notions of model theory, like compactness, quantifier elimination, and preservation theorems, and led to results such as the Lefschetz Principle for algebraically closed fields and its analogue for real closed fields, and hence to more concrete applications like those by Robinson to Hilbert's 17th problem and algebraically closed valued fields. Of course, it required great insight to realize that simple ideas of this nature could be useful at all, and familiarity with this development is recommended.

To this very limited arsenal the sixties and seventies added the systematic use of saturation and ultraproducts, and of the Robinsonian notions

*model completion* and *existentially closed model*.

The main new application in the sixties was the spectacular work by Ax-Kochen and Ersov, with non-standard analysis also attracting attention. In the seventies Macintyre and Denef extended the range of applications by focusing on the structure of definable sets, in $p$-adic fields in their case, rather than dealing only with sentences as in most earlier work. This change of focus was a key inspiration for introducing o-minimal structures in the next decade, when new interactions with pure model theory occurred.

In the mean time pure model theory had undergone a deep transformation, starting with Morley's seminal proof of his categoricity theorem in the sixties. To deal with the related issue of how many models of a given size a countable theory can have, Shelah and others developed a rather massive machinery, called *stability theory.* In this way Shelah discovered some highly robust dividing lines among theories, and these dichotomies have turned out to be also of great significance for the study of definable sets. With additional influence of work by Baldwin-Lachlan and programmatic ideas of Zilber, people began a systematic investigation of the underlying pregeometries of stable structures and the groups that can be defined in such structures; this direction goes under the name of *geometric stability theory.* This huge internal model-theoretic development was unrelated to the concerns of applied model theory as discussed earlier. Over the last

*Date*: February 2007.

twenty years, however, Hrushovski has achieved a remarkable synthesis of these two streams of model theory by connecting geometric stability theory to diophantine questions. Key words on the diophantine side:

*Mordell-Lang* and *Manin-Mumford*.

One meeting ground is the subject of differentially closed fields. These objects were invented by Robinson around 1960, but their deeper algebraic and model-theoretic properties were established by means of stability theory.

In these notes we shall deal with algebraically closed fields and differentially closed fields, with emphasis on model-theoretic aspects, develop some elementary algebraic geometry (partly in the context of noetherian spaces and zariski-structures), and some model theory of groups. Towards the end we shall use this to give the Pillay-Ziegler proof of the Mordell-Lang property for function fields in characteristic zero.

**Notation and terminology.** Model-theoretic notations and terminology are as in my notes *Introduction to model-theoretic stability.* If $\mathcal{M}$ and $\mathcal{N}$ are structures for the same one-sorted language, then $\mathcal{M} \subseteq \mathcal{N}$ means that $\mathcal{M}$ is a substructure of $\mathcal{N}$.

By "ring" we mean "commutative ring with 1" unless we explicitly allow otherwise. Rings are viewed as structures for the language $\{0, 1, -, +, \cdot\}$ of rings, and terms like "ring (homo)morphism" and "subring" are used in that sense. Given a ring $R$ and $a_1, \dots, a_n \in R$ we let $(a_1, \dots, a_n)R$ (or $(a_1, \dots, a_n)$ if $R$ is clear from the context) denote the ideal $a_1R + \cdots + a_nR$ of $R$ generated by $a_1, \dots, a_n$. Given a ring $R$ we let $R[T_1, \dots, T_n]$ be the ring of polynomials in distinct indeterminates $T_1, \dots, T_n$ with coefficients from $R$, and if $f \in R[T_1, \dots, T_n]$ is presented in the form $\sum_{\boldsymbol{i}} a_{\boldsymbol{i}} T^{\boldsymbol{i}}$ it is understood that $\boldsymbol{i} = (i_1, \dots, i_n)$ ranges over $\mathbb{N}^n$, that the coefficients $a_{\boldsymbol{i}}$ belong to $R$, with $a_{\boldsymbol{i}} \neq 0$ for only finitely many $\boldsymbol{i}$, and that $T^{\boldsymbol{i}} := T_1^{i_1} \cdots T_n^{i_n}$. If $R$ is a subring of a ring $S$ and $f \in R[T_1, \dots, T_n]$, a *zero* of $f$ in $S$ is a point $b \in S^n$ such that $f(b) = 0$. I recommend Lang's *Algebra* for algebraic notions and results that are used but not explained in the present notes.

An *algebra* on a set $X$ is a subalgebra of the boolean algebra of all subsets of $X$. Given a collection $\mathcal{C}$ of subsets of a set $X$, a *boolean combination of sets of* $\mathcal{C}$ *inside* $X$ is an element of the algebra on $X$ generated by $\mathcal{C}$.

For sets $X, Y$ we write $X \subset Y$ or $Y \supset X$ to indicate that $X$ is a *proper* subset of $Y$. Given subsets $C, C_1, \dots, C_n$ of a set $X$ we say that $C_1, \dots, C_n$ *cover* $C$ if $C \subseteq C_1 \cup \cdots \cup C_n$. By *space* we shall mean *topological space*. Given an ambient space $X$ and $P \subseteq X$ we let $\mathrm{cl}(P)$ and $\mathrm{int}(P)$ be the closure and interior of $P$ in $X$.

## 2. Algebraically closed fields

We establish here the basic model-theoretic facts about algebraically closed fields: elimination of quantifiers, the Nullstellensatz, perfect subfields as definably closed sets, definable functions, strong minimality, Morley rank = transcendence degree, and elimination of imaginaries.

Throughout this section we let $K$, $E$ and $F$ denote fields, and until further notice "algebraic over", "algebraically closed", and "algebraic closure" are taken in the sense of field theory; as we shall see, these notions agree in the context of algebraically closed fields with the model-theoretic notions. By ACF we mean here the theory of algebraically closed fields in the language of rings, and for $p$ a prime number or $p = 0$ we let $\mathrm{ACF}(p)$ be the theory of algebraically closed fields of characteristic $p$. In this section $p$ ranges over the set $\{0, 2, 3, 5, \dots\}$ of possible characteristics.

We assume the reader knows from Algebra that any field $K$ has an algebraic closure $K^{\mathrm{a}}$, that is, $K^{\mathrm{a}}$ is an algebraically closed overfield of $K$ and algebraic over $K$; these properties determine $K^{\mathrm{a}}$ up to isomorphism over $K$ (but $K^{\mathrm{a}}$ has usually many automorphisms over $K$). Any embedding of $K$ into an algebraically closed field $E$ can be extended to an embedding of $K^{\mathrm{a}}$ into $E$. If $E$ is an algebraically closed extension of $K$, then there is a unique field $K'$ such that $K \subseteq K' \subseteq E$ and $K'$ is an algebraic closure of $K$, namely

$$K' = \{a \in E : \ a \text{ is algebraic over } K\}$$

and we shall call this $K'$ the *algebraic closure of $K$ in $E$*. We also assume familiarity with algebraic independence and transcendence bases.

The "oldest" algebraically closed field is of course the field $\mathbb{C}$ of complex numbers, but the importance of $\mathbb{C}$ derives also from its amazing analytic structure. Other algebraically closed fields of independent interest are the algebraic closures of the finite fields $\mathbb{F}_p$ and of $\mathbb{Q}$. Model theory suggests, however, that we can profit by working in an elementary class of structures, even if our aim is to understand just a single model in this class.

**Quantifier Elimination.** We shall use the following QE-test:

**Lemma 2.1.** *Let $T$ be a one-sorted theory. Then* (1) $\Leftrightarrow$ (2)*:*

(1) *$T$ admits* QE*;*
(2) *whenever $\mathcal{M} = (M; \dots)$ and $\mathcal{N} = (N; \dots)$ are models of $T$ such that $\mathcal{N}$ is $|M|^+$-saturated, and $\mathcal{A}$ is a proper substructure of $\mathcal{M}$ and $\phi : \mathcal{A} \to \mathcal{N}$ is an embedding, then $\phi$ extends to an embedding of a strictly larger substructure of $\mathcal{M}$ into $\mathcal{N}$.*

Of course, in (2) one can iterate the extension process and extend $\phi$ to an embedding of $\mathcal{M}$ into $\mathcal{N}$.

**Theorem 2.2.** ACF *has* QE*, and* $\mathrm{ACF}(p)$ *is complete for each $p$.*

*Proof.* Let $E$ and $F$ be algebraically closed fields such that $F$ is $|E|^+$-saturated, and let $R$ be a proper subring of $E$ and $\phi : R \to F$ an embedding. If $R$ is not a field we can extend $\phi$ to its fraction field inside $E$. So assume $R$ is a field. If $R$ is not algebraically closed, we can extend $\phi$ to the algebraic closure of $R$ in $E$. So we can assume $R$ is an algebraically closed field. Take any $a \in E \setminus R$. Then $f(a) \neq 0$ for all nonzero polynomials $f(T) \in R[T]$, that is, $a$ is transcendental over $R$. By saturation we can take $b \in F$ transcendental over the subfield $\phi(R)$ of $F$. Then $\phi$ extends to an embedding $R[a] \to F$ sending $a$ to $b$. This proves that ACF has QE. The second part of the theorem now follows since for $p > 0$ the field $\mathbb{F}_p$ embeds into every model of ACF($p$), and the ring $\mathbb{Z}$ embeds into every model of ACF(0). $\square$

The substructures of algebraically closed fields are exactly the domains, so by the above, ACF is the model completion of the theory of domains.

The following consequences of QE make up the *Constructibility Theorem* (Tarski-Chevalley) and the *Nullstellensatz* (Hilbert).

**Corollary 2.3.** *Let $E$ be an algebraically closed field with subfield $K$.*

(1) *The subsets of $E^n$ definable over $K$ in $E$ are exactly the boolean combinations inside $E^n$ of the zerosets*

$$\{a \in E^n : \ f(a) = 0\}, \qquad (f \in K[T_1, \dots, T_n]).$$

(2) *If $f_1, \dots, f_k, g_1, \dots, g_l \in K[T_1, \dots, T_n]$ and there is an overfield $F$ of $K$ with a point $a \in F^n$ such that*

$$f_1(a) = \cdots = f_k(a) = 0, \ g_1(a) \neq 0, \dots, g_l(a) \neq 0,$$

*then there is such a point $a \in E^n$.*

(3) *Let $g_1, \dots, g_m \in K[T_1, \dots, T_n]$. Then $g_1, \dots, g_m$ have no common zero in $E$ if and only if there are $f_1, \dots, f_m \in K[T_1, \dots, T_n]$ such that $f_1 g_1 + \cdots + f_m g_m = 1$ (in $K[T_1, \dots, T_n]$).*

(4) *the maximal ideals of $E[T_1, \dots, T_n]$ are exactly the ideals*

$$(T_1 - a_1, \dots, T_n - a_n)E[T_1, \dots, T_n], \quad (a_1, \dots, a_n \in E).$$

*Proof.* Item (1) is immediate from QE. In (2), extend $F$ to be algebraically closed, and use that then by QE we have $E \equiv_K F$. In (3), suppose there are no $f_1, \dots, f_m \in K[T_1, \dots, T_n]$ such that $f_1 g_1 + \cdots + f_m g_m = 1$. Then the ideal of $K[T_1, \dots, T_n]$ generated by $g_1, \dots, g_m$ is a proper ideal, and thus contained in a maximal ideal $\mathfrak{m}$ of $K[T_1, \dots, T_n]$. Then $\mathfrak{m} \cap K = \{0\}$, so

$$K[T_1, \dots, T_n]/\mathfrak{m} = K[t_1, \dots, t_n], \quad (t_i := T_i + \mathfrak{m}, \ i = 1, \dots, n)$$

is a field extension of $K$, and $g(t_1, \dots, t_n) = g(T_1, \dots, T_n) + \mathfrak{m}$ for each $g \in K[T_1, \dots, T_n]$, in particular, $g_1, \dots, g_m$ have $(t_1, \dots, t_n)$ as a common zero in an extension field of $K$, and thus $g_1, \dots, g_m$ have a common zero in $E$ by (2).

As to (4), let $R$ be a ring and $a = (a_1, \dots, a_n) \in R^n$, and consider the kernel of the ring morphism

$$f \mapsto f(a) : \ R[T_1, \dots, T_n] \to R.$$

We claim this kernel is $(T_1 - a_1, \dots, T_n - a_n)R[T_1, \dots, T_n]$. The latter ideal is certainly part of the kernel. Let $f \in R[T_1, \dots, T_n]$ and rewrite $f$ as a polynomial in $T_1 - a_1, \dots, T_n - a_n$, so $f = f^*(T_1 - a_1, \dots, T_n - a_n)$ with $f^* \in R[T_1, \dots, T_n]$. If $f$ is in the kernel, then $f(a) = f^*(0) = 0$, so $f^*$

has constant term zero, that is, $f^* \in (T_1, \dots, T_n)R[T_1, \dots, T_n]$, and thus $f \in (T_1 - a_1, \dots, T_n - a_n)R[T_1, \dots, T_n]$. If $R$ is a field, the surjectivity of the substitution morphism above shows that its kernel is a maximal ideal of $R[T_1, \dots, T_n]$. It remains to show that for $R = E$ this gives all maximal ideals of $E[T_1, \dots, T_n]$. Let $\mathfrak{m}$ be a maximal ideal of $E[T_1, \dots, T_n]$ and let $g_1, \dots, g_m$ generate this ideal. (By Hilbert's basis theorem there is a finite set of generators.) By (3) we have a common zero $a = (a_1, \dots, a_n) \in E^n$ of $g_1, \dots, g_m$ and then $a$ is a zero of all polynomials in $\mathfrak{m}$, so by our earlier consideration we have $\mathfrak{m} \subseteq (T_1 - a_1, \dots, T_n - a_n)E[T_1, \dots, T_n]$. By the maximality of $\mathfrak{m}$ this inclusion is an equality. □

**Exercise.** Typical Robinsonian uses of model-theoretic compactness + QE yield the existence of uniform bounds in (2) and (3) above:

(i) Given an upper bound $d \in \mathbb{N}$ on the degrees of $f_1, \dots, f_k, g_1, \dots, g_l$ in (2), there is $A = A(d, k, l, n) \in \mathbb{N}$ such that if the system of equations and inequations in (2) has a solution in $E$, then it has a solution in an intermediate field $K'$, $K \subseteq K' \subseteq E$, with $[K' : K] \leq A$.

(ii) Given an upper bound $d \in \mathbb{N}$ on the degrees of $g_1, \dots, g_m$ as in (3), there is $B = B(d, m, n) \in \mathbb{N}$ such that if $g_1, \dots, g_m$ have no common zero in $E$, then there are $f_1, \dots, f_m \in K[T_1, \dots, T_n]$ of degree $\leq B$ such that $f_1 g_1 + \cdots + f_m g_m = 1$.

(Here "$A = A(d, k, l, n)$" indicates that $A$ depends only on $d, k, l, n$, not on $K$ or the particular polynomials involved, and likewise with "$B = B(d, m, n)$". One can even take $A = A(d, l, n)$ and $B = B(d, n)$.)

**Definable closure.** If $E$ is algebraically closed with subset $S$, then the definable closure $\operatorname{dcl}(S)$ of $S$ in $E$ contains at least the subfield of $E$ generated by $S$, and equals (the underlying set of) this subfield when $E$ has characteristic zero:

**Proposition 2.4.** *Let $E$ be algebraically closed of characteristic zero, with subfield $K$. Then $K$ is definably closed in $E$.*

*Proof.* Let $a \in E \setminus K$; we claim that then $fa \neq a$ for some $f \in \operatorname{Aut}(E|K)$. (It is clear that the proposition follows from this claim.) If $a$ is transcendental over $K$, take a transcendence basis $B$ of $E$ over $K$ with $a \in B$, take the automorphism of $K(B)$ over $K$ that sends each $b \in B$ to $b + 1$, and then extend this automorphism to an automorphism of the algebraic closure $E$ of $K(B)$. Suppose $a$ is algebraic over $K$. Since $a \notin K$, the minimum polynomial of $a$ over $K$ is of degree $> 1$, so has a zero $b \in E$ with $b \neq a$ (here we use that $E$ has characteristic zero). Take an automorphism $\sigma$ of the algebraic closure $K^{\mathrm{a}}$ of $K$ in $E$ over $K$ that sends $a$ to $b$, take a transcendence basis $B$ of $E$ over $K^{\mathrm{a}}$, and extend $\sigma$ to the automorphism of $K^{\mathrm{a}}(B)$ that is the identity on $B$, and then extend further to an automorphism of $E$. □

Characterizations of definable closures of this type lead to corresponding descriptions of definable functions. In this case definable functions are piecewise rational functions:

**Corollary 2.5.** *Let $E$ be algebraically closed of characteristic zero, with subfield $K$, and let $X \subseteq E^n$ and $f : X \to E$ be $K$-definable in $E$. Then there are $g_1, \dots, g_k, h_1, \dots, h_k \in K[T_1, \dots, T_n]$ such that for each $x \in X$ there is $i \in \{1, \dots, k\}$ with $h_i(x) \neq 0$ and $f(x) = g_i(x)/h_i(x)$.*

*Proof.* Extending $E$ if necessary we can assume $E$ is $|K|^+$-saturated. Let $x \in X$. Then $f(x) \in \mathrm{dcl}(K \cup \{x\}) = K(x)$ by the proposition above, that is, $f(x) = g(x)/h(x)$ with polynomials $g, h \in K[T_1, \dots, T_n]$, $h(x) \neq 0$. Now use saturation. $\square$

Suppose $E$ is algebraically closed of characteristic $p > 0$. Then we have a 0-definable automorphism $x \mapsto x^p$ of $E$, the Frobenius map, and the inverse

$$y \mapsto y^{1/p}$$

of this map is not given piecewise by rational functions. The $n$th iterate $x \mapsto x^{p^n}$ of the Frobenius map has inverse $y \mapsto y^{1/p^n}$, and as we shall see, these inverse maps are the only obstructions in getting an analogue in positive characteristic of the above. Recall that a field $K$ of characteristic $p > 0$ is said to be *perfect* if every element of $K$ is a $p$th power $x^p$ of some $x \in K$. In particular, every finite field is perfect. For any subfield $K$ of $E$ there is a smallest perfect subfield of $E$ that contains $K$, namely

$$K^{1/p^\infty} := \bigcup_n K^{1/p^n}, \quad \text{where } K^{1/p^n} := \{x^{1/p^n} : x \in K\} \subseteq E,$$

and by the next result $K^{1/p^\infty}$ is the definable closure of $K$ in $E$.

**Proposition 2.6.** *Let $E$ be algebraically closed of characteristic $p > 0$, with perfect subfield $K$. Then $K$ is definably closed in $E$.*

The proof is identical to that of Proposition 2.4, using the fact that an irreducible polynomial in one variable over a perfect field is separable.

**Corollary 2.7.** *Let $E$ be algebraically closed of characteristic $p > 0$, with perfect subfield $K$, and let $X \subseteq E^n$ and $f : X \to E$ be $K$-definable in $E$. Then there are $g_1, \dots, g_k, h_1, \dots, h_k \in K[T_1, \dots, T_n]$ and an $n$ with the following property: for each $x \in X$ there is $i \in \{1, \dots, k\}$ such that*

$$h_i(x^{1/p^n}) \neq 0 \quad \text{and} \quad f(x) = g_i(x^{1/p^n})/h_i(x^{1/p^n}),$$

*where $x^{1/p^n} := (x_1^{1/p^n}, \dots, x_n^{1/p^n})$ for $x = (x_1, \dots, x_n) \in E^n$.*

Here is an application, usually stated only for injective endomorphisms of algebraic varieties as a theorem of Ax:

**Corollary 2.8.** *Let $E$ be algebraically closed, and suppose $X \subseteq E^n$ and $f : X \to X$ are definable in $E$ such that $f$ is injective. Then $f$ is surjective.*

*Proof.* Consider first the case that $E$ is an algebraic closure of a finite field $K$ of characteristic $p > 0$. After increasing $K$ we can assume that $X$ and $f$ are definable over $K$. Now $E$ is the union of the intermediate finite fields $F$ with $K \subseteq F \subseteq E$, and all such $F$ being perfect, it follows from Corollary 2.7 that $f$ maps $X(F) := X \cap F^n$ into $X(F)$, so $f(X(F)) = X(F)$ by injectivity. Taking the union over all these $F$ we get $f(X) = X$, so we are done for this particular $E$. The corollary is equivalent to certain sentences in the language of rings holding in all algebraically closed fields; we have shown these sentences hold in all algebraic closures of finite fields. Therefore they hold in all algebraically closed fields. □

**Strong minimality.**

**Corollary 2.9.** *Suppose $E$ is algebraically closed and $X \subseteq E$ is definable in $E$. Then $X$ is finite or cofinite.*

*Proof.* Use QE, the fact that a non-zero polynomial $f(T) \in E[T]$ has only finitely many zeros in $E$, and that the subsets of $E$ that are finite or cofinite are the elements of an algebra on $E$. □

The significance of this fact is that the completions $\mathrm{ACF}(p)$ of ACF are strongly minimal theories in the following sense.

Let $L$ be a one-sorted language and let $\mathcal{M} = (M; \dots)$ be an infinite $L$-structure. Then $\mathcal{M}$ is said to be *strongly minimal* if for each 0-definable relation $R \subseteq M^{n+1}$ in $\mathcal{M}$ there is $m$ such that for all $a \in M^n$, either $|R(a)| \leq m$ or $|M \setminus R(a)| \leq m$; when $\mathcal{M}$ is $\aleph_0$-saturated, this is equivalent to the requirement that every $X \subseteq M$ definable in $\mathcal{M}$ is finite or cofinite. If $\mathcal{M}$ is strongly minimal, so is every $L$-structure elementarily equivalent to $\mathcal{M}$. Thus strong minimality is really a property of the theory $\mathrm{Th}(\mathcal{M})$ of $\mathcal{M}$, and we say that a complete $L$-theory $T$ is strongly minimal if it has an infinite strongly minimal model.

Suppose $\mathcal{M}$ is strongly minimal and $\aleph_0$-saturated, and let $T = \mathrm{Th}(\mathcal{M})$. Note that if $X \subseteq M$ is definable in $\mathcal{M}$, then $\mathrm{MR}(X) = 0$ when $X$ is finite, and $\mathrm{MR}(X) = 1$ otherwise. Thus $T$ is totally transcendental, by the equivalence (1) $\Leftrightarrow$ (3) of Corollary 8.4 in *Introduction to model-theoretic stability.* In particular, each completion $\mathrm{ACF}(p)$ of ACF is omega-stable.

**Exercise.** Let $E$ be algebraically closed, $K$ a subfield, and $x$ a variable. Then elements $a, b \in E$ realize the same $x$-type over $K$ in $E$ iff they are either both transcendental over $K$, or both algebraic over $K$ with the same minimum polynomial over $K$. The field $E$ is saturated iff $E$ has infinite transcendence degree over its prime field.

**Morley rank and transcendence degree.** If $E$ is algebraically closed with subset $S$, then the (model-theoretic) algebraic closure $\mathrm{acl}(S)$ of $S$ in $E$ contains obviously the field-theoretic algebraic closure in $E$ of the subfield of $E$ generated by $S$, and is in fact equal to (the underlying set of) this field-theoretic algebraic closure:

**Lemma 2.10.** *Let $E$ be algebraically closed with algebraically closed subfield $K$. Then $K$ is algebraically closed in $E$ in the model theory sense.*

*Proof.* Obvious from $K \preceq E$. $\square$

In Section 11 of *Introduction to model-theoretic stability* we saw that strong minimality has strong consequences. But there we worked in a big model $\mathbb{M}$ with $\kappa(\mathbb{M}) > 2^{|L|}$. In order to use results from those notes we therefore fix in the remainder of this subsection an algebraically closed field $\Omega$ of size $|\Omega| > 2^{\aleph_0}$. Then $\Omega$ is saturated (by an earlier exercise), and thus big with $\kappa(\Omega) = |\Omega|$. In this subsection $K$ is a small subfield of $\Omega$, so $\Omega$ has infinite transcendence degree over $K$.

By the strong minimality of $\Omega$ the operation $S \mapsto \mathrm{acl}(S)$ on the power set of $\Omega$ makes $\Omega$ into a pregeometry, and one checks easily that a subset of $\Omega$ is $K$-independent in the sense of this pregeometry iff it is algebraically independent over $K$. Thus for a set $S \subseteq \Omega$, the size $\mathrm{rk}_K S$ of any maximal $K$-independent subset of $S$ equals the transcendence degree $\mathrm{trdeg}_K K(S)$ of the field $K(S)$ over $K$. (We only use this for finite $S$.) By results in Section 11 of the notes already mentioned it follows that for $a_1, \dots, a_n \in \Omega$ we have

$$\mathrm{MR}((a_1, \dots, a_n)|K) = \mathrm{trdeg}_K K(a_1, \dots, a_n).$$

**Proposition 2.11.** *Let $X \subseteq \Omega^n$ be nonempty and definable in $\Omega$ over $K$. Then* $\mathrm{MR}(X) = \max\{\mathrm{trdeg}_K K(a) : a \in X\}$*, so* $0 \le \mathrm{MR}(X) \le n$.

*Proof.* By Section 9 in *Introduction to model-theoretic stability* we have

$$\mathrm{MR}(X) = \max\{\mathrm{MR}(a|K) : a \in X\}$$

Now combine this with the identity preceding the proposition. $\square$

In particular, $\mathrm{MR}(\Omega^n) = n$.

**Elimination of imaginaries.** Let $T$ be a complete theory in a one-sorted language and $\mathcal{M} = (M; \dots)$ a model of $T$. Recall that for $T$ to have EI (elimination of imaginaries) means that if $E$ is a 0-definable equivalence relation on $M^m$, then there is a 0-definable map $f : M^m \to M^n$ for some $n$ such that for all $a, b \in M^m$,

$$aEb \iff f(a) = f(b).$$

(The point is that then $f$ induces a bijection $E(a) \mapsto f(a)$ of the quotient set $M^m/E$ onto the 0-definable set $f(M^m) \subseteq M^n$ in $\mathcal{M}$, so this quotient set can be treated via this bijection as a 0-definable set itself. Recall also that if $T$ has EI, then the above holds with "$A$-definable" in place of "0-definable", for any parameter set $A$ in $\mathcal{M}$.)

In this subsection $\Omega$ is a big algebraically closed field. We shall prove that every set $X \subseteq \Omega^n$ definable in $\Omega$ has a code in $\Omega$; see Sections 4, 5 of *Introduction to model-theoretic stability* for facts about *coding*. Once established—for $\Omega$ of any characteristic—it follows by Lemma 4.7 in those notes that $\mathrm{ACF}(p)$ has EI, for each $p$.

Consider first the special case where $n = 1$ and $X \subseteq \Omega$ is finite, say $X = \{a_1, \dots, a_d\}$ with distinct $a_1, \dots, a_d$. The trick is to consider the polynomial

$$(T + a_1) \cdots (T + a_d) = T^d + b_1 T^{d-1} + \cdots + b_d, \quad (b_1, \dots, b_d \in \Omega).$$

Unique factorization of $\Omega[T]$ yields that for all $\sigma \in \mathrm{Aut}(\Omega)$,

$$\sigma(X) = X \iff \sigma(b_1) = b_1, \dots, \sigma(b_d) = b_d,$$

so $(b_1, \dots, b_d)$ codes $X$ in $\Omega$, by an exercise in Section 5 of *Introduction to model-theoretic stability.* As a special case, a set $\{a_1, a_2\} \subseteq \Omega$ is coded in $\Omega$ by the pair $(a_1 + a_2, a_1 a_2) \in \Omega^2$.

Next, let $n$ be arbitrary and let $X \subseteq \Omega^n$ be finite, so $X = \{a_1, \dots, a_d\}$ with distinct $a_1, \dots, a_d$, where $a_i = (a_{i1}, \dots, a_{in}) \in \Omega^n$ for $i = 1, \dots, d$. We adapt the previous argument by forming the polynomial

$$f(Y, T) := (T + a_{11} Y_1 + \cdots + a_{1n} Y_n) \cdots (T + a_{d1} Y_1 + \cdots + a_{dn} Y_n) \in \Omega[Y, T],$$

in the distinct variables $Y_1, \dots, Y_n, T$ over $\Omega$, with $Y = (Y_1, \dots, Y_n)$. Then

$$f(Y, T) = \sum_{\boldsymbol{i}, j} b_{\boldsymbol{i}, j} Y^{\boldsymbol{i}} T^j, \qquad (\text{all } b_{\boldsymbol{i}, j} \in \Omega),$$

where the sum is over the tuples $\boldsymbol{i}, j$ with $\boldsymbol{i} \in \mathbb{N}^n$, $j \in \mathbb{N}$, $|\boldsymbol{i}| + j = d$. Again by unique factorization in $\Omega[Y, T]$ we have for any automorphism $\sigma$ of $\Omega$,

$$\sigma(X) = X \iff \sigma(b_{\boldsymbol{i}, j}) = b_{\boldsymbol{i}, j} \text{ for all } \boldsymbol{i}, j \text{ as above.}$$

Thus the finite tuple $(b_{\boldsymbol{i}, j})$ codes $X$ in $\Omega$. We have shown: *each finite subset of $\Omega^n$ has a code in $\Omega$.* (This particular coding of finite sets works just as well when $\Omega$ is any big field, not necessarily algebraically closed, and of course we can also allow here extra structure on $\Omega$.)

Next we show that coding arbitrary definable subsets of $\Omega^n$ can be reduced to coding *finite* sets. This reduction works in a more general setting, which is as follows. Let $T$ be a strongly minimal (one-sorted) complete theory. Take a big model $\mathbb{M}$ of $T$, and assume that $\mathrm{acl}(\emptyset) \subseteq \mathbb{M}$ is infinite. (Note that then in *every* model $\mathcal{M}$ of $T$ the parameterset $\mathrm{acl}(\emptyset) \subseteq M$ is infinite. Note also that this assumption is satisfied for $T = \mathrm{ACF}(p)$, for any $p$.) For each $n$, take a 0-definable finite set $\Phi_n \subseteq \mathbb{M}$ such that $|\Phi_n| > n$. (For example, $\Phi_n = \{\sigma(c_i) : \sigma \in \mathrm{Aut}(\mathbb{M}),\ 0 \le i \le n\}$ where $c_0, \dots, c_n$ are distinct elements of $\mathrm{acl}(\emptyset) \subseteq \mathbb{M}$.) Let $X \subseteq \mathbb{M}^m$ be a nonempty definable set; we assign to $X$ a finite nonempty set $\Phi(X) \subseteq X$. This is done by induction on $m$. If $m = 1$ (so $X \subseteq \mathbb{M}$), then $\Phi(X) := X$ when $X$ is finite, and otherwise $\Phi(X) := X \cap \Phi_n$ where $|\mathbb{M} \setminus X| = n$. For $m > 1$, let $\pi : \mathbb{M}^m \to \mathbb{M}^{m-1}$ be given by $\pi(a_1, \dots, a_m) = (a_1, \dots, a_{m-1})$, and assume inductively that $\Phi\big(\pi(X)\big)$ is a finite nonempty subset of $\pi(X)$. Then

$$\Phi(X) := \{(a, b) \in \mathbb{M}^{m-1} \times \mathbb{M} = \mathbb{M}^m :\ a \in \Phi\big(\pi(X)\big),\ b \in \Phi\big(X(a)\big)\}$$

is clearly a finite nonempty subset of $X$.

It is easy to see that for all nonempty definable $X \subseteq \mathbb{M}^m$ and $\sigma \in \mathrm{Aut}(\mathbb{M})$,

$$\Phi\big(\sigma(X)\big) \;=\; \sigma\big(\Phi(X)\big).$$

(This is intuitively plausible because $\Phi(X)$ does not depend on a choice of formula defining $X$, but just on $X$ itself. In any case, it follows by induction on $m$, using for $m = 1$ that $\sigma(\Phi_n) = \Phi_n$ for all $\sigma \in \mathrm{Aut}(\mathbb{M})$.)

**Lemma 2.12.** *Let $Y \subseteq \mathbb{M}^n$ be definable in $\mathbb{M}$. Then there is a finite set $\Phi \subseteq \mathbb{M}^m$ (for some $m$) such that for all $\sigma \in \mathrm{Aut}(\mathbb{M})$,*

$$\sigma(Y) = Y \iff \sigma(\Phi) = \Phi.$$

*Proof.* Take a 0-definable relation $R \subseteq \mathbb{M}^{m+n} = \mathbb{M}^m \times \mathbb{M}^n$ such that $Y = R(a)$ for some $a \in \mathbb{M}^m$. Consider the 0-definable equivalence relation $\sim$ on $\mathbb{M}^m$ given by $a \sim b \iff R(a) = R(b)$. If $X$ is an equivalence class of $\sim$, then by the remark preceding the lemma,

$$\sigma(X) = X \iff \sigma\big(\Phi(X)\big) = \Phi(X), \qquad \text{for all } \sigma \in \mathrm{Aut}(\mathbb{M}).$$

Also, taking for $X$ the equivalence class of some $a \in \mathbb{M}^m$ such that $R(a) = Y$,

$$\sigma(Y) = Y \iff \sigma(X) = X, \quad \text{for all } \sigma \in \mathrm{Aut}(\mathbb{M}),$$

so $\Phi := \Phi(X)$ has the desired property. $\square$

Combining this lemma with the earlier result that each finite subset of each $\Omega^m$ has a code in $\Omega$ it follows that each definable subset of each $\Omega^n$ has a code in $\Omega$. Thus $\mathrm{ACF}(p)$ has EI, for each $p$.

Let $\sim_n$ be the equivalence relation on $\mathbb{M}^n$ defined by

$$(a_1, \dots, a_n) \sim_n (b_1, \dots, b_n) \iff \begin{array}{l} \text{there is a permutation } \pi \text{ of } \{1, \dots, n\} \\ \text{such that } b_i = a_{\pi(i)} \text{ for } i = 1, \dots, n. \end{array}$$

Hence $\sim_n$ is 0-definable in $\mathbb{M}$, and is the identity on $\mathbb{M}$ for $n = 1$. Thus the quotient set $\mathbb{M}^n/\sim_n$ is the underlying set of a sort in the language of $\mathbb{M}^{\mathrm{eq}}$ and the quotient map $f_{\sim_n} : \mathbb{M}^n \to \mathbb{M}^n/\sim_n$ given by $f_{\sim_n}(a) := a/\sim_n$ is 0-definable in $\mathbb{M}^{\mathrm{eq}}$. These quotients are enough to get EI, as the following result states in a more precise way.

**The smallest field of definition of a polynomial ideal.** In Section 4 we shall prove that the theory of differentially closed fields has EI, and to prepare for this we establish here an important fact about polynomial ideals over fields, Proposition 2.14 below.

**Lemma 2.13.** *Let $F$ be finitely generated as a field over its subfield $\mathbf{k}$, and let $K$ be an intermediate field, $\mathbf{k} \subseteq K \subseteq F$. Then $K$ is finitely generated as a field over $\mathbf{k}$.*

*Proof.* By adjoining to $\mathbf{k}$ a finite transcendence basis of $K$ over $\mathbf{k}$ we can assume that $K$ is algebraic over $\mathbf{k}$. It suffices to show that then the dimension $[K : \mathbf{k}]$ of $K$ as a $\mathbf{k}$-linear space is finite. Let $B$ be a transcendence basis of $F$ over $\mathbf{k}$. Then $B$ is also a transcendence basis of $F$ over $K$, so if $e_1, \dots, e_n \in K$ are linearly independent over $\mathbf{k}$, they remain linearly independent over $\mathbf{k}(B)$. Now $F$ is algebraic over $\mathbf{k}(B)$ and finitely generated as a field over $\mathbf{k}(B)$, hence $[F : \mathbf{k}(B)]$ is finite, so $[K(B) : \mathbf{k}(B)]$ is finite, and thus $[K : \mathbf{k}]$ is finite. $\square$

Let $I$ be an ideal of $F[T_1, \dots, T_n]$. A *field of definition* of $I$ is a subfield $K$ of $F$ such that $I$ is generated by polynomials in $K[T_1, \dots, T_n]$. Since $I$ is finitely generated, it has a finitely generated field of definition.

**Proposition 2.14.** *I has a smallest field of definition.*

*Proof.* Let $F[T_1, \dots, T_n]/I = F[t_1, \dots, t_n]$, $t_i = T_i + I$ for $i = 1, \dots, n$. Let $\alpha = (\alpha_1, \dots, \alpha_n)$ range over $\mathbb{N}^n$. As an $F$-linear space, $F[t_1, \dots, t_n]$ is generated by the elements $t^\alpha := t_1^{\alpha_1} \cdots t_n^{\alpha_n}$. Take $\Lambda \subseteq \mathbb{N}^n$ such that the family $(t^\lambda)_{\lambda \in \Lambda}$ is a basis of this vector space over $F$; below we let $\lambda$ range over $\Lambda$. For each $\alpha$ we have

$$T^\alpha \;=\; f_\alpha + \sum_\lambda c_{\alpha\lambda} T^\lambda, \qquad f_\alpha \in I,\ c_{\alpha\lambda} \in F \text{ for each } \lambda \in \Lambda,$$

where $c_{\alpha\lambda} \neq 0$ for only finitely many $\lambda$. Let $K$ be the subfield of $F$ generated by all $c_{\alpha\lambda}$. Then $f_\alpha \in K[T_1, \dots, T_n]$ for each $\alpha \in \mathbb{N}^n$; we claim that $I$ is generated by the $f_\alpha$. To see why, let $f = \sum_\alpha a_\alpha T^\alpha \in I$ (all $a_\alpha \in F$). Then

$$\begin{aligned} f &= \sum_\alpha a_\alpha \big(f_\alpha + \sum_\lambda c_{\alpha\lambda} T^\lambda\big) \\ &= \sum_\alpha a_\alpha f_\alpha + \sum_\alpha a_\alpha \sum_\lambda c_{\alpha\lambda} T^\lambda \\ &= \sum_\alpha a_\alpha f_\alpha + \sum_\lambda \big(\sum_\alpha a_\alpha c_{\alpha\lambda}\big) T^\lambda. \end{aligned}$$

Going modulo $I$ yields $\sum_\alpha a_\alpha c_{\alpha\lambda} = 0$ for each $\lambda$, hence $f = \sum_\alpha a_\alpha f_\alpha$.

By this claim, $K$ is a field of definition of $I$. Let $E$ with $E \subseteq F$ be any field of definition of $I$. It remains to show that $K \subseteq E$. Let $g_1, \dots, g_m \in E[T_1, \dots, T_n]$ generate $I$. For each $\alpha$ we have $f_\alpha = T^\alpha - \sum_\lambda c_{\alpha\lambda} T^\lambda \in I$, so we can take $h_{\alpha 1}, \dots, h_{\alpha m} \in F[T_1, \dots, T_n]$ such that

$$T^\alpha - \sum_\lambda c_{\alpha\lambda} T^\lambda = \sum_{j=1}^m g_j h_{\alpha j}.$$

Fix $\alpha$, and replace in this identity the nonzero $c_{\alpha\lambda}$ and the nonzero coefficients of the $h_{\alpha j}$ by variables. Then the above identity translates into a finite system of linear equations in these variables, with coefficients in $E$ and with a solution in $F$. Therefore this system has a solution in $E$, so we have elements $c^E_{\alpha\lambda}$ in $E$, nonzero for only finitely many $\lambda$, and we can arrange the $h_{\alpha j}$ to be in $E[T_1, \dots, T_n]$ such that

$$T^\alpha - \sum_\lambda c^E_{\alpha\lambda} T^\lambda = \sum_{j=1}^m g_j h_{\alpha j}.$$

By the basis property of the $T^\lambda$ this forces $c^E_{\alpha\lambda} = c_{\alpha\lambda}$ for all $\lambda$. Since $K$ is generated by the $c_{\alpha\lambda}$, this yields $K \subseteq E$. □

A smallest field of definition of $I$ is unique, by the very meaning of *smallest*. Let $K$ be the smallest field of definition of $I$. Then $K$ is contained in a finitely generated subfield of $F$, and is thus itself a finitely generated field by Lemma 2.13. Take $a = (a_1, \dots, a_m) \in F^m$ such that $K = \mathbb{F}(a)$ where $\mathbb{F}$ is the prime field of $F$. Extend each $\sigma \in \mathrm{Aut}(F)$ to an automorphism of the ring $F[T_1, \dots, T_n]$, also denoted by $\sigma$, by requiring $\sigma(T_i) = T_i$ for $i = 1, \dots, n$. Then we have:

**Corollary 2.15.** *For all* $\sigma \in \mathrm{Aut}(F)$*,*

$$\sigma(I) = I \iff \sigma(a) = a.$$

*Proof.* Let $\sigma \in \mathrm{Aut}(F)$. If $\sigma(a) = a$, then $\sigma$ is the identity on $K$, so $\sigma(I) = I$. Conversely, suppose that $\sigma(I) = I$. With the notations used in the proof of Proposition 2.14, this gives for all $\alpha$,

$$T^\alpha \ = \ \sigma(f_\alpha) + \sum_\lambda \sigma(c_{\alpha\lambda}) T^\lambda,$$

and $\sigma(f_\alpha) \in \sigma(I) = I$, so $t^\alpha = \sum_\lambda \sigma(c_{\alpha\lambda}) t^\lambda$, hence $\sigma(c_{\alpha\lambda}) = c_{\alpha\lambda}$ for all $\alpha, \lambda$. Thus $\sigma$ is the identity on $K$. □

This fact can be used to give another proof that $\mathrm{ACF}(p)$ has EI, but we shall use it instead for differentially closed fields in Section 4.

**Algebraically closed fields with a distinguished subring.** In this subsection $E$ and $F$ denote *algebraically closed* fields. Let $L(U)$ be the language of rings augmented by the unary relation symbol $U$, and consider $L(U)$-structures $(E, R)$ where $R$ is (the underlying set of) a subring of $E$.

Such $R$ is said to be *small in* $E$, or a *small subring of* $E$, if for each $n \geq 1$ there is $a \in E$ such that $f(a) \neq 0$ for all nonzero polynomials $f(T) \in R[T]$ of degree $n$. (This has nothing to do with the notion of a small parameter set in a big $\mathbb{M}$.) For example, any proper algebraically closed subfield of $E$ is small in $E$. Note that there is a set $\Sigma(\text{small})$ of $L(U)$-sentences such that for every $E$ and subring $R$ of $E$,

$$(E, R) \models \Sigma(\text{small}) \iff R \text{ is small in } E.$$

(It follows from a famous theorem of E. Artin that if a subring $R$ is not small in $E$, then the fraction field of $R$ is either $E$ itself, or is a real closed field with $E$ of dimension 2 as a vector space over this fraction field. Thus we can take $\Sigma(\text{small})$ to consist of a single sentence; we shall not use this in what follows.)

**Proposition 2.16.** *For any $L(U)$-sentence $\sigma(U)$ there is an $L$-sentence $\sigma$ such that for every $E$ and small subring $R$ of $E$,*

$$(E, R) \models \sigma(U) \iff R \models \sigma.$$

*Proof.* By Stone duality this reduces to proving that $\mathrm{Th}(E, R)$ is completely determined by $\mathrm{Th}(R)$, for $E$ and $R$ as in the proposition; more precisely, it suffices to show:

*Let $R$ and $S$ be subrings of $E$ and $F$ and small in $E$ and $F$, respectively, and suppose that $R \equiv S$ as rings. Then $(E, R) \equiv (F, S)$.*

The statement of the proposition is of the kind that allows us to use the continuum hypothesis CH in its proof without sacrificing generality. Assuming CH, we can reduce to the case that $(E, R)$ and $(F, S)$ are saturated of size $\aleph_1$. In particular, $R$ and $S$ are saturated and either both finite, or both of size $\aleph_1$, and in any case, $R$ and $S$ are isomorphic. It is also easy to check —and here smallness comes in—that $E$ has transcendence degree $\aleph_1$ over the fraction field of $R$ inside $E$, and likewise with $F$ relative to $S$. Thus an isomorphism between $R$ and $S$ extends to an isomorphism between $E$ and $F$, and thus $(E, R) \cong (F, S)$. $\square$

**Remark.** We have assumed familiarity with Stone duality and its uses as in the proof above; for those not yet used to this routine we give the details in this case. Take the boolean algebra $B(U)$ of $L(U)$-sentences modulo equivalence in all structures $(E, R)$ as in the proposition, and take the boolean algebra $B$ of $L$-sentences modulo equivalence in all domains. We can construct for each $L$-sentence $\sigma$ an $L(U)$-sentence $\sigma(U)$ such that the equivalence of the proposition holds for every $E$ and small subring $R$ of $E$; this assignment $\sigma \mapsto \sigma(U)$ induces an embedding $\iota : B \to B(U)$ of boolean algebras. To prove the proposition it suffices to check that $\iota$ is an isomorphism. By Stone duality this reduces to showing that the $\iota$-image of any ultrafilter on $B$ extends uniquely to an ultrafilter on $B(U)$. It remains to use the obvious correspondence between ultrafilters on $B$ and complete theories of domains, and between ultrafilters on $B(U)$ and complete theories of structures $(E, R)$ as in the proposition.

The following special case is worth noting.

**Corollary 2.17.** *The $L(U)$-theory whose models are the $(E, R)$ with $E$ of characteristic $p$ and $R$ a proper algebraically closed subfield is complete.*

The proof of the proposition works also when the small subrings are equipped with extra structure. This leads to a much better version of Proposition 2.16:

**Proposition 2.18.** *For any $L(U)$-formula $\phi(U)(x)$, $x = (x_1, \ldots, x_n)$, there is an $L$-formula $\phi(x)$ such that for every $E$ and small subring $R$ of $E$,*

$$(E, R) \models \phi(U)(a) \iff R \models \phi(a), \quad \textit{for all } a \in R^n.$$

*Proof.* As before this reduces by Stone duality to proving the following:

*Let $R$ and $S$ be subrings of $E$ and $F$ and small in $E$ and $F$, respectively. Let $a_1, \dots, a_n \in R$, $b_1, \dots, b_n \in S$ be such that $(R, a_1, \dots, a_n) \equiv (S, b_1, \dots, b_n)$, as rings with labeled elements. Then $(E, R, a_1, \dots, a_n) \equiv (F, S, b_1, \dots, b_n)$.*

The proof is basically the same as that of Proposition 2.16. □

**Corollary 2.19.** *Let $E$ be an algebraically closed field and $R$ a small subring of $E$. Then for any set $X \subseteq E^n$ definable in $(E, R)$ its trace $X \cap R^n$ is definable in the ring $R$.*

## 3. Noetherian spaces

We have already used Hilbert's basis theorem in constructing the smallest field of definition of a polynomial ideal. In this section we study noetherianity in a topological setting, with a corresponding notion of Krull dimension, and relate this to Morley rank. This applies directly to algebraically closed fields to give various elementary facts of algebraic geometry, but the general facts on noetherian spaces can also be applied later when dealing with differential fields. Noetherianity is a kind of topological-algebraic counterpart to omega-stability, and these two phenomena often go together.

In this section $X, Y, Z$ denote spaces.

**Remark.** The product set $X \times Y$ is often equipped with a topology that is not necessarily the product topology, but where the projection maps $\pi_X : X \times Y \to X$ and $\pi_Y : X \times Y \to Y$ are nevertheless continuous. Then we have for $X' \subseteq X$, $Y' \subseteq Y$,

$$X' \text{ closed in } X,\ Y' \text{ closed in } Y \implies X' \times Y' \text{ closed in } X \times Y,$$
$$X' \text{ open in } X,\ Y' \text{ open in } Y \implies X' \times Y' \text{ open in } X \times Y.$$

This is because $X' \times Y' = \pi_X^{-1}(X') \cap \pi_Y^{-1}(Y')$.

**Definition.** $X$ is said to be *noetherian* if it satisfies the descending chain condition on closed sets: there is no strictly descending infinite sequence $C_0 \supset C_1 \supset \cdots$ of closed subsets of $X$; equivalently, each nonempty collection of closed subsets of $X$ has a minimal element with respect to inclusion.

**Remarks.** A noetherian space is compact, but in the absence of being hausdorff this is less useful than the following facts.

(1) Each subspace of a noetherian space is noetherian.
(2) If $X$ is noetherian and $f : X \to Y$ is continuous, then $f(X) \subseteq Y$ is noetherian.
(3) If $X$ is covered by finitely many noetherian subspaces, then $X$ is noetherian.

**Key Example.** Let $\mathbf{k}$ be a field with subfield $K$. Each set $S \subseteq K[T_1, \dots, T_n]$ of polynomials determines the set

$$\mathrm{Z}(S) := \{t \in \mathbf{k}^n : \ f(t) = 0 \text{ for all } f \in S\}$$

of zeros of $S$ in $\mathbf{k}$. The subsets of $\mathbf{k}^n$ of the from $\mathrm{Z}(S)$ with $S$ as above are called the $K$-*algebraic* subsets of $\mathbf{k}^n$, and also the $K$-*Zariski closed* (or just $K$-closed) subsets of $\mathbf{k}^n$. They are the closed sets of a topology on $\mathbf{k}^n$, called the $K$-*Zariski topology* on $\mathbf{k}^n$. To see this, use that

$$\bigcap_{i \in I} \mathrm{Z}(S_i) \ = \ \mathrm{Z}\big(\bigcup_{i \in I} S_i\big)$$

where $(S_i)_{i \in I}$ is any family of subsets of $K[T_1, \dots, T_n]$, and that

$$\mathrm{Z}(S_1) \cup \mathrm{Z}(S_2) = \mathrm{Z}(\{f_1 f_2 : f_1 \in S_1, \ f_2 \in S_2\})$$

for $S_1, S_2 \subseteq K[T_1, \dots, T_n]$. Given any polynomials $f_1, \dots, f_m \in K[T_1, \dots, T_n]$ the polynomial map

$$t \mapsto (f_1(t), \dots, f_m(t)) \ : \ \mathbf{k}^n \to \mathbf{k}^m$$

is continuous for the $K$-Zariski topologies on $\mathbf{k}^n$ and $\mathbf{k}^m$. This topology is not hausdorff if $\mathbf{k}$ is infinite and $n > 0$. Every singleton $\{a\}$ with $a \in K^n$ is $K$-closed in $\mathbf{k}^n$. When $K = \mathbf{k}$, we omit the prefix $K$ in expressions like "$K$-algebraic", and "$K$-Zariski topology".

**Fact.** The set $\mathbf{k}^n$ with its $K$-Zariski topology is a noetherian space. To see why this is so, we put for any set $C \subseteq \mathbf{k}^n$,

$$\mathrm{I}_K(C) := \{f \in K[T_1, \dots, T_n] : \ f(c) = 0 \text{ for all } c \in C\},$$

an ideal of $K[T_1, \dots, T_n]$. If $C_0 \supset C_1 \supset \cdots$ were a strictly descending infinite sequence of $K$-algebraic subsets of $\mathbf{k}^n$, then

$$\mathrm{I}_K(C_0) \subset \mathrm{I}_K(C_1) \subset \cdots$$

would be a strictly ascending sequence of ideals of $K[T_1, \dots, T_n]$, which contradicts the noetherianity of the ring $K[T_1, \dots, T_n]$.

For $f_1, \dots, f_m \in K[T_1, \dots, T_n]$ we put

$$\mathrm{Z}(f_1, \dots, f_m) := \mathrm{Z}(\{f_1, \dots, f_m\}) = \{a \in \mathbf{k}^n : \ f_1(a) = \cdots = f_m(a) = 0\}.$$

Actually, the noetherianity of $K[T_1, \dots, T_n]$ (Hilbert's basis theorem) yields that for any subset $S$ of $K[T_1, \dots, T_n]$ there are $f_1, \dots, f_m \in S$ such that each $f \in S$ is a $K[T_1, \dots, T_n]$-linear combination of $f_1, \dots, f_m$, and thus $\mathrm{Z}(S) = \mathrm{Z}(f_1, \dots, f_m)$: we need only consider zerosets of finite collections of polynomials. For algebraically closed $\mathbf{k}$ this means that the subsets of $\mathbf{k}^n$ that are $K$-definable in the field $\mathbf{k}$ are exactly the boolean combinations inside $\mathbf{k}^n$ of the $K$-algebraic subsets of $\mathbf{k}^n$.

**Exercise.** With assumptions as in the Key Example, let $I$ and $J$ be ideals of $K[T_1, \dots, T_n]$. Then $\mathrm{Z}(I \cap J) = \mathrm{Z}(I) \cup \mathrm{Z}(J)$ and $\mathrm{Z}(I + J) = \mathrm{Z}(I) \cap \mathrm{Z}(J)$.

The proof of the next result contains a useful device.

**Lemma 3.1.** *Let $K$ be a subfield of a field $\mathbf{k}$. Then the intersection of an algebraic subset of $\mathbf{k}^n$ with $K^n$ is an algebraic subset of $K^n$. In other words, the Zariski topology on $\mathbf{k}^n$ induces the Zariski topology on $K^n$.*

*Proof.* Let $f \in \mathbf{k}[T_1, \dots, T_n]$. It suffices to find polynomials $f_1, \dots, f_m \in K[T_1, \dots, T_n]$ such that for all $a \in K^n$,

$$f(a) = 0 \iff f_1(a) = \cdots = f_m(a) = 0.$$

Take a basis $b_1, \dots, b_m$ of the $K$-linear subspace of $\mathbf{k}$ generated by the coefficients of $f$. Then $f = b_1 f_1 + \cdots + b_m f_m$ with $f_1, \dots, f_m \in K[T_1, \dots, T_n]$, and then $f_1, \dots, f_m$ have the desired property. $\square$

**Exercise.** Let $P$ be a set and $\mathcal{C}$ a collection of subsets of $P$ such that $\emptyset \in \mathcal{C}$, $P \in \mathcal{C}$, for all $C, C' \in \mathcal{C}$ also $C \cap C' \in \mathcal{C}$, and there is no infinite sequence $C_0, C_1, C_2, \dots$ in $\mathcal{C}$ such that $C_0 \supset C_1 \supset \cdots$. Then

(1) each $\mathcal{G} \subseteq \mathcal{C}$ has a finite subset $\mathcal{G}_0$ with $\bigcap \mathcal{G} = \bigcap \mathcal{G}_0$;
(2) the finite unions of sets in $\mathcal{C}$ are the closed sets of a noetherian topology on $P$.

**Other example.** Let $V$ be a vector space, that is, a left module, over a (not necessarily commutative) division ring $\mathbf{k}$. An *affine subset* of $V^n$ is a nonempty intersection inside $V^n$ of finitely many sets of the form

$$\{(v_1, \dots, v_n) \in V^n : \ \lambda_1 v_1 + \cdots + \lambda_n v_n = b\}$$

where $\lambda_1, \dots, \lambda_n \in \mathbf{k}$ and $b \in V$. We leave it as an exercise to show:

(i) Every affine subset of $V^n$ is an intersection inside $V^n$ of at most $n$ subsets of $V^n$ of the form displayed above.
(ii) The finite unions of affine subsets of $V^n$ are the closed sets of a noetherian topology on $V^n$.
(iii) Let $T^\infty_{\mathbf{k}}$ be the theory of infinite vector spaces over $\mathbf{k}$ in the language $\{0, -, +\}$ augmented by a unary function symbol $\lambda$ for each $\lambda \in \mathbf{k}$ to be interpreted as the function $v \mapsto \lambda v$ in each vector space over $\mathbf{k}$. Then $T^\infty_{\mathbf{k}}$ has QE and is complete.
(iv) Assume $V$ is infinite. Then the definable subsets of $V^n$ are exactly the boolean combinations inside $V^n$ of the affine subsets of $V^n$.

**Irreducibility.** A space $X$ is said to be *irreducible* if $X \neq \emptyset$ and $X$ is not the union of two proper closed subsets; equivalently, $X \neq \emptyset$ and any two nonempty open subsets of $X$ have a nonempty intersection. (Note that then $X$ is connected and each nonempty open subset of $X$ is irreducible and dense in $X$.)

**Lemma 3.2.** *Irreducibility has the following invariance properties:*

(1) *$X \subseteq Y$ is irreducible iff $\mathrm{cl}(X) \subseteq Y$ is irreducible.*
(2) *If $f : X \to Y$ is continuous and $X$ is irreducible, then $f(X) \subseteq Y$ is irreducible, and thus $\mathrm{cl}\, f(X)$ is irreducible by (1).*

(3) *Let $X, Y$ be irreducible, and let $X \times Y$ be given a topology such that for all $a \in X$ and $b \in Y$ the maps $y \mapsto (a, y) : Y \to X \times Y$ and $x \mapsto (x, b) : X \to X \times Y$ are continuous. Then $X \times Y$ is irreducible.*

*Proof.* Since (1) and (2) are immediate, we only give the proof of (3). Let $X \times Y = F_1 \cup F_2$ where $F_1, F_2$ are closed in $X \times Y$. For $i = 1, 2$, put

$$F_i^* := \{x \in X : \{x\} \times Y \subseteq F_i\} = \bigcap_{b \in Y} \{x \in X : (x, b) \in F_i\},$$

an intersection of closed subsets of $X$, so $F_i^*$ is closed in $X$. For each $a \in X$ we have $Y = F_1(a) \cup F_2(a)$, and $F_1(a), F_2(a)$ are closed in $Y$, so $Y = F_1(a)$ or $Y = F_2(a)$. Hence, for each $a \in X$ there is $i \in \{1, 2\}$ with $a \in F_i^*$, so $X = F_1^* \cup F_2^*$, and thus $X = F_1^*$ or $X = F_2^*$. It follows that $X \times Y = F_1$ or $X \times Y = F_2$. $\square$

Special case of (1): for each $x \in X$ the subspace $\mathrm{cl}\{x\}$ of $X$ is irreducible.

**Lemma 3.3.** *Suppose $X$ is a finite union of irreducible closed subsets. Then $X$ has irreducible closed subsets $C_1, \ldots, C_m$ such that $X = C_1 \cup \cdots \cup C_m$ and $C_i \not\subseteq C_j$ for $i \neq j$. This property determines $\{C_1, \ldots, C_m\}$ uniquely.*

*Proof.* Take irreducible closed subsets $C_1, \ldots, C_m$ of $X$ covering $X$ with $C_i \not\subseteq C_j$ for $i \neq j$. Suppose $D_1, \ldots, D_n$ are also irreducible closed subsets of $X$ that cover $X$ with $D_k \not\subseteq D_l$ for all distinct $k, l \in \{1, \ldots, n\}$. Given any $C_i$ we have $C_i = (C_i \cap D_1) \cup \cdots \cup (C_i \cap D_n)$, so $C_i \subseteq D_k$ for suitable $k$. By symmetry, $D_k \subseteq C_j$ for suitable $j$ and thus $C_i \subseteq C_j$, which forces $i = j$, and thus $C_i = D_k$. Hence $m = n$ and $\{C_1, \ldots, C_m\} = \{D_1, \ldots, D_n\}$. $\square$

With $X$ and $C_1, \ldots, C_m$ as in this lemma, no $C_i$ is contained in the union of the $C_j$ with $j \neq i$: $X$ is the "irredundant union of $C_1, \ldots, C_m$". The $C_1, \ldots, C_m$ as in this lemma are called the *irreducible components* of $X$. The lemma applies to the empty space with $m = 0$.

**Exercise.** Let $X$ and $Y$ be finite unions of irreducible closed subsets and let $X \times Y$ be given a topology such that the projection maps $X \times Y \to X$ and $X \times Y \to Y$ are continuous and for all $a \in X$ and $b \in Y$ the maps $y \mapsto (a, y) : Y \to X \times Y$ and $x \mapsto (x, b) : X \to X \times Y$ are continuous.

Then $X \times Y$ is a finite union of irreducible closed subsets, and the irreducible components of $X \times Y$ are the sets $C \times D$ where $C$ is an irreducible component of $X$ and $D$ is an irreducible component of $Y$.

**Lemma 3.4.** *Each noetherian space is a finite union of irreducible closed subsets.*

*Proof.* Suppose $X$ is noetherian but not a finite union of irreducible closed subsets. Then we can take a minimal closed subset $Y$ of $X$ that is not a finite union of irreducible closed subsets. Then $Y \neq \emptyset$ and $Y$ is not irreducible, so $Y = C \cup D$ with $C, D$ proper closed subsets of $Y$. Then $C$ and $D$ are finite unions of irreducible closed subsets, so $Y$ is as well, a contradiction. $\square$

Thus each noetherian space is the irredundant union of its (finitely many) irreducible components. It is easy to check that in the Key Example earlier in this section a $K$-algebraic set $C \subseteq \mathbf{k}^n$ is irreducible iff its ideal $\mathrm{I}_K(C)$ is a prime ideal of $K[T_1, \ldots, T_n]$. Since the topology on $\mathbf{k}^n$ depends here on $K$ we shall use the term *$K$-irreducible* instead of *irreducible*.

**Proposition 3.5.** *Let $\mathbf{k}$ be an algebraically closed field with subfield $K$. Using notations from the* Key Example*, a prime ideal $\mathfrak{p}$ of $K[T_1, \ldots, T_n]$ satisfies $\mathrm{I}_K(\mathrm{Z}(\mathfrak{p})) = \mathfrak{p}$, and we have a bijection*

$$\{\text{prime ideals of } K[T_1, \ldots, T_n]\} \to \{K\text{-irreducible } K\text{-closed subsets of } \mathbf{k}^n\}$$

*given by $\mathfrak{p} \mapsto \mathrm{Z}(\mathfrak{p})$, with inverse given by $C \mapsto \mathrm{I}_K(C)$.*

*Proof.* The inclusion $I \subseteq \mathrm{I}_K(\mathrm{Z}(I))$ holds for any ideal $I$ of $K[T_1, \ldots, T_n]$ (without assuming that $\mathbf{k}$ is algebraically closed). Let $\mathfrak{p}$ be a prime ideal of $K[T_1, \ldots, T_n]$ and $f \in \mathrm{I}_K(\mathrm{Z}(\mathfrak{p}))$. Suppose towards a contradiction that $f \notin \mathfrak{p}$. Introduce the field extension $K(t_1, \ldots, t_n)$ of $K$ as the fraction field of the domain

$$K[t_1, \ldots, t_n] := K[T_1, \ldots, T_n]/\mathfrak{p}, \quad t_i := T_i + \mathfrak{p},\ i = 1, \ldots, n.$$

Put $t = (t_1, \ldots, t_n)$, so $f(t) = f + \mathfrak{p} \neq 0$ in $K(t)$. Let $f_1, \ldots, f_m \in K[T_1, \ldots, T_n]$ generate $\mathfrak{p}$, so $f_1(t) = \cdots = f_m(t) = 0$. By (2) of Corollary 2.3 this gives a zero of $\mathfrak{p}$ in $\mathbf{k}$ that is not a zero of $f$, and we have a contradiction. The rest is routine. $\square$

The irreducible components of a noetherian space are like the irreducible factors of a polynomial, and this is more than just a resemblance: let $K$ be a subfield of an algebraically closed field $\mathbf{k}$, and let $f \in K[T_1, \ldots, T_n]$, so

$$\mathrm{Z}(f) := \{a \in \mathbf{k}^n : \ f(a) = 0\}$$

is a $K$-closed subspace of $\mathbf{k}^n$. If $f = 0$, then $\mathrm{Z}(f) = \mathbf{k}^n$ is clearly $K$-irreducible, since the trivial ideal of $K[T_1, \ldots, T_n]$ is prime. If $f \neq 0$, then $f$ is irreducible (in $K[T_1, \ldots, T_n]$) iff the ideal $(f)$ of $K[T_1, \ldots, T_n]$ is prime, and in that case $\mathrm{Z}(f)$ is a $K$-irreducible proper $K$-closed subset of $\mathbf{k}^n$. More generally, if $f \neq 0$, then $\mathrm{Z}(f)$ is a proper $K$-closed subset of $\mathbf{k}^n$ and we can take irreducible factors $f_1, \ldots, f_m$ of $f$ in $K[T_1, \ldots, T_n]$ such that each irreducible factor of $f$ in $K[T_1, \ldots, T_n]$ equals $f_i$ for exactly one $i \in \{1, \ldots, m\}$, up to a factor from $K^\times$, and then $\mathrm{Z}(f_1), \ldots, \mathrm{Z}(f_m)$ are the distinct $K$-irreducible components of $\mathrm{Z}(f)$.

We now extend the above correspondence between prime ideals and irreducible closed sets to a correspondence between radical ideals and closed sets. First we review the facts on radical ideals. Let $R$ be a ring and $I$ an ideal of $R$. Then $I$ said to be *radical* if for all $a \in R$ such that $a^2 \in I$ we have $a \in I$ (and thus for all $a \in R$ and all $n$, if $a^n \in I$, then $a \in I$). Note: $I$ is radical iff $R/I$ has no nonzero nilpotents. The smallest radical ideal of $R$ that contains $I$, called the *radical* of $I$, is

$$\sqrt{I} := \{a \in R : \ a^n \in I \text{ for some } n\},$$

and $\sqrt{I}$ is the intersection within $R$ of the prime ideals of $R$ that contain $I$. If $R$ is noetherian, then $\sqrt{I}$ is the intersection of finitely many prime ideals of $R$.

**Exercise.** If $R$ has no nonzero nilpotents, then the polynomial ring $R[Y]$ has no nonzero nilpotents.

**Corollary 3.6.** *Let* $\mathbf{k}$ *be an algebraically closed field with subfield* $K$. *With notations from the* Key Example, *every ideal* $I$ *of* $K[T_1, \dots, T_n]$ *satisfies* $\mathrm{I}_K(\mathrm{Z}(I)) = \sqrt{I}$, *and we have a bijection*

$$\{\textit{radical ideals of } K[T_1, \dots, T_n]\} \to \{K\textit{-closed subsets of } \mathbf{k}^n\}$$

*given by* $I \mapsto \mathrm{Z}(I)$, *with inverse given by* $C \mapsto \mathrm{I}_K(C)$.

*Proof.* Let $I$ be an ideal of $K[T_1, \dots, T_n]$, so

$$\sqrt{I} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m, \quad \mathfrak{p}_1, \dots, \mathfrak{p}_m \text{ prime ideals of } K[T_1, \dots, T_n], \text{ hence}$$

$$\mathrm{Z}(I) = \mathrm{Z}(\sqrt{I}) = \mathrm{Z}(\mathfrak{p}_1) \cup \cdots \cup \mathrm{Z}(\mathfrak{p}_m), \text{ so by Proposition 3.5,}$$

$$\mathrm{I}_K(\mathrm{Z}(I)) = \mathrm{I}_K(\mathrm{Z}(\mathfrak{p}_1)) \cap \cdots \cap \mathrm{I}_K(\mathrm{Z}(\mathfrak{p}_m)) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m = \sqrt{I}.$$

The rest follows easily. □

In the proof above we can arrange that $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ for $1 \le i < j \le m$, and then $\mathrm{Z}(\mathfrak{p}_1). \dots, \mathrm{Z}(\mathfrak{p}_m)$ are the $K$-irreducible components of $\mathrm{Z}(I) \subseteq \mathbf{k}^n$.

**Exercises.** Let $V$ be an infinite vector space over a division ring $\mathbf{k}$ and give each $V^n$ the noetherian topology whose closed sets are the finite unions of affine subsets of $V^n$. Then the irreducible closed subsets of $V^n$ are exactly the affine subsets of $V^n$. An *affine* function on $V^n$ is defined to be a function $f : V^n \to V$ such that for some $\lambda_1, \dots, \lambda_n \in \mathbf{k}$ and $a \in V$ we have

$$f(v_1, \dots, v_n) = \lambda_1 v_1 + \cdots + \lambda_n v_n + a \text{ for all } v_1, \dots, v_n \in V.$$

(1) For any subset $S$ of $V$, $\mathrm{dcl}(S) = \mathrm{acl}(S)$ is the $\mathbf{k}$-linear span of $S$.
(2) If $X \subseteq V^n$ and $f : X \to V$ are definable in $V$, then there are affine functions $f_1, \dots, f_m$ on $V^n$ such that for each $x \in X$ we have $f(x) = f_i(x)$ for some $i \in \{1, \dots, m\}$.

**Constructibility.** A *constructible* set in $X$ is a boolean combination inside $X$ of closed subsets of $X$, equivalently, it is a finite union

$$(Y_1 \setminus Z_1) \cup \cdots \cup (Y_n \setminus Z_n)$$

where all $Y_i, Z_i$ are closed subsets of $X$.

It follows from this definition that if $X$ is irreducible, then a constructible set in $X$ is dense in $X$ iff it contains a nonempty open subset of $X$. In particular, if $X$ is irreducible, and $Y$ is a constructible set in $X$, then either $Y$ or $X \setminus Y$ contains a nonempty open subset of $X$.

Let $\mathrm{con}(X)$ be the boolean algebra of constructible subsets of $X$. If $Y$ is a closed irreducible subset of $X$, then by the previous remark,

$$F(Y) := \{Z \in \mathrm{con}(X) : \ Z \text{ contains a nonempty open subset of } Y\}$$

is an ultrafilter of $\mathrm{con}(X)$ and $Y$ is the smallest closed subset of $X$ that belongs to $F(Y)$.

**Lemma 3.7.** *Suppose $X$ is noetherian. Then the map*

$$Y \mapsto F(Y) : \ \{\textit{irreducible closed subsets of } X\} \to \mathrm{St}\big(\mathrm{con}(X)\big)$$

*is a bijection.*

*Proof.* The previous remarks show that this map is injective. Let $F$ be an ultrafilter of $\mathrm{con}(X)$ and take $Y$ minimal among the irreducible closed subsets of $X$ that belong to $F$. Then $F(Y) \subseteq F$, and thus $F(Y) = F$. □

Let us consider the case that $K$ is a subfield of an algebraically closed field $\mathbf{k}$. Then the constructible sets in $\mathbf{k}^n$ with its $K$-topology will be called *$K$-constructible subsets of* $\mathbf{k}^n$, and they are exactly the $K$-definable subsets of $\mathbf{k}^n$. In combination with the earlier correspondence between prime ideals of $K[T_1,\dots,T_n]$ and $K$-irreducible $K$-closed sets in $\mathbf{k}^n$ this yields a bijection

$$\{\text{prime ideals of } K[T_1,\dots,T_n]\} \to \mathrm{St}(\mathbf{k}^n|K)$$

that assigns to each prime ideal $I$ of $K[T_1,\dots,T_n]$ the ultrafilter (or type, if you prefer) in the boolean algebra of $K$-definable sets in $\mathbf{k}^n$ consisting of all $K$-definable sets in $\mathbf{k}^n$ that contain a set of the form $\{a \in Z(I) : f(a) \neq 0\}$ with $f \in K[T_1,\dots,T_n],\ f \notin I$.

**Exercise.** Let $X$ be noetherian, let $Y \in \mathrm{con}(X)$, and let $C_1,\dots,C_m$ be the irreducible components of $\mathrm{cl}(Y)$. Then $Y \cap C_i$ contains a nonempty open subset of $C_i$, for $i = 1,\dots,m$.

**Canonical filtration of a constructible set.** In this subsection $X$ is a noetherian space. Let $Y$ be a nonempty constructible set in $X$ and define closed subsets $F_0(Y), F_1(Y)$ of $X$ as follows:

$$F_0(Y) := \mathrm{cl}(Y), \qquad F_1(Y) := \mathrm{cl}\big(F_0(Y) \setminus Y\big).$$

It is immediate that $F_0(Y) \supseteq F_1(Y)$, and $F_0(Y) \setminus F_1(Y) \subseteq Y$. We claim that $F_0(Y) \supset F_1(Y)$. Let $C_1,\dots,C_m$ be the distinct irreducible components of $F_0(Y)$. Then $Y$ contains a nonempty open subset $U_i$ of $C_i$ for $i = 1,\dots,m$, so $F_1(Y) \subseteq D_1 \cup \dots \cup D_m$ where $D_i := C_i \setminus U_i$ is a proper closed subset of $C_i$ for $i = 1,\dots,m$, so $F_1(Y) \subset F_0(Y)$, as claimed.

Now $Y$ is the disjoint union of $F_0(Y) \setminus F_1(Y)$ and $Y_1 := Y \cap F_1(Y)$, and if the constructible set $Y_1$ is not empty, we repeat the above with $Y_1$ in place of $Y$, and set

$$F_2(Y) := F_0(Y_1), \qquad F_3(Y) := F_1(Y_1).$$

Continuing in this way we obtain a descending chain

$$F_0(Y) \supset F_1(Y) \supseteq F_2(Y) \supset F_3(Y) \supseteq \dots \supseteq F_{2p}(Y) \supset F_{2p+1}(Y) = \emptyset$$

that stops as soon as we reach the empty set. It has the property that

$$Y = \bigcup_{i=0}^{p} F_{2i}(Y) \setminus F_{2i+1}(Y).$$

We call the sequence $F_0(Y), \dots, F_{2p}(Y)$ the *canonical filtration of* $Y$. (If $Y$ is closed in $X$, then this sequence has just one term, namely $F_0(Y) = Y$.) Note that if $h : X \to X$ is a homeomorphism, then $h\big(F_0(Y)\big), \dots, h\big(F_{2p}(Y)\big)$ is the canonical filtration of $h(Y)$.

This canonical filtration leads to the following lemma, which is used in the next section to help eliminate imaginaries.

**Lemma 3.8.** *Let* $\mathbb{M}$ *be a big many-sorted* $L$*-structure, let* $y$ *be a finite multivariable, and let* $\mathbb{M}_y$ *be given a noetherian topology such that:*

1. *each closed subset of* $\mathbb{M}_y$ *is definable in* $\mathbb{M}$ *and has a code in* $\mathbb{M}$*;*
2. *every* $\sigma \in \mathrm{Aut}(\mathbb{M})$ *induces a homeomorphism* $a \mapsto \sigma(a) : \mathbb{M}_y \to \mathbb{M}_y$.

*Then every constructible subset of* $\mathbb{M}_y$ *has a code in* $\mathbb{M}$.

*Proof.* Let $Y$ be a nonempty constructible subset of $\mathbb{M}_y$, let $F_0(Y), \dots, F_{2p}(Y)$ be the canonical filtration of $Y$, and let $\sigma \in \mathrm{Aut}(\mathbb{M})$. Then $F_i\big(\sigma(Y)\big) = \sigma\big(F_i(Y)\big)$ for $i = 0, \dots, 2p$ by (2), and thus

$$\sigma(Y) = Y \iff \sigma\big(F_i(Y)\big) = F_i(Y) \text{ for } i = 0, \dots, 2p.$$

Let $a_i$ be a code of $F_i(Y)$ in $\mathbb{M}$ for $i = 0, \dots, 2p$. Then by the above $(a_0, a_1, \dots, a_{2p})$ is a code of $Y$ in $\mathbb{M}$. $\square$

**Constructible sets in noetherian spaces are ranked.** Section 2 of *Introduction to model-theoretic stability* introduced the rank of an element of a boolean algebra. The case of main interest is when every nonzero element of the boolean algebra is ranked. When $X$ is noetherian its boolean algebra of constructible sets has this useful property:

**Proposition 3.9.** *If* $X$ *is noetherian, then every nonempty constructible set in* $X$ *is ranked as an element of the boolean algebra* $\mathrm{con}(X)$.

Towards proving this, first a definition and a lemma that works for general $X$. By transfinite recursion we assign to each ordinal $\lambda$ an ideal $J_\lambda$ of $\mathrm{con}(X)$ such that $J_\lambda \subseteq J_\mu$ for $\lambda \le \mu$:

1. $J_0 :=$ the ideal of $\mathrm{con}(X)$ generated by the minimal closed nonempty subsets of $X$;
2. for $\lambda > 0$, assume inductively that $J_\alpha$ is an ideal of $\mathrm{con}(X)$ for all $\alpha < \lambda$, and that $J_\alpha \subseteq J_\beta$ whenever $\alpha \le \beta < \lambda$; put $J_{<\lambda} := \bigcup_{\alpha<\lambda} J_\alpha$; then $J_\lambda$ is defined to be the ideal of $\mathrm{con}(X)$ generated by $J_{<\lambda}$ and the closed subsets of $X$ that are minimal with respect to not belonging to $J_{<\lambda}$.

For convenience we let $J_{<0} = \{\emptyset\}$ be the trivial ideal of $\mathrm{con}(X)$.

In section 2 of *Introduction to model-theoretic stability* we defined the ideals $I_\lambda$ and $I_{<\lambda}$ of a boolean algebra $B$. For $B = \mathrm{con}(X)$ these ideals are related to the $J_\lambda$ as follows:

**Lemma 3.10.** $J_\lambda \subseteq I_\lambda$.

*Proof.* To get $J_0 \subseteq I_0$, let $Y$ be a minimal closed nonempty subset of $X$; it suffices to show that then $Y$ is an atom of $\mathrm{con}(X)$. If $Y$ were not an atom of $\mathrm{con}(X)$, then $Y$ would have a proper nonempty subset $P \setminus Q$ with $Y \supseteq P \supseteq Q$ and $P, Q$ closed in $X$, and then either $\emptyset \neq P \neq Y$ or $\emptyset \neq Q \neq Y$, a contradiction in both cases.

Let $\lambda > 0$ and let $Y$ be a closed subset of $X$ that is minimal with respect to not belonging to $J_{<\lambda}$. We claim that then the image of $Y$ in $\mathrm{con}(X)/J_{<\lambda}$ is an atom of $\mathrm{con}(X)/J_{<\lambda}$. Suppose otherwise. Then we have closed $P, Q$ in $X$ with $Y \supseteq P \supseteq Q$ such that in the quotient algebra $\mathrm{con}(X)/J_{<\lambda}$,

$$\emptyset/J_{<\lambda} \;\neq\; (P \setminus Q)/J_{<\lambda} \;\neq\; Y/J_{<\lambda}.$$

This easily gives a contradiction using the minimality of $Y$. With this claim and the inductive assumption that $J_{<\lambda} \subseteq I_{<\lambda}$ we obtain $J_\lambda \subseteq I_\lambda$. □

Note that there is always a $\lambda$ such that $J_\lambda = J_{\lambda+1}$, and that if $J_\lambda = J_{\lambda+1}$, then $J_\lambda = J_\mu$ for all ordinals $\mu \geq \lambda$. If $X$ is noetherian and $J_\lambda = J_{\lambda+1}$, then clearly all closed subsets of $X$ belong to $J_\lambda$, and thus $J_\lambda = \mathrm{con}(X)$. Proposition 3.9 above is an immediate consequence of this observation and lemma 3.10.

**Krull dimension.** This is a notion of dimension suitable for noetherian spaces and loosely related to Cantor-Bendixson rank for such spaces. In this subsection we take supremums and infimums in $\mathbb{N} \cup \{-\infty, +\infty\}$. We define the *Krull dimension* of $X$ to be the supremum of the set of $n$ for which there is a chain

$$C_0 \subset C_1 \subset \cdots \subset C_n$$

of irreducible closed subsets of $X$. In particular, the Krull dimension of $X$ is $-\infty$ iff $X = \emptyset$. We denote the Krull dimension of $X$ by $\dim(X)$. (If $X$ is a nonempty hausdorff space, then $\dim(X) = 0$, so Krull dimension is of no interest for hausdorff spaces.) For a point $x \in X$ we define the *Krull dimension of $X$ at $x$* and denote by $\dim_x(X)$ the infimum of the Krull dimensions of the open neighborhoods of $x$ in $X$.

**Lemma 3.11.** *Let $x \in X$.*

1. *If $X \subseteq Y$, then* $\dim(X) \leq \dim(Y)$ *and* $\dim_x(X) \leq \dim_x(Y)$.
2. *If $V$ is a neighborhood of $x$ in $X$, then* $\dim_x(X) = \dim_x(V)$.
3. *Let $X_1, \ldots, X_n$ be closed subsets of $X$ that cover $X$. Then*

$$\dim(X) = \sup\{\dim(X_i) : \; 1 \leq i \leq n\},$$
$$\dim_x(X) = \sup\{\dim_x(X_i) : \; 1 \leq i \leq n, \; x \in X_i\}.$$

*Proof.* For (1), use that the closure in any space of an irreducible subset is irreducible. For (2) and (3), use (1). □

**Corollary 3.12.** *Suppose $X$ is noetherian. Then*

(1) $\dim(X) = \sup\{\dim(C) :$ *$C$ is an irreducible component of $X\}$;*
(2) *for each $x \in X$ we have*

$$\dim_x(X) = \sup\{\dim_x(C) : \textit{ C is an irreducible component of } X,\ x \in C\}.$$

**Lemma 3.13.** $\dim(X) = \sup_{x\in X} \dim_x(X)$.

*Proof.* It is clear that $\dim(X) \geq \dim_x(X)$ for each $x \in X$. Conversely, assume $\dim(X) \geq n$. Take a chain $C_0 \subset \cdots \subset C_n$ of closed irreducible sets in $X$, and take $x \in C_0$. Then for any open neighborhood $U$ of $x$ in $X$ each set $U \cap C_i$ is open in $C_i$ (so $\mathrm{cl}(U \cap C_i) = C_i$), and closed and irreducible in $U$, so we have a chain $U \cap C_0 \subset \cdots \subset U \cap C_n$ in $U$ witnessing $\dim(U) \geq n$. Hence $\dim_x(X) \geq n$. □

**Corollary 3.14.** *If $(U_i)$ is a covering of $X$ by open subsets, then*

$$\dim(X) = \sup_i \dim(U_i).$$

**Lemma 3.15.** *Let $X \times Y$ be given a topology making the projection maps $X \times Y \to X$ and $X \times Y \to Y$ continuous, such that for all $a \in X$ and $b \in Y$ the maps $y \mapsto (a, y) : Y \to X \times Y$ and $x \mapsto (x, b) : X \to X \times Y$ are continuous. Then*

$$\dim(X \times Y) \geq \dim X + \dim Y.$$

*Proof.* Suppose $\dim X \geq m$ and $\dim Y \geq n$; it suffices to show that then $\dim(X \times Y) \geq m + n$. Take chains

$$X_0 \subset X_1 \subset \cdots \subset X_m, \qquad Y_0 \subset Y_1 \subset \cdots \subset Y_n$$

of irreducible closed sets in $X$, respectively $Y$. Then each set $X_i \times Y_j$ is closed in $X \times Y$, and irreducible by ... This gives a chain

$$X_0 \times Y_0 \subset X_0 \times Y_1 \subset \cdots \subset X_0 \times Y_n \subset X_1 \times Y_n \subset \cdots \subset X_m \times Y_n$$

of irreducible closed sets in $X \times Y$, so $\dim(X \times Y) \geq m + n$. □

**Cantor-Bendixson rank versus Krull dimension.** To relate these two dimension notions we need the following.

**Lemma 3.16.** *Suppose $X$ is noetherian. Then the ideal $J_n$ of $\mathrm{con}(X)$ is generated by the irreducible closed $C \subseteq X$ with $\dim(C) \leq n$, and thus contains no closed $C \subseteq X$ with $\dim(C) > n$.*

*Proof.* For $n = 0$ this is because the minimal nonempty closed subsets of $X$ are exactly the irreducible closed sets in $X$ of Krull dimension 0. Assuming inductively that the statement holds for a certain $n$, use that the closed subsets of $X$ that are minimal with respect to not belonging to $J_n$ are the closed irreducible sets in $X$ of Krull dimension $n + 1$. □

Recall that $X$ as an element of the boolean algebra $\mathrm{con}(X)$ has a Cantor-Bendixson rank $\mathrm{rk}(X)$, defined as in Section 2 of *Introduction to model-theoretic stability.*

**Corollary 3.17.** *Assume $X$ is noetherian. Then* $\mathrm{rk}(X) \le \dim(X)$.

*Proof.* If $\mathrm{rk}(X) \ge n$, then $X \notin I_m$ for $m < n$, so $X \notin J_m$ for $m < n$ by Lemma 3.10, hence $\dim(X) \ge n$ by Lemma 3.16. □

We say that *rank is strictly monotone in $X$* if $\mathrm{rk}(X_0) < \mathrm{rk}(X_1)$ for all closed irreducible $X_0, X_1$ in $X$ with $X_0 \subset X_1$.

**Lemma 3.18.** *Suppose $X$ is covered by open subsets $U_1, \dots, U_n$ such that rank is strictly monotone in each $U_i$. Then rank is strictly monotone in $X$.*

*Proof.* Let $X_0, X_1 \subseteq X$ be closed irreducible with $X_0 \subset X_1$. Then $\mathrm{rk}(U_i \cap X_0) < \mathrm{rk}(U_i \cap X_1)$ if $U_i \cap X_1 \ne \emptyset$. Hence

$$\mathrm{rk}(X_0) = \max_i \mathrm{rk}(U_i \cap X_0) < \max_i \mathrm{rk}(U_i \cap X_1) = \mathrm{rk}(X_1).$$

□

**Proposition 3.19.** *Suppose $X$ is noetherian, rank is strictly monotone in $X$, and* $\mathrm{rk}(X) < \omega$. *Let $Y$ be a constructible set in $X$. Then*

(1) $\mathrm{rk}(Y) = \mathrm{rk}\big(\mathrm{cl}(Y)\big) = \dim(Y)$;
(2) *if* $Y \ne \emptyset$, *then* $\mathrm{rk}\big(\mathrm{cl}(Y) \setminus Y\big) < \mathrm{rk}(Y)$;
(3) *if $Y$ is irreducible, then* $\deg(Y) = 1$;
(4) *if* $Y \ne \emptyset$, *then* $\deg(Y)$ *is the number of irreducible components of* $\mathrm{cl}(Y)$ *of the same rank as $Y$;*
(5) *rank is strictly monotone in $Y$.*

*Proof.* It follows from Corollary 3.17 and the assumptions on $X$ that $\mathrm{rk}(X) = \dim(X)$. Next, observe that the assumptions on $X$ are inherited by closed subspaces of $X$, so $\mathrm{rk}(C) = \dim(C)$ for all closed $C \subseteq X$.

Let $U$ be nonempty open in a closed irreducible $C \subseteq X$. Then $C = \mathrm{cl}(U)$, $\mathrm{rk}(C \setminus U) < \mathrm{rk}(C)$ and thus $\mathrm{rk}(U) = \mathrm{rk}(C)$. We claim that rank is strictly monotone in $U$. To see why, let $U_0, U_1$ be closed irreducible in $U$ with $U_0 \subset U_1$. Then $\mathrm{cl}(U_i) \cap U = U_i$, $\mathrm{cl}(U_i)$ is closed irreducible in $X$ with $U_i$ nonempty open in $\mathrm{cl}(U_i)$, for $i = 0, 1$, and $\mathrm{cl}(U_0) \subset \mathrm{cl}(U_1)$, hence $\mathrm{rk}(U_0) = \mathrm{rk}(\mathrm{cl}(U_0)) < \mathrm{rk}(\mathrm{cl}(U_1)) = \mathrm{rk}(U_1)$.

Using these facts we now obtain the desired results on the constructible set $Y$ as follows. The case $Y = \emptyset$ is trivial, so assume $Y \ne \emptyset$, and let $C_1, \dots, C_m$ be the irreducible components of $\mathrm{cl}(Y)$. Then $Y \cap C_i$ contains a nonempty open subset $U_i$ of $C_i$, for each $i$, by an earlier exercise. Hence

$$\max_i \mathrm{rk}(C_i) \;\le\; \mathrm{rk}(Y) \;\le \mathrm{rk}(\mathrm{cl}(Y)) = \max_i \mathrm{rk}(C_i),$$

and likewise with "dim" instead of "rk" and thus (1) holds. Also,

$$\mathrm{cl}(Y) \setminus Y \;\subseteq\; \bigcup_i C_i \setminus U_i,$$

which gives (2). We leave (3) and (4) as an exercise. As to (5), let $Y_0, Y_1$ be closed irreducible sets in $Y$ with $Y_0 \subset Y_1$. Then $\mathrm{cl}(Y_0)$ and $\mathrm{cl}(Y_1)$ are closed irreducible in $X$ and $\mathrm{cl}(Y_0) \subset \mathrm{cl}(Y_1)$, so

$$\mathrm{rk}(Y_0) = \mathrm{rk}\big(\mathrm{cl}(Y_0)\big) < \mathrm{rk}\big(\mathrm{cl}(Y_1)\big) = \mathrm{rk}(Y_1),$$

as desired. □

**Exercise.** Let $V$ be an infinite vector space over a division ring $\mathbf{k}$ and give $V^n$ the noetherian topology whose closed sets are the finite unions of affine subsets of $V^n$. Then rank is strictly monotone in $V^n$, and $\mathrm{rk}(V^n) = n$.

**Morley rank = Krull dimension.** Let $\Omega$ be an algebraically closed field of infinite transcendence degree over its prime field; so $\Omega$ is saturated. We give $\Omega^n$ its Zariski topology, and make every set $Y \subseteq \Omega^n$ into a (noetherian) subspace of $\Omega^n$, with Krull dimension $\dim(Y)$. If $Y \subseteq \Omega^n$ is also definable in $\Omega$, then $\mathrm{MR}(Y)$ is defined, and is the Cantor-Bendixson rank $\mathrm{rk}(Y)$ of $Y$ viewed as an element of the boolean algebra of definable subsets of $\Omega^n$. Recall that $\mathrm{MR}(\Omega^n) = n$.

**Theorem 3.20.** *Let $Y \subseteq \Omega^n$ be definable in $\Omega$. Then*

1. $\mathrm{MR}(Y) = \dim(Y)$*;*
2. $\mathrm{MR}(Y) = \mathrm{MR}\big(\mathrm{cl}(Y)\big)$*;*
3. *if $Y \neq \emptyset$, then* $\mathrm{MR}\big(\mathrm{cl}(Y) \setminus Y\big) < \mathrm{MR}(Y)$*;*
4. *if $Y$ is irreducible, then* $\mathrm{MD}(Y) = 1$*;*
5. *if $Y \neq \emptyset$, then* $\mathrm{MD}(Y)$ *is the number of irreducible components of* $\mathrm{cl}(Y)$ *of the same Morley rank as $Y$.*

By Proposition 3.19 it suffices to show that (Morley) rank is strictly monotone in $\Omega^n$; this strict monotonicity follows from Lemma 3.22 below by noting that any closed irreducible set in $\Omega^n$ is actually $K$-closed (and thus $K$-irreducible) for some finitely generated subfield $K$ of $\Omega$, and that $\Omega$ has infinite transcendence degree over such $K$.

More generally, let $K$ be any subfield of $\Omega$ over which $\Omega$ has infinite transcendence degree, and let in the next two lemmas $X$ be a $K$-irreducible $K$-closed set in $\Omega^n$. Let $\mathfrak{p} := \mathrm{I}_K(X)$, so $\mathfrak{p}$ is a prime ideal of $K[T_1, \dots, T_n]$. Then

$$K[T_1, \dots, T_n]/\mathfrak{p} \;=\; K[t_1, \dots, t_n], \qquad t_i = T_i + \mathfrak{p}, i = 1, \dots, n.$$

Put $t = (t_1, \dots, t_n)$, so $K[t]$ has fraction field $K(t)$, and as we saw in the proof of Proposition 3.5 we have $f(t) = 0$ for all $f \in \mathfrak{p}$ and $f(t) \neq 0$ for all $f \in K[T_1, \dots, T_n]$ with $f \notin \mathfrak{p}$.

**Lemma 3.21.** $\mathrm{MR}(X) = \mathrm{trdeg}_K K(t)$.

*Proof.* By Proposition 2.11 we have

$$\mathrm{MR}(X) = \max\{\mathrm{trdeg}_K K(a) : \; a \in X\}.$$

Since $K(t)$ can be embedded into $\Omega$ over $K$, this gives $\mathrm{MR}(X) \geq \mathrm{trdeg}_K K(t)$. Let $a = (a_1, \ldots, a_n) \in X$. Then we have a surjective $K$-algebra morphism

$$f(t) \mapsto f(a) \ : \ K[t] \to K[a], \qquad (f \in K[T_1, \ldots, T_n]).$$

If $\Lambda \subseteq \{1, \ldots, n\}$ and $(a_\lambda)_{\lambda \in \Lambda}$ is algebraically independent over $K$, then $(t_\lambda)_{\lambda \in \Lambda}$ is algebraically independent over $K$, as is easily checked. It follows that $\mathrm{trdeg}_K K(t) \geq \mathrm{trdeg}_K K(a)$. □

**Lemma 3.22.** *Let $Y$ be a $K$-irreducible $K$-closed proper subset of $X$. Then $\mathrm{MR}(Y) < \mathrm{MR}(X)$.*

*Proof.* Let $\mathfrak{q} := \mathrm{I}_K(Y)$, so $\mathfrak{p}$ is properly contained in $\mathfrak{q}$. Let

$$K[T_1, \ldots, T_n]/\mathfrak{q} \ = \ K[u_1, \ldots, u_n], \qquad u_i = T_i + \mathfrak{q}, i = 1, \ldots, n,$$

and $u := (u_1, \ldots, u_n)$. Then we have a non-injective $K$-algebra morphism

$$f(t) \mapsto f(u) \ : \ K[t] \mapsto K[u], \qquad (f \in K[T_1, \ldots, T_n]).$$

By the previous lemma and its proof we have $\mathrm{trdeg}_K K(t) \geq \mathrm{trdeg}_K K(u)$, and it suffices to show that this inequality is strict. Towards a contradiction, assume $\mathrm{trdeg}_K K(t) = \mathrm{trdeg}_K K(u)$. We may as well assume that $u_1, \ldots, u_m$ is a transcendence basis of $K(u)$ over $K$, and then $t_1, \ldots, t_m$ is a transcendence basis of $K(t)$ over $K$. Then the above morphism extends to a $K$-algebra morphism

$$K(t_1, \ldots, t_m)[t_{m+1}, \ldots, t_n] \to K(u_1, \ldots, u_m)[u_{m+1}, \ldots, u_n]$$

with the left-hand side taken as a subring of $K(t)$ and the right-hand side as a subring of $K(u)$. But both sides are clearly fields, so this morphism is injective, and we have a contradiction. □

## 4. Differential Fields

Differential fields are fields equipped with a derivation. (See below for a precise definition.) We are going to show that the theory of differential fields of characteristic 0 has a model completion, the theory of *differentially closed fields*. The theory of differentially closed fields is complete and omega-stable and has elimination of imaginaries. Given a differentially closed field $\mathbb{U}$ the zerosets of differential polynomials generate a natural noetherian topology on each $\mathbb{U}^n$. These are some of the main facts to be established in this section.

**Differential rings.** A *derivation* on a ring $R$ is a map $\partial \colon R \to R$ satisfying $\partial(a + b) = \partial(a) + \partial(b)$ and $\partial(ab) = \partial(a)b + a\partial(b)$ for all $a, b \in R$. Any ring $R$ has the trivial derivation on it, which maps every element of $R$ to 0. When $\partial$ is a derivation on the ring $R$ and $\partial$ is clear from the context, then, with $a \in R$, we also write $a'$ and $a''$ instead of $\partial(a)$ and $\partial(\partial(a))$, and similarly $a^{(n)}$ for $\partial^n(a)$, with $\partial^n$ the $n$th iterate of $\partial$, in particular, $a^{(0)} = a$.

*Example.* For a ring $A$ and indeterminate $x$ the polynomial ring $A[x]$ has the derivation $\frac{d}{dx}$ given by

$$\sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=1}^{n} i a_{i-1} x^{i-1} \qquad (a_0, \dots, a_n \in A).$$

It is the unique derivation on $A[x]$ with $a' = 0$ for all $a \in A$ and $x' = 1$. More generally, given a ring $A$, distinct indeterminates $x_1, \dots, x_n$, and $i \in \{1, \dots, n\}$ we have the derivation $\frac{\partial}{\partial x_i}$ on $A[x_1, \dots, x_n]$ which is just $\frac{d}{dx_i}$ as above when the elements of $A[x_1, \dots, x_n]$ are viewed as polynomials in $x_i$ with coefficients in $A[x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n]$.

A *differential ring* is a ring together with a derivation on the ring. A *differential field* is a differential ring whose underlying ring is a field. Let $R$ be a differential ring with derivation $\partial$ in this subsection. The elements $a \in R$ such that $a' = 0$ are called *constants* and they are the elements of a subring of $R$, called the *ring of constants* of $R$ and denoted by $C_R$ (or just $C$ if $R$ is clear from the context). In the example above the ring of constants of $A[x]$ with the derivation $\frac{d}{dx}$ is $A$ if $A$ is a domain of characteristic 0. The ring of constants of a differential field $K$ is a subfield $C_K$ of $K$, called the *field of constants* of $K$. In particular, there is only one derivation on $\mathbb{Q}$, namely the trivial derivation.

One easily shows that $(a^n)' = na^{n-1}a'$ for $n > 0$ and $a \in R$, and that if $a$ is a unit, then $(a^k)' = ka^{k-1}a'$ for $k \in \mathbb{Z}$. To a polynomial

$$f = f(T) = \sum_{i=0}^{n} a_i T^i = a_0 + a_1 T + \cdots + a_n T^n \in R[T] \qquad (a_0, \dots, a_n \in R)$$

we associate the polynomials $f^\partial, f' \in R[T]$:

$$f^\partial = \sum_{i=0}^{n} a_i' T^i, \qquad f' = \frac{df}{dT} := \sum_{i=1}^{n} i a_i T^{i-1}.$$

It is easy to check that both maps $f \mapsto f^\partial$ and $f \mapsto f'$ are derivations on $R[T]$. With this notation we have for $a \in R$,

$$f(a)' = f^\partial(a) + f'(a) \cdot a',$$

as is easily checked. Here are some consequences of this identity:

**Lemma 4.1.** *Let $K$ be a differential field of characteristic zero.*

(1) *$C_K$ is relatively algebraically closed in $K$.*
(2) *If $K$ is algebraically closed as a field, so is $C_K$.*
(3) *Let $E$ be an overfield of $K$ and algebraic over $K$. Then there is a unique derivation on $E$ that extends the derivation of $K$.*

*Proof.* As to (1), suppose $a \in K$ is algebraic over $C_K$. Take the minimum polynomial $f(T) \in K[T]$ of $a$ over $K$, so $f(a) = 0$. Since $K$ has characteristic zero we have $f'(a) \neq 0$. Then the identity above yields $0 = f'(a)a'$, so $a' = 0$, hence $a \in C_K$. Item (2) is obvious from (1). As to (3), let $\partial$ be extended to a derivation on $E$. Then for any $a \in E$ and $f(T) \in K[T]$ with $f(a) = 0$ and $f'(a) \neq 0$ we have

$$a' = \frac{-f^{\partial}(a)}{f'(a)},$$

so there is at most one such derivation on $E$. To construct such a derivation, let $a \in E$; it suffices to get a derivation on $K[a] = K(a)$ extending $\partial$. Let $f(T)$ be the minimum polynomial of $a$ over $K$, so the ring morphism

$$K[T] \to K[a], \quad g(T) \mapsto g(a)$$

has kernel $fK[T]$. Consider the additive map

$$d : K[T] \to K[a] = K(a), \qquad d(g) = g^{\partial}(a) + g'(a)\frac{-f^{\partial}(a)}{f'(a)}.$$

An easy computation shows that if $g \in fK[T]$, then $d(g) = 0$, so $fK[T]$ is in the kernel of the additive map $d$, and thus $d$ induces an additive map $K[a] \to K[a]$ that sends $g(a)$ to $g^{\partial}(a) + g'(a)\frac{-f^{\partial}(a)}{f'(a)}$ for each $g \in K[T]$. This last map is easily checked to be a derivation on $K[a]$ extending $\partial$. $\square$

For later use we extend the identity right before the lemma to polynomials in several variables. Let $f \in R[T_1, \dots, T_n]$, $f = \sum_{\boldsymbol{i}} a_{\boldsymbol{i}} T^{\boldsymbol{i}}$, and put

$$f^{\partial} := \sum_{\boldsymbol{i}} a'_{\boldsymbol{i}} T^{\boldsymbol{i}}.$$

Then $f \mapsto f^{\partial}$ is easily checked to be a derivation on $R[T_1, \dots, T_n]$.

**Lemma 4.2.** *Let $b = (b_1, \dots, b_n) \in R^n$ and $f \in R[T_1, \dots, T_n]$. Then*

$$f(b)' = f^{\partial}(b) + \sum_{i=1}^{n} \frac{\partial f}{\partial T_i}(b) \cdot b'_i.$$

We leave the proof as a routine exercise.

If $R$ is a differential domain (that is, the underlying ring of $R$ is a domain), then $\partial$ extends uniquely to a derivation of its fraction field by

$$(a/b)' := (a'b - ab')/b^2 \text{ for } a, b \in R,\ b \neq 0,$$

and we always consider the derivation of $R$ extended in this way. We actually need an easy variant of this fact:

**Lemma 4.3.** *Let $D$ be a domain with fraction field $F$ and let $\partial : D \to F$ be a derivation into $F$, that is, $\partial(a+b) = \partial(a) + \partial(b)$ and $\partial(ab) = \partial(a)b + a\partial(b)$ for all $a, b \in D$. Then $\partial$ extends uniquely to a derivation on $F$.*

For later use the reader should prove the following elementary facts by similar reasoning as before.

**Exercise.** Let $A$ be a subring of the ring $B$ and suppose the function $\partial : A \to B$ is a derivation of $A$ into $B$, that is, for all $x, y \in A$,

$$\partial(x+y) = \partial(x) + \partial(y), \quad \partial(xy) = x\partial(y) + \partial(x)y.$$

(i) If $A, B$ are domains with fraction fields $E \subseteq F$, respectively, then $\partial$ extends uniquely to a derivation of $E$ into $F$.
(ii) If $x, y \in B$ and $f(x) \neq 0$ for all nonzero $f \in A[T]$, then $\partial$ extends uniquely to a derivation $d$ of $A[x]$ into $B$ with $d(x) = y$.
(iii) If $A$ and $B$ are fields and $x \in B$ is separably algebraic over $A$, then $\partial$ extends uniquely to a derivation of $A[x]$ into $B$.
(iv) If $A$ and $B$ are fields, then $\partial$ extends to a derivation of $B$.

The *language of differential rings* is the language $\{0, 1, -, +, \cdot\}$ of rings augmented by an extra unary function symbol $\partial$. We view differential rings as structures for this language in the obvious way, and a "differential ring morphism" is just a map from a differential ring into a differential ring that is a morphism with respect to this language. Likewise, a differential subring of $R$ is a subring of $R$ closed under $\partial$, and is viewed as a substructure of $R$ with respect to the language of differential rings by restricting the derivation of $R$ to this subring.

If $S$ is a differential overring of $R$ (that is, $S$ is a differential ring with $R$ as differential subring), and $a \in S$, then

$$R[a]_{\mathrm{d}} := R[a, a', a'', \dots]$$

is easily seen to be the differential subring of $S$ generated by $a$ over $R$, in other words, the elements of $R[a]_{\mathrm{d}}$ have the form $f(a, a', \dots, a^{(n)})$ with $f(T_0, \dots, T_n) \in R[T_0, \dots, T_n]$.

**Simple extensions of differential fields.** In positive characteristic there are complications. A modified notion of derivation, called *Hasse derivation* is more appropriate in that case, but we shall not go there.

*We assume from now on that differential fields have characteristic zero.*

In the rest of this section $K$ is a differential field.

Consider an element $a$ in a differential field extension of $K$. Then $a$ is said to be *differentially algebraic over* $K$ if there is a nonzero polynomial $f \in K[T_0, \dots, T_n]$ (for some $n$) such that $f(a, a', \dots, a^{(n)}) = 0$; if there is no such $f$ (that is, $a, a', a'', \dots$ are algebraically independent over the field $K$), then we call $a$ *differentially transcendental over* $K$. If $b$ is also an element in a differential field extension of $K$ and $a$ and $b$ are both differentially transcendental over $K$, then by Lemma 4.2 we have a differential ring isomorphism $K[a]_{\mathrm{d}} \cong K[b]_{\mathrm{d}}$ that is the identity on $K$ and sends $a$ to $b$.

Suppose $a$ is differentially algebraic over $K$. Take $n$ minimal such that we have a nonzero polynomial $f(T_0, \dots, T_n) \in K[T_0, \dots, T_n]$ with

$$f(a, a', \dots, a^{(n)}) = 0.$$

Note that $f \notin K$ and $T_n$ appears in $f$. By factoring we can arrange that $f$ is irreducible in $K[T_0,\dots,T_n]$. The key point is that then $f$ completely determines the isomorphism type of $a$ over $K$. To explain what we mean by this, note that by the minimality of $n$ we have $g(a,a',\dots,a^{(n-1)}) \neq 0$ for all nonzero $g \in K[T_0,\dots,T_{n-1}]$. Let us call $f$ with these properties a *minimal polynomial of $a$ over $K$*; it is easily seen to be unique up to a factor from $K^\times$. A precise statement of the claim that $f$ determines the isomorphism type of $a$ over $K$ is as follows.

**Lemma 4.4.** *Let $a$ and $b$ in differential field extensions of $K$ be differentially algebraic over $K$ with common minimal polynomial $f \in K[T_0,\dots,T_n]$ over $K$, such that $T_n$ appears in $f$. Then there is a differential ring isomorphism $K[a]_{\mathrm{d}} \cong K[b]_{\mathrm{d}}$ that is the identity on $K$ and sends $a$ to $b$.*

*Proof.* Put $\vec{a} := (a,a',\dots,a^{(n)})$ and $\vec{b} := (b,b',\dots,b^{(n)})$. The ring morphism $h \mapsto h(\vec{a}) : K[T_0,\dots,T_n] \to K[\vec{a}]$ has kernel $fK[T_0,\dots,T_n]$, and likewise with $b$ instead of $a$, so we have a ring isomorphism $K[\vec{a}] \cong K[\vec{b}]$ over $K$ that sends $a^{(i)}$ to $b^{(i)}$ for $i = 0,\dots,n$. Lemma 4.2 gives

$$h(\vec{a})' \;=\; h^{\partial}(\vec{a}) + \sum_{i=0}^{n} \frac{\partial h}{\partial T_i}(\vec{a}) \cdot a^{(i+1)} \quad \text{for } h \in K[T_0,\dots,T_n].$$

Now $(\partial f/\partial T_n)(\vec{a}) \neq 0$, so for $h = f$ we obtain

$$a^{(n+1)} \;=\; -\frac{f^{\partial}(\vec{a}) + \sum_{i=0}^{n-1} (\partial f/\partial T_i)(\vec{a}) \cdot a^{(i+1)}}{(\partial f/\partial T_n)(\vec{a})} \in K(\vec{a}),$$

so $K[\vec{a}]' \subseteq K(\vec{a})$ (as sets), hence $K[\vec{a}] \subseteq K[a]_{\mathrm{d}} \subseteq K(\vec{a})$ (as rings). Likewise with $b$ instead of $a$, so the ring isomorphism above extends to a differential ring isomorphism as desired. ☐

We can also construct an element with a prescribed minimal polynomial:

**Lemma 4.5.** *Let $f \in K[T_0,\dots,T_n]$ be irreducible such that $T_n$ appears in $f$. Then there is an element $a$ in a differential field extension of $K$ such that $a$ is differentially algebraic over $K$ with minimal polynomial $f$ over $K$.*

*Proof.* We have $K[T_0,\dots,T_n]/(f) = K[t_0,\dots,t_n] = K[t]$, with $t_i := T_i + (f)$, $i = 0,\dots,n$ and $t = (t_0,\dots,t_n)$, so $K[t]$ is a domain with fraction field $K(t)$, and $f(t) = 0$ but $(\partial f/\partial T_n)(t) \neq 0$. We are going to extend $\partial$ to a derivation on $K(t)$ such that $t_i' = t_{i+1}$ for $0 \le i < n$. We first set

$$t_{n+1} := -\frac{f^{\partial}(t) + \sum_{i=0}^{n-1} (\partial f/\partial T_i)(t) \cdot t_{i+1}}{(\partial f/\partial T_n)(t)} \quad \text{in } K(t),$$

which by Lemma 4.2 is the value that $t_n'$ will necessarily have for any derivation on $K(t)$ extending $\partial$ with $t_i' = t_{i+1}$ for $0 \le i < n$. Next we define the additive map $d : K[T_0,\dots,T_n] \to K(t)$ by

$$d(h) := h^{\partial}(t) + \sum_{i=0}^{n} \frac{\partial h}{\partial T_i}(t) \cdot t_{i+1}.$$

As in the proof of Lemma 4.1 we check that $(f)$ is part of the kernel of $d$ and that the induced additive map

$$h(t) \mapsto h^{\partial}(t) + \sum_{i=0}^{n} \frac{\partial h}{\partial T_i}(t) \cdot t_{i+1} \ : \ K[t] \to K(t)$$

is a derivation into $K(t)$, which by Lemma 4.3 extends uniquely to a derivation on $K(t)$. This derivation extends $\partial$, and setting $a := t_0$ we have $a^{(i)} = t_i$ for $i = 0, \ldots, n$. This $a$ has the desired property. □

**Differentially closed fields.** A consequence of the last lemma is that if $T_n$ appears in $f \in K[T_0, \ldots, T_n]$, and $g \in K[T_0, \ldots, T_{n-1}] \setminus \{0\}$, then there is an $a$ in a differential field extension of $K$ such that

$$f(a, a', \ldots, a^{(n)}) = 0, \quad g(a, a', \ldots, a^{(n-1)}) \neq 0.$$

(This consequence does not mention irreducibility; to use the lemma, replace $f$ by an irreducible factor in $K[T_0, \ldots, T_n]$ in which $T_n$ appears.) Note that if $K$ is existentially closed as a differential field, such an $a$ already exists in $K$ itself.

We define $K$ to be *differentially closed* if for all $f$ and $g$ as above there is an $a \in K$ satisfying the above equation and inequation. By taking $n = 0$ we see that a differentially closed field is algebraically closed as a field. Also, existentially closed differential fields are differentially closed, and so every differential field embeds into a differentially closed field. Note that there is a set of universal-existential sentences in the language of differential rings whose models are exactly the differentially closed fields. We let DCF be the theory of differentially closed fields in this language.

**Theorem 4.6.** DCF *has* QE *and is complete.*

*Proof.* Let $E$ and $F$ be differentially closed fields such that $F$ is $|E|^+$-saturated, and let $R$ be a proper differential subring of $E$ and $\phi : R \to F$ an embedding. If $R$ is not a field we can extend $\phi$ to its fraction field inside $E$ (which is also a differential subfield of $E$). So assume $R$ is a differential field $K$. Take any $a \in E \setminus K$. Consider first the case that $a$ is differentially transcendental over $K$. By saturation we can take $b \in F$ differentially transcendental over the subfield $\phi(K)$ of $F$. Then $\phi$ extends to an embedding $K[a] \to F$ sending $a$ to $b$. Next assume that $a$ is differentially algebraic over $K$, and let $f \in K[T_0, \ldots, T_n]$, with $T_n$ appearing in $f$, be a minimal polynomial of $a$ over $K$, so

$$f(a, a', \ldots, a^{(n)}) = 0, \ g(a, a', \ldots, a^{(n-1)}) \neq 0 \text{ for all } g \in K[T_0, \ldots, T_{n-1}] \setminus K.$$

By saturation we can take $b \in F$ such that this equation and these inequations hold with $b$ instead of $a$ and with $f$ and the $g$'s replaced by their $\phi$-images. Then by Lemma 4.4 we can extend $\phi$ to an embedding of $K[a]_{\mathrm{d}}$ into $F$ that sends $a$ to $b$.

This finishes the proof that DCF has QE. The second part of the theorem now follows since the ring $\mathbb{Z}$ with the trivial derivation embeds into every differentially closed field. $\square$

The substructures of differentially closed fields are exactly the differential domains of characteristic zero, so DCF is by the above the model completion of the theory of differential domains of characteristic zero.

Let $\mathbb{U}$ be a differentially closed field, $K$ a differential subfield, and $x$ a variable. It follows from QE and Lemma 4.4 that $a, b \in \mathbb{U}$ realize the same $x$-type over $K$ in $\mathbb{U}$ iff they are either both differentially transcendental over $K$, or both differentially algebraic over $K$ with a common minimal polynomial over $K$. In particular, if $K$ is countable and $\mathbb{U}$ is big, there are only countably many $x$-types over $K$ realized in $\mathbb{U}$, and thus by the equivalence (1) $\Leftrightarrow$ (4) of Corollary 8.3 in *Introduction to model-theoretic stability*:

**Corollary 4.7.** DCF *is omega-stable.*

There are obvious analogies between ACF(0) and DCF; we shall see more of those, but DCF is less misleading as an example of an omega-stable theory.

From now on $\mathbb{U}$ is a differentially closed field and $C$ denotes its constant field, so $C$ is an algebraically closed field. Morley ranks and Morley degrees in this section are with respect to the model $\mathbb{U}$ of DCF. We shall see that $\mathrm{MR}(C) = 1$ and $\mathrm{MR}(\mathbb{U}) = \omega$, where $C$ and $\mathbb{U}$ are taken as definable sets in $\mathbb{U}$.

**Exercise.** $\{y \in \mathbb{U} : \ y^{(n)} = 0\}$ is a $C$-linear subspace of $\mathbb{U}$ of dimension $n$, and if $n > 0$ and $g \in \mathbb{U}[T_0, \dots, T_{n-1}] \setminus \{0\}$, then $g(y, y', \dots, y^{(n-1)}) \neq 0$ for some $y$ in this subspace.

**Definably closed and algebraically closed sets.** It is easy to characterize these sets in $\mathbb{U}$:

**Proposition 4.8.** *Let $K$ a differential subfield of $\mathbb{U}$. Then $K$ is definably closed in $\mathbb{U}$.*

*Proof.* By extending $\mathbb{U}$ if necessary we first arrange that $\mathbb{U}$ is $|K|^{+}$-saturated. Let $a \in \mathbb{U} \setminus K$. It suffices to show then there is a $b \in \mathbb{U}$ such that $a \neq b$ and $a$ and $b$ realize the same type over $K$ in $\mathbb{U}$. Assume first that $a$ is algebraic over $K$ (in the field sense), and let $f(T) \in K[T]$ be its minimum polynomial over $K$. Since $a \notin K$ the degree of $f$ is $> 1$, so $f$ has a zero $b \neq a$ in $\mathbb{U}$. Then $b$ has the desired property by the remarks preceding Corollary 4.7. Next, assume $a$ is transcendental and differentially algebraic over $K$. So it has a minimal polynomial $f \in K[T_0, \dots, T_n]$ with $n > 0$ and $T_n$ appearing in $f$. Given any nonzero polynomials $g_1, \dots, g_m \in K[T_0, \dots, T_{n-1}]$, the axioms of DCF guarantee the existence of a $t \in \mathbb{U}$ such that

$$f(t, \dots, t^{(n)}) = 0, \qquad g(t, \dots, t^{(n-1)}) \cdot (t - a) \neq 0, \quad g := g_1 \cdots g_m.$$

By saturation this gives $b \neq a$ in $\mathbb{U}$ such that $b$ is differentially algebraic over $K$ with minimal polynomial $f$ over $K$. Then $a$ and $b$ realize the same type over $K$ in $\Omega$. Finally, if $a$ is differentially transcendental over $K$ a similar argument gives $b \neq a$ in $\mathbb{U}$ such that $b$ is differentially transcendental over $K$, and then $a$ and $b$ realize the same type over $K$ in $\mathbb{U}$. □

**Proposition 4.9.** *Let $K$ be a differential subfield of $\mathbb{U}$ and suppose $K$ is algebraically closed as a field. Then $K$ is algebraically closed in $\mathbb{U}$ in the model theory sense.*

*Proof.* By extending $\mathbb{U}$ if necessary we first arrange that $\mathbb{U}$ is $|K|^+$-saturated. Let $a \in \mathbb{U} \setminus K$. It suffices to show then there are infinitely many $b \in \mathbb{U}$ that realize the same type as $a$ over $K$ in $\mathbb{U}$. The proof follows the steps in the proof of Proposition 4.8, but note that $a$ is not algebraic over $K$, so this case drops out. □

**Differential polynomials.** Let $R$ be a differential ring and $Y = (Y_i)_{i \in I}$ a family of distinct indeterminates. We define $R[Y]_{\mathrm{d}}$, the *ring of differential polynomials in $Y$ over $R$*, as follows. As a ring, $R[Y]_{\mathrm{d}}$ is just the polynomial ring $R[(Y_i^{(j)})]$ in distinct indeterminates $Y_i^{(j)}$ $(i \in I,\ j \in \mathbb{N})$ over $R$. (Of course, only finitely many of the $Y_i^{(j)}$ actually appear in any given differential polynomial $P(Y) \in R[Y]_{\mathrm{d}}$.) We make $R[Y]_{\mathrm{d}}$ into a differential overring of $R$ whose derivation, also denoted by $\partial$, is uniquely determined by the requirements that it extends the derivation $\partial$ of $R$ and satisfies

$$\partial(Y_i^{(j)}) = Y_i^{(j+1)}, \qquad (i \in I,\ j \in \mathbb{N}).$$

Note that if $R$ is a domain, so is $R[Y]_{\mathrm{d}}$. Likewise, if $R$ has no nonzero nilpotents, neither does $R[Y]_{\mathrm{d}}$, by an exercise in the previous section.

We continue with the case that $I$ is finite, say $I = \{1, \dots, n\}$, and then also denote $R[Y]_{\mathrm{d}}$ by $R[Y_1, \dots, Y_n]_{\mathrm{d}}$. For $y_1, \dots, y_n$ in a differential overring $S$ of $R$ we have a unique differential ring morphism

$$P(Y_1, \dots, Y_n) \mapsto P(y_1, \dots, y_n) \ : \ R[Y_1, \dots, Y_n]_{\mathrm{d}} \to S$$

that is the identity on $R$ and sends $Y_i$ to $y_i$, $i = 1, \dots, n$: $P(y_1, \dots, y_n)$ is just the element of $S$ obtained by substituting $y_i, y_i', y_i'', \dots$ for $Y_i, Y_i', Y_i'', \dots$ in $P(Y_1, \dots, Y_n) \in R[Y_1, \dots, Y_n]_{\mathrm{d}}$, for $i = 1, \dots, n$. We let $R[y_1, \dots, y_n]_{\mathrm{d}}$ be the image of this differential ring morphism, so $R[y_1, \dots, y_n]_{\mathrm{d}}$ is the differential subring of $S$ generated by $y_1, \dots, y_n$ over $R$.

If $E$ is a differential overfield of $K$ and $y = (y_1, \dots, y_n) \in E^n$, then $K(y)_{\mathrm{d}}$ denotes the fraction field of $K[y]_{\mathrm{d}}$ inside $E$, so $K(y)_{\mathrm{d}}$ is the differential subfield of $E$ generated by $y_1, \dots, y_n$ over $K$, and its elements are the $P(y)/Q(y)$ such that $P, Q \in K[Y_1, \dots, Y_n]_{\mathrm{d}}$ with $Q(y) \neq 0$.

We can now state some easy consequences of Propositions 4.8 and 4.9, in terms of the closure operations dcl and acl in our ambient $\mathbb{U}$.

**Corollary 4.10.** *Let $K$ be a differential subfield of $\mathbb{U}$ and consider a point $a = (a_1, \dots, a_n) \in \mathbb{U}^n$. Then*

(1) $\mathrm{dcl}(Ka)$ *is the underlying set of* $K(a)_{\mathrm{d}}$*;*
(2) $\mathrm{acl}(Ka)$ *is the underlying set of the algebraic closure in the field sense of* $K(a)_{\mathrm{d}}$ *in* $\mathbb{U}$*.*

Item (1) yields a differential analogue of Corollary 2.5:

**Corollary 4.11.** *Let* $K$ *be a differential subfield of* $\mathbb{U}$*, and let* $X \subseteq \mathbb{U}^n$ *and* $f : X \to \mathbb{U}$ *be* $K$*-definable in* $\mathbb{U}$*. Then there are* $g_1, \ldots, g_k, h_1, \ldots, h_k \in K[Y_1, \ldots, Y_n]_{\mathrm{d}}$ *such that for each* $y \in X$ *there is* $i \in \{1, \ldots, k\}$ *with* $h_i(y) \neq 0$ *and* $f(y) = g_i(y)/h_i(y)$*.*

**Exercise.** Let $K$ be a differential subfield of $\mathbb{U}$ and let $S \subseteq \mathbb{U}$ be definable in $\mathbb{U}$ over $K$. Then $S$ is finite iff $S \subseteq \{a \in \mathbb{U} : f(a) = 0\}$ for some $f \in K[T] \setminus \{0\}$.

In terms of differential polynomials QE for DCF means the following:

**Corollary 4.12.** *Let* $K$ *be a differential subfield of* $\mathbb{U}$*. Then the subsets of* $\mathbb{U}^n$ *that are* $K$*-definable in* $\mathbb{U}$ *are exactly the boolean combinations inside* $\mathbb{U}^n$ *of the sets*

$$\{y \in \mathbb{U}^n : P(y) = 0\}, \quad P \in K[Y]_{\mathrm{d}},\ Y = (Y_1, \ldots, Y_n).$$

Just as with ordinary polynomials we have:

**Lemma 4.13.** *Let* $E$ *be a differential overfield of* $K$*, and* $P \in E[Y]_{\mathrm{d}}$*,* $Y = (Y_1, \ldots, Y_n)$*. Then there are* $P_1, \ldots, P_m \in K[Y]_{\mathrm{d}}$ *such that for all* $y \in K^n$*,*

$$P(y) = 0 \iff P_1(y) = \cdots = P_m(y) = 0.$$

The proof is the same as that of Lemma 3.1. As a consequence, the structure induced by $\mathbb{U}$ on $C$ is just the field structure of $C$:

**Corollary 4.14.** *Suppose* $S \subseteq \mathbb{U}^n$ *is definable in* $\mathbb{U}$*. Then* $S \cap C^n$ *is definable in the field* $C$*.*

*Proof.* By QE we reduce to the case that $S = \{y \in \mathbb{U}^n : P(y) = 0\}$ where $P \in \mathbb{U}[Y]_{\mathrm{d}}$, $Y = (Y_1, \ldots, Y_n)$. Now apply the previous lemma with $K = C$. □

The fact that $\mathbb{U}$ induces on the field $C$ no extra structure is important. Here is one consequence that we shall need later in the proof of "Mordell-Lang for function fields of characteristic zero".

**Lemma 4.15.** *Let* $X \subseteq C^m$ *be definable in* $\mathbb{U}$*, let* $Y \subseteq \mathbb{U}^n$ *be definable in* $\mathbb{U}$ *as algebraically closed field, and let* $f : X \to Y$ *be definable in* $\mathbb{U}$*. Then* $f$ *extends to a map* $f' : X' \to Y$ *where* $X \subseteq X' \subseteq X(\mathbb{U})$ *and* $X'$ *and* $f'$ *are definable in* $\mathbb{U}$ *as algebraically closed field.*

*Proof.* We can assume that $\mathbb{U}$ is big. Take a small differential subfield $K$ of $\mathbb{U}$ such that $X$, $Y$, and $f$ are definable over $K$ in $\mathbb{U}$. If $a \in X$, then $a \in C^m$, so $K(a)_{\mathrm{d}} = K(a)$ is the definable closure of $Ka$ in $\mathbb{U}$, hence $f(a) \in K(a)^n$, and so there are $f_1, \dots, f_n, g \in K[T_1, \dots, T_n]$ with $g(a) \neq 0$ such that

$$f(a) = \frac{1}{g(a)}\big(f_1(a), \dots, f_n(a)\big).$$

Saturation yields a finite partition of $X$ into disjoint subsets $X_1, \dots, X_N$ that are definable in the algebraically closed field $\mathbb{U}$, such that for $i = 1, \dots, N$ we have polynomials $f_{i1}, \dots, f_{in}, g_i \in K[T_1, \dots, T_n]$ with the property that $g_i$ has no zero in $X_i$ and for all $a \in X_i$,

$$f(a) = \frac{1}{g_i(a)}\big(f_{i1}(a), \dots, f_{in}(a)\big).$$

For $i = 1, \dots, N$ we have $X_i \subseteq C^m$, so $X_i$ is definable in $C$, and we put

$$X_i' := \{a \in X_i(\mathbb{U}) : \ \frac{1}{g_i(a)}\big(f_{i1}(a), \dots, f_{in}(a)\big) \in Y\},$$

Set $X' := X_1' \cup \dots \cup X_N'$, and define $f' : X' \to Y$ by

$$f'(a) := \frac{1}{g_i(a)}\big(f_{i1}(a), \dots, f_{in}(a)\big) \qquad \text{for } a \in X_i',\ i = 1, \dots, N.$$

$\square$

**Remark**. By Corollary 4.14 the set $C \subseteq \mathbb{U}$ is strongly minimal in $\mathbb{U}$, that is, $\mathrm{MR}(C) = 1$, $\mathrm{MD}(C) = 1$. By the Exercise following Corollary 4.7 we have for each $n$ a $C$-linear bijection from $C^n \subseteq \mathbb{U}^n$ onto the $C$-linear subspace

$$\mathrm{Z}(Y^{(n)}) := \{y \in \mathbb{U} : \ y^{(n)} = 0\}$$

of $\mathbb{U}$, so $\mathrm{MR}\big(\mathrm{Z}(Y^{(n)})\big) = n$, $\mathrm{MD}\big(\mathrm{Z}(Y^{(n)})\big) = 1$. It follows that $\mathrm{MR}(\mathbb{U}) \geq \omega$. The reverse inequality will be established later.

Let $R$ be a differential ring and $Y$ a single indeterminate. Given $f(Y) \in R[Y]_{\mathrm{d}}$ with $f \notin R$, the smallest $r \in \mathbb{N}$ such that $f(Y) \in R[Y, Y', \dots, Y^{(r)}]$ is called the **order** of the differential polynomial $P$ and denoted by $\operatorname{ord} f$. For $f \in R \subseteq R[Y]_{\mathrm{d}}$ we set $\operatorname{ord} f := -\infty$.

Suppose $a$ in a differential field extension of $K$ is differentially algebraic over $K$ with minimal polynomial $F \in K[T_0, \dots, T_n]$ over $K$ where $T_n$ appears in $F$. The ordinary polynomial $F$ plays here the role of the differential polynomial $f(Y) := F(Y, Y', \dots, Y^{(n)}) \in K[Y]_{\mathrm{d}}$, and we also call $f$ a *minimal differential polynomial* of $a$ over $K$. Then $\operatorname{ord} f = n$, and $f$ is irreducible in the unique factorization domain $K[Y]_{\mathrm{d}}$, and $K(a)_{\mathrm{d}} = K(a, \dots, a^{(n)})$ with $\operatorname{trdeg}_K K(a)_{\mathrm{d}} = n$.

**Lemma 4.16.** *Let $K$ be a differential subfield of $\mathbb{U}$ and let $S \subseteq \mathbb{U}$ be definable in $\mathbb{U}$ over $K$. Then $S$ is infinite iff $S \supseteq \{a \in \mathbb{U} : \ f(a) = 0,\ g(a) \neq 0\}$ for some $f, g \in K[Y]_{\mathrm{d}}$ with $0 \leq \operatorname{ord} g < \operatorname{ord} f$.*

*Proof.* By passing to some elementary extension of $\mathbb{U}$ we can assume that $\mathbb{U}$ is $|K|^+$-saturated. Suppose $S$ is infinite. Then

$$|S| = |\mathbb{U}| > |\operatorname{acl}(K)| = |K|,$$

so $S$ has an element $a$ that is not algebraic over $K$. Consider first the case that $a$ is differentially transcendental over $K$. Then our earlier quantifier-free description of $\operatorname{tp}(a|K)$ gives a $g \in K[Y]_{\mathrm{d}}$ with $g \notin K$ such that

$$S \supseteq \{a \in \mathbb{U} : \ g(a) \neq 0\}.$$

Take any $f \in K[Y]_{\mathrm{d}}$ with $\operatorname{ord} g < \operatorname{ord} f$. Then

$$S \supseteq \{a \in \mathbb{U} : \ f(a) = 0, \ g(a) \neq 0\}.$$

Next, assume $a$ is differentially algebraic over $K$ with minimal differential polynomial $f \in K[Y]_{\mathrm{d}}$ over $K$. Then $\operatorname{ord} f > 0$ and our earlier quantifier-free description of $\operatorname{tp}(a|K)$ gives the existence of $g \in K[Y]_{\mathrm{d}}$ such that

$$0 \leq \operatorname{ord} g < \operatorname{ord} f, \qquad S \supseteq \{a \in \mathbb{U} : \ f(a) = 0, \ g(a) \neq 0\}.$$

The other direction of the lemma is clear from earlier results. $\square$

**Corollary 4.17.** *Let $S \subseteq \mathbb{U}^{n+1}$ be definable in $\mathbb{U}$. Then there is $m$ such that for all $a \in \mathbb{U}^n$, either $|S(a)| \leq m$ or $S(a)$ is infinite.*

*Proof.* We can reduce to the case that $S$ is 0-definable and $\mathbb{U}$ is $\aleph_0$-saturated. The set of $a \in \mathbb{U}^n$ for which $S(a)$ is finite is both a union of 0-definable subsets of $\mathbb{U}^n$ and an intersection of 0-definable subsets of $\mathbb{U}^n$: this follows from the previous lemma with $K = \mathbb{Q}(a)_{\mathrm{d}}$. Thus the set of such $a$ is 0-definable. $\square$

**Differential ideals and division.** In this subsection $R$ is differential ring. A *differential ideal* of $R$ is an ideal $I$ of $R$ such that $\partial I \subseteq I$. Given any subset $A$ of $R$ the differential ideal generated by $A$ in $R$ (that is, the smallest differential ideal of $R$ that contains $A$) is the ideal of $R$ generated by the $a^{(n)}$ with $a \in A$, and is denoted by $[A]$. When $A = \{a_1, \dots, a_m\} \subseteq R$, this differential ideal $[A]$ is also denoted by $[a_1, \dots, a_m]$. If $I$ is a differential ideal of $R$, then we regard the residue ring $R/I$ as a differential ring by setting $(a/I)' := a'/I$ for $a \in R$, so that the map

$$a \mapsto a/I \ : \ R \to R/I$$

is a differential ring morphism with kernel $I$. Conversely, the kernel of a differential ring morphism from $R$ into a differential ring is a differential ideal of $R$.

Division with remainder for polynomials causes a drop in degree. This is the key to the algebraic properties of polynomial rings, in particular to Hilbert's basis theorem for polynomial ideals. In this subsection we derive an analogue of division for *differential* polynomials.

Fix a differential indeterminate $Y$. Let $P \in R[Y]_{\mathrm{d}}$ with $P \notin R$. Let $m = \operatorname{ord} P$, call $Y^{(m)}$ the *leader* of $P$ and denote it by $u_P$, so with $u = u_P$,

$$P = a_d u^d + a_{d-1} u^{d-1} + \cdots + a_0, \qquad a_0, \ldots, a_d \in R[Y, \ldots, Y^{(m-1)}],\ a_d \neq 0.$$

We put $d_P := d$, the degree of $P$ as a polynomial in $u_P$, and we also define

$$i_P := a_d \qquad \text{(the } \textit{initial} \text{ of } P\text{)},$$
$$s_P := \frac{\partial P}{\partial u_P} \qquad \text{(the } \textit{separant} \text{ of } P\text{), so } \ s_P = d a_d u^{d-1} + \cdots + a_1.$$

**Example.** Let $P = (Y')^3 - Y''(Y''')^2 + (Y')^2 Y''' \in K[Y]_{\mathrm{d}}$. Then

$$u_P = Y''',\ d_P = 2,\ i_P = -Y'',\ s_P = -2Y''Y''' + (Y')^2.$$

We define a strict partial order $<$ on $R[Y]_{\mathrm{d}}$ as follows: for $P, Q \in R[Y]_{\mathrm{d}}$,

$$P < Q \ :\Longleftrightarrow \ \text{either } \operatorname{ord} P < \operatorname{ord} Q, \text{ or } 0 \leq \operatorname{ord} P = \operatorname{ord} Q \text{ and } d_P < d_Q,$$

in particular, if $P \in R$, then

$$P < Q \iff Q \notin R.$$

If $P \in R[Y]_{\mathrm{d}},\ P \notin R$, then $i_P < P$, $s_P < P$, and with $u := u_P$,

$$P = i_P u^d + Q, \quad Q \in R[Y]_{\mathrm{d}},\ Q < P,$$

and by an easy induction on $i \geq 1$,

$$P^{(i)} \ = \ s_P u^{(i)} + P_i, \quad P_i \in R[Y]_{\mathrm{d}},\ P_i < u^{(i)}.$$

A key fact about this partial ordering is that there is no infinite strictly decreasing sequence in $R[Y]_{\mathrm{d}}$.

The next result is Ritt's analogue for differential polynomials of division with remainder. The proof is constructive.

**Theorem 4.18.** *Let $F, G \in R[Y]_{\mathrm{d}}$, $F \notin R$. Then*

$$i_F^p s_F^q G \ \equiv \ G^* \mod [F]$$

*for some $p, q \in \mathbb{N}$ and $G^* \in R[Y]_{\mathrm{d}}$ with $G^* < F$.*

*Proof.* By induction on $\operatorname{ord} G$. If $G < F$ we can take $p = q = 0$ and $G^* = G$. If $\operatorname{ord} G = \operatorname{ord} F = m$ and $d_G \geq d_F$, then ordinary division by $F$ in the polynomial ring $R[Y, \ldots, Y^{(m)}]$ yields

$$i_F^p G = QF + G^*, \qquad p = 1 + d_G - d_F,\ Q, G^* \in R[Y, \ldots, Y^{(m)}],\ G^* < G,$$

and we are done. It remains to consider the case that $\operatorname{ord} G > \operatorname{ord} F = m$, say $\operatorname{ord} G = m + i$, $i \geq 1$. We shall prove that

$$i_F^p s_F^q G \ \equiv \ G^* \mod (F, F', \ldots, F^{(i)}) \text{ in the ring } R[Y, \ldots, Y^{(m+i)}]$$

for suitable $p, q \in \mathbb{N}$ and $G^* \in R[Y]_{\mathrm{d}}$ with $G^* < F$. Set $u := u_F$. Then

$$F^{(i)} = s_F u^{(i)} + F_i, \quad F_i \in R[Y]_{\mathrm{d}},\ \operatorname{ord} F_i < m + i.$$

Ordinary division by $F^{(i)}$ in the polynomial ring $R[Y,\dots,Y^{(m+i)}]$ gives

$$s_F^d G = Q_i F^{(i)} + G_i, \quad d = d_G,\ Q_i, G_i \in R[Y]_{\mathrm{d}},\ \operatorname{ord} G_i < m+i.$$

Inductively, assume that we have $p, q \in \mathbb{N}$ and $G_i^* \in R[Y]_{\mathrm{d}}$ such that

$$i_F^p s_F^q G_i \equiv G^* \mod (F,\dots,F^{(i-1)}), \quad G^* < F.$$

with the ideal $(F,\dots,F^{(i-1)})$ taken in $R[Y,\dots,Y^{(m+i-1)}]$. In combination with the previous identity this gives, with $d = d_G$,

$$i_F^p s_F^{d+q} G \equiv G^* \mod (F,\dots,F^{(i)})$$

with the ideal $(F,\dots,F^{(i)})$ taken in $R[Y,\dots,Y^{(m+i)}]$. □

**Remark.** The proof shows that if we ask only that $\operatorname{ord} G^* \le \operatorname{ord} F$ rather than $G^* < F$, then we can take $p = 0$.

**The $\partial$-basis theorem and the $\partial$-topology.** Let $K$ be a differential subfield of $\mathbb{U}$ in this subsection. For any set $S \subseteq K[Y_1,\dots,Y_n]_{\mathrm{d}}$ of differential polynomials we put

$$\mathrm{Z}(S) := \{y \in \mathbb{U}^n :\ P(y) = 0 \text{ for all } P \in S\}.$$

As in the case of the Zariski topology we see that these sets $Z(S)$ are the closed sets of a topology on $\mathbb{U}^n$, called the $(\partial, K)$-topology of $\mathbb{U}^n$. The main aim of this section is to show:

**Theorem 4.19.** *$\mathbb{U}^n$ with the $(\partial, K)$-topology is a noetherian space.*

For $F_1,\dots,F_m \in K[Y_1,\dots,Y_n]_{\mathrm{d}}$ we put

$$\mathrm{Z}(F_1,\dots,F_m) := \mathrm{Z}(\{F_1,\dots,F_m\}) = \{a \in \mathbb{U}^n :\ F_1(a) = \cdots = F_m(a) = 0\}.$$

Theorem 4.19 says that any set $S \subseteq K[Y_1,\dots,Y_n]_{\mathrm{d}}$ has elements $F_1,\dots,F_m$ such that $\mathrm{Z}(S) = \mathrm{Z}(F_1,\dots,F_m)$.

Noetherianity of the Zariski topology came from Hilbert's basis theorem for polynomial ideals. Likewise, the theorem above will follow from a basis theorem for the differential polynomial ring $K[Y_1,\dots,Y_n]_{\mathrm{d}}$ due to Ritt and Raudenbusch; but in contrast to Hilbert's basis theorem we need to restrict attention to *radical* differential ideals.

*In the rest of this subsection $R$ is a differential ring containing $\mathbb{Q}$ as a subring.*

**Lemma 4.20.** *Let $I$ be a differential ideal of $R$. Then $\sqrt{I}$ is a differential ideal of $R$.*

*Proof.* First, for $a \in R$ and $1 \le i \le n$, induction on $i$ gives

$$a^{n-i}(a')^{2i-1} \in \sum_{j=0}^{i} \mathbb{Q}[a, a', \dots, a^{(i)}](a^n)^{(j)}.$$

If $a^n \in I$, then $i = n$ gives $(a')^{2n-1} \in I$. □

**Lemma 4.21.** *Let $I$ be a radical differential ideal of $R$ and $a \in R$. Then the ideal $I : a := \{b \in R : ab \in I\}$ is a radical differential ideal of $R$.*

*Proof.* Let $b \in I : a$. Then $ab \in I$, so $ab' + a'b \in I$, and multiplication by $ab'$ gives $(ab')^2 \in I$, so $ab' \in I$, so $b' \in I : a$. Thus $I : a$ is a differential ideal of $R$, and is clearly radical since $I$ is. $\square$

**Lemma 4.22.** *Let $S, T$ be subsets of $R$. Then $\sqrt{[S]} \cdot \sqrt{[T]} \subseteq \sqrt{[ST]}$.*

*Proof.* Let $a \in \sqrt{[S]}$; we wish to show $a\sqrt{[T]} \subseteq \sqrt{[ST]}$, that is, $\sqrt{[T]} \subseteq \sqrt{[ST]} : a$. By the previous lemma, $\sqrt{[ST]} : a$ is a radical differential ideal, so it is enough to show that $T \subseteq \sqrt{[ST]} : a$. So, given $b \in T$, it remains to show that $ab \in \sqrt{[ST]}$, that is, $a \in \sqrt{[ST]} : b$. But $\sqrt{[ST]} : b$ is a radical differential ideal and contains $S$, so contains $a$. $\square$

**Lemma 4.23.** *Let $I$ be a radical differential ideal of $R$. Then $I$ is an intersection of prime differential ideals of $R$.*

*Proof.* Let $s \in R \setminus I$; it is enough to show that then there is a prime differential ideal $\mathfrak{p} \supseteq I$ of $R$ such that $s \notin \mathfrak{p}$. To obtain $\mathfrak{p}$, note first that $I$ is disjoint from the multiplicative set $S := \{1, s, s^2, \dots\}$. Let $\mathfrak{p}$ be maximal among the differential ideals of $R$ that contain $I$ and are disjoint from $S$. Then $S \cap \sqrt{\mathfrak{p}} = \emptyset$, so $\mathfrak{p} = \sqrt{\mathfrak{p}}$ is radical. In fact, $\mathfrak{p}$ is prime. Otherwise, take $a, b \in R \setminus \mathfrak{p}$ with $ab \in \mathfrak{p}$, so we can take $m, n$ such that $s^m \in [\mathfrak{p} \cup \{a\}]$ and $s^n \in [\mathfrak{p} \cup \{b\}]$, so

$$s^{m+n} \in [\mathfrak{p} \cup \{a\}][\mathfrak{p} \cup \{b\}] \subseteq \sqrt{[\mathfrak{p} \cup \{ab\}]} = \mathfrak{p}$$

by the previous lemma, and we have a contradiction. $\square$

A *basis* of a radical differential ideal $I$ of $R$ is a *finite* set $B \subseteq R$ such that $I = \sqrt{[B]}$. As with ordinary noetherianity the usual arguments show that the following two conditions are equivalent:

(1) Every radical differential ideal of $R$ has a basis.
(2) *Ascending chain condition for radical differential ideals of $R$*: there is no strictly increasing infinite sequence $I_0 \subset I_1 \subset I_2 \subset \dots$ of radical differential ideals of $R$.

**Exercise.** If $S$ is a subset of $R$, $a \in R$, and $\sqrt{[S \cup \{a\}]}$ has a basis, then it has a basis $\{s_1, \dots, s_m, a\}$ with $s_1, \dots, s_m \in S$.

We now fix a differential indeterminate $Y$ and recall from the subsection on differential polynomials that if $R$ has no nonzero nilpotents, then $R[Y]_{\mathrm{d}}$ has no nonzero nilpotents. We now have things ready for the $\partial$-basis theorem.

**Theorem 4.24.** *Assume that every radical differential ideal of $R$ has a basis. Then every radical differential ideal of $R[Y]_{\mathrm{d}}$ has a basis.*

*Proof.* Let $I$ be a radical differential ideal of $R[Y]_{\mathrm{d}}$. If $1 \in I$, then $\{1\}$ is a basis of $I$, so assume $1 \notin I$. Then $I \cap R$ is a radical differential ideal of $R$, and thus has a basis $\{b_1, \dots, b_m\}$. The image of $I$ under the natural morphism

$R[Y]_{\mathrm{d}} \to (R/I \cap R)[Y]_{\mathrm{d}}$ is a radical differential ideal of $(R/I \cap R)[Y]_{\mathrm{d}}$, and if $\{c_1, \dots, c_n\} \subseteq R[Y]_{\mathrm{d}}$ is such that its image under this morphism is a basis of the image of $I$ in $(R/I \cap R)[Y]_{\mathrm{d}}$ under this morphism, then $\{b_1, \dots, b_m, c_1, \dots, c_n\}$ is a basis of $I$. Thus we can work modulo $I \cap R$: replace $R$ by $R/I \cap R$ and $I$ by its image under the natural morphism $R[Y]_{\mathrm{d}} \to (R/I \cap R)[Y]_{\mathrm{d}}$. After renaming we are in the case that $I \cap R = \{0\}$ and $R$ has no nonzero nilpotents. With this assumption, we are done if $I$ is the trivial ideal, so assume $I \neq \{0\}$. Take a nonzero $F \in I$ such that there is no nonzero $G \in I$ with $G < F$. Note that $F \notin R$, so $d := d_F > 0$.

We proceed by induction on the quantity $(\operatorname{ord} F, d) \in \mathbb{N}^2$, which depends only on $I$ and not on the choice of $F$. Setting $u := u_F$ we have

$$\begin{aligned} s_F &= i_F \cdot du^{d-1} + f, \quad \text{where } f \in R[Y]_d,\ \deg_u f < d-1, \text{ so} \\ i_F s_F &= i_F^2 \cdot du^{d-1} + i_F f. \end{aligned}$$

Now $i_F \neq 0$ and $R$ has no nonzero nilpotents, so $i_F^2 \neq 0$. In view of $\mathbb{Q} \subseteq R$, it follows easily that $i_F s_F \neq 0$. Also $i_F s_F < F$, hence $i_F s_F \notin I$. Inductively we can therefore assume that $\sqrt{[I \cup \{i_F s_F\}]}$ has a basis; by the exercise preceding the theorem we can assume it has a basis $\{F_1, \dots, F_n, i_F s_F\}$ with $F_1, \dots, F_n \in I$. We shall prove that then $\{F, F_1, \dots, F_n\}$ is a basis of $I$.

**Claim.** $i_F s_F I \subseteq \sqrt{[F]}$. To see why, let $G \in I$, so by Theorem 4.18,

$$i_F^p s_F^q G = G^* + H, \qquad p, q \in \mathbb{N},\ G^*, H \in R[Y]_{\mathrm{d}},\ G^* < F,\ H \in [F].$$

Then $G^* \in I$, so $G^* = 0$, hence $i_F^p s_F^q G \in [F]$, and thus $i_F s_F G \in \sqrt{[F]}$.

This claim and Lemma 4.22 give for $P \in I$,

$$\begin{aligned} P^2 \in I\sqrt{[I \cup \{i_F s_F\}]} &\subseteq I\sqrt{[F_1, \dots, F_n, i_F s_F]} \\ &\subseteq \sqrt{[F_1 I \cup \dots \cup F_n I \cup i_F s_F I]} \subseteq \sqrt{[F, F_1, \dots, F_n]}, \end{aligned}$$

so $P \in \sqrt{[F, F_1, \dots, F_n]}$. This gives

$$I = \sqrt{[F, F_1, \dots, F_n]},$$

so $\{F, F_1, \dots, F_n\}$ is a basis of $I$ as promised. $\square$

This proof is close to the usual one, but is more constructive by indicating how a basis might be obtained under suitable conditions.

**Corollary 4.25.** *Every radical differential ideal of $K[Y_1, \dots, Y_n]_{\mathrm{d}}$ has a basis.*

This follows from Theorem 4.24 by induction on $n$, starting with the trivial case $n = 0$. In particular, the ascending chain condition for radical differential ideals of $K[Y_1, \dots, Y_n]_{\mathrm{d}}$ is satisfied. Now, $K$ being a differential subfield of $\mathbb{U}$, we assign to each $(\partial, K)$-closed set $C \subseteq \mathbb{U}^n$ the radical differential ideal

$$\mathrm{I}_K(C) := \{F \in K[Y_1, \dots, Y_n]_{\mathrm{d}} :\ F(y) = 0 \text{ for all } y \in C\}$$

of $K[Y_1,\dots,Y_n]_{\mathrm{d}}$, so $\mathrm{Z}(\mathrm{I}_K(C)) = C$. The ascending chain condition on radical differential ideals of $K[Y_1,\dots,Y_n]_{\mathrm{d}}$ now yields the descending chain condition on $(\partial, K)$-closed subsets of $\mathbb{U}^n$, and so Theorem 4.19 is established.

If the radical differential ideal $I$ of $K[Y_1,\dots,Y_n]_{\mathrm{d}}$ has basis $\{F_1,\dots,F_m\}$, then $\mathrm{Z}(I) = \mathrm{Z}(F_1,\dots,F_m)$. In particular, every $(\partial, K)$-closed set in $\mathbb{U}^n$ is definable in $\mathbb{U}$ over $K$. As in the case of algebraically closed fields we have:

**Proposition 4.26.** *If $I$ is a differential ideal of $K[Y_1,\dots,Y_n]_{\mathrm{d}}$, then*

$$\mathrm{I}_K(\mathrm{Z}(I)) = \sqrt{I}.$$

*The set of radical differential ideals of $K[Y_1,\dots,Y_n]_{\mathrm{d}}$ is in bijective correspondence with the set of $(\partial, K)$-closed subsets of $\mathbb{U}^n$, by $I \mapsto \mathrm{Z}(I)$, with inverse $C \mapsto \mathrm{I}_K(C)$, and under this bijection the prime differential ideals of $K[Y_1,\dots,Y_n]_{\mathrm{d}}$ correspond to the irreducible $(\partial, K)$-closed subsets of $\mathbb{U}^n$.*

The proof is similar to that of Proposition 3.5 and its corollary, using that each prime differential ideal of $K[Y_1,\dots,Y_n]_{\mathrm{d}}$ has a basis, and the following general fact.

**Lemma 4.27.** *Assume that every radical differential ideal of $R$ has a basis. Then every radical differential ideal is an intersection of finitely many prime differential ideals of $R$.*

*Proof.* Otherwise, take a radical differential ideal $I$ of $R$ that is maximal among the radical differential ideals that are not intersections of finitely many prime differential ideals of $R$. In particular, $I \neq R$ and $I$ is not prime, so we can take $a, b \in R$ with $ab \in I$ and $a, b \notin I$. Then every prime differential ideal of $R$ containing $I$ contains $a$ or $b$. To get a contradiction, represent $\sqrt{[I \cup \{a\}]}$ and $\sqrt{[I \cup \{b\}]}$ as finite intersections of prime differential ideals of $R$, and use that by Lemma 4.23 we have $I = \sqrt{[I \cup \{a\}]} \cap \sqrt{[I \cup \{b\}]}$. $\square$

**Elimination of imaginaries for** DCF**.** The $(\partial, \mathbb{U})$-topology on $\mathbb{U}^n$ is also called its $\partial$-topology.

**Theorem 4.28.** DCF *admits elimination of imaginaries.*

*Proof.* Let $\mathbb{U}$ be a big differentially closed field. To show that DCF has EI, let $X \subseteq \mathbb{U}^n$ be any definable set; it suffices to show that then $X$ has a code in $\mathbb{U}$. By Lemma 3.8 we reduce to the case that $X$ is $\partial$-closed in $\mathbb{U}^n$. In this case we put

$$I := \mathrm{I}_{\mathbb{U}}(X) = \{F \in \mathbb{U}[Y_1,\dots,Y_n]_{\mathrm{d}} : F(a) = 0 \text{ for all } a \in X\}.$$

Extend each $\sigma \in \mathrm{Aut}(\mathbb{U})$ to an automorphism, also denoted by $\sigma$, of the differential ring $\mathbb{U}[Y_1,\dots,Y_n]_{\mathrm{d}}$ by requiring $\sigma(Y_i) = Y_i$ for $i = 1,\dots,n$. Then for all $\sigma \in \mathrm{Aut}(\mathbb{U})$,

$$\sigma(I) = I \iff \sigma(X) = X.$$

Take a basis $B$ of $I$, and take a natural number $p$ so large that

$$B \subseteq \mathbb{U}[Y_i^{(j)} : \ i = 1,\dots,n, j = 0,\dots,p],$$

and put $I(p) := I \cap \mathbb{U}[Y_i^{(j)}:\ i=1,\dots,n,\ j=0,\dots,p]$, so $I = \sqrt{[I(p)]}$, and thus for all $\sigma \in \mathrm{Aut}(\mathbb{U})$,

$$\sigma\big(I(p)\big) = I(p) \iff \sigma(I) = I.$$

By the remarks following Proposition 2.14 we can take $a \in \mathbb{U}^N$, for some natural number $N$, such that for all field automorphisms $\sigma$ of $\mathbb{U}$ we have

$$\sigma(a) = a \iff \sigma\big(I(p)\big) = I(p).$$

Then $a$ codes $X$ by the above. □

**Differential prime ideals of $K[Y]_{\mathrm{d}}$.** In this subsection $Y$ is a single indeterminate. Suppose $a$ in a differential field extension of $K$ is differentially algebraic over $K$ with minimal differential polynomial $F \in K[Y]_{\mathrm{d}}$ over $K$ of order $n$. We define

$$\mathfrak{p}_K(a) := \{G \in K[Y]_{\mathrm{d}}:\ G(a) = 0\},$$

a differential prime ideal of $K[Y]_{\mathrm{d}}$.

**Lemma 4.29.** $\mathfrak{p}_K(a) = \sqrt{[F]} : s_F$. *For every nonzero differential prime ideal* $\mathfrak{p}$ *of* $K[Y]_{\mathrm{d}}$ *there is a* $b$ *in a differential field extension of* $K$ *such that* $b$ *is differentially algebraic over* $K$ *and* $\mathfrak{p} = \mathfrak{p}_K(b)$.

*Proof.* From $F(a) = 0$ and $s_F(a) \neq 0$ we get $\mathfrak{p}_K(a) \supseteq \sqrt{[F]} : s_F$. For the reverse inclusion, let $G \in \mathfrak{p}_K(a)$. By the remark following Theorem 4.18,

$$s_F^q G \equiv G^* \mod [F], \text{ where } q \in \mathbb{N},\ G^* \in K[Y]_{\mathrm{d}},\ \operatorname{ord} G^* \leq \operatorname{ord} G.$$

Then $G^*(a) = 0$, and so $G^* \in FK[Y,\dots,Y^{(n)}]$, using Lemmas 4.4 and 4.5 and their proof. Hence $s_F^q G \in [F]$, and thus $G \in \sqrt{[F]} : s_F$.

Let $\mathfrak{p}$ be a nonzero differential prime ideal of $K[Y]_{\mathrm{d}}$. Take a nonzero $\Phi \in \mathfrak{p}$ such that there is no $G \in \mathfrak{p}$ with $G < \Phi$. Then $\Phi \in K[Y]_{\mathrm{d}}$ is irreducible. By Lemma 4.5 we can take $b$ in a differential field extension of $K$ such that $b$ is differentially algebraic over $K$ with $\Phi$ as minimum differential polynomial over $K$. Since $s_\Phi \notin \mathfrak{p}$ we have

$$\mathfrak{p}_K(b) \;=\; \sqrt{[\Phi]} : s_\Phi \;\subseteq\; \mathfrak{p}.$$

For the reverse inclusion, let $G \in \mathfrak{p}$. By Theorem 4.18 we have $i_\Phi^p s_\Phi^q G \in [\Phi]$, with suitable $p, q \in \mathbb{N}$, hence $i_\Phi G \in \sqrt{[\Phi]} : s_\Phi = \mathfrak{p}_K(b)$, so $G \in \mathfrak{p}_K(b)$ in view of $i_\Phi(b) \neq 0$. Thus $\mathfrak{p} = \mathfrak{p}_K(b)$, as desired. □

By the basis theorem there must exist $F_1,\dots,F_m \in K[Y]_{\mathrm{d}}$ such that

$$\sqrt{[F]} : s_F \;=\; \sqrt{[F, F_1, \dots, F_m]},$$

but it seems that no effective construction of $F_1,\dots,F_m$ from $F$ is known. For example, do there exist $F_1,\dots,F_m$ as above where $m$ and the orders and total degrees of $F_1,\dots,F_m$ can be bounded in terms of the order and total degree of $F$?

Let $\mathfrak{p}$ be a nonzero differential prime ideal of $K[Y]_{\mathrm{d}}$, and put

$$\operatorname{ord}\mathfrak{p} := \min\{\operatorname{ord} F : 0 \neq F \in \mathfrak{p}\} \quad \text{(a natural number).}$$

An element $a$ in a differential field extension that is differentiallly algebraic over $K$ such that $\mathfrak{p} = \mathfrak{p}_K(a)$ is also said to be a *generic zero* of $\mathfrak{p}$ over $K$; note that for such $a$ we have $\operatorname{ord}\mathfrak{p} := \operatorname{trdeg}_K K(a)_{\mathrm{d}}$.

**Lemma 4.30.** *Let $\mathfrak{p}$ and $\mathfrak{q}$ be nonzero differential prime ideals of $K[Y]_{\mathrm{d}}$ such that $\mathfrak{p} \subset \mathfrak{q}$. Then* $\operatorname{ord}\mathfrak{p} > \operatorname{ord}\mathfrak{q}$.

*Proof.* Take generic zeros $a$ and $b$ of $\mathfrak{p}$ and $\mathfrak{q}$ over $K$, respectively, and let $F, G \in K[Y]_{\mathrm{d}}$ be minimimal differential polynomials of $a$ and $b$ over $K$, respectively. Then $F \in \mathfrak{p}$, so $F \in \mathfrak{q}$, and thus $\operatorname{ord}\mathfrak{p} = \operatorname{ord} F \geq \operatorname{ord} G = \operatorname{ord}\mathfrak{q}$. If $\operatorname{ord} F = \operatorname{ord} G = n$, then $F \in GK[Y, \dots, Y^{(n)}]$ by Lemmas 4.4 and 4.5 and their proof, but $F \in K[Y]_{\mathrm{d}}$ is irreducible, so $F = cG$ for some $c \in K^{\times}$, and thus $\mathfrak{p} = \mathfrak{q}$, contradicting $\mathfrak{p} \subset \mathfrak{q}$. $\square$

In the rest of this subsection $\mathbb{U}$ is a big differentially closed field, and the set $\mathbb{U}$ is given its $\partial$-topology. We apply the above with $K = \mathbb{U}$.

**Lemma 4.31.** *Let $X$ be an irreducible closed subset of $\mathbb{U}$ with $X \neq \mathbb{U}$, so $\mathfrak{p} := \mathrm{I}(X)$ is a nonzero differential prime ideal of $\mathbb{U}[Y]_{\mathrm{d}}$. Then*

$$\mathrm{MR}(X) \leq \dim(X) \leq \operatorname{ord}\mathfrak{p},$$

*where $\dim(X)$ is the Krull dimension of $X$ as a noetherian subspace of $\mathbb{U}$.*

*Proof.* Consider a chain

$$X_0 \subset X_1 \subset \cdots \subset X_n = X$$

of irreducible closed subsets of $\mathbb{U}$, and put $\mathfrak{p}_i := \mathrm{I}(X_i)$ for $i = 0, \dots, n$. This gives a chain

$$\mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_n = \mathfrak{p}$$

of nonzero differential prime ideals of $K[Y]_{\mathrm{d}}$, so by the previous lemma,

$$\operatorname{ord}\mathfrak{p}_0 < \cdots < \operatorname{ord}\mathfrak{p}_n = \operatorname{ord}\mathfrak{p},$$

so $\operatorname{ord}\mathfrak{p} \geq n$. It follows that $\operatorname{ord}\mathfrak{p} \geq \dim(X)$. The inequality $\mathrm{MR}(X) \leq \dim(X)$ follows from Corollary 3.17. $\square$

**Corollary 4.32.** $\mathrm{MR}(X) < \omega$ *for every proper closed subset $X$ of $\mathbb{U}$, and* $\mathrm{MR}(\mathbb{U}) = \omega$, $\mathrm{MD}(\mathbb{U}) = 1$.

*Proof.* The first assertion follows from the lemma above. By the remark following Corollary 4.14 we have $\mathrm{MR}(\mathbb{U}) \geq \omega$. Suppose towards a contradiction that either $\mathrm{MR}(\mathbb{U}) > \omega$, or $\mathrm{MR}(\mathbb{U}) = \omega$ and $\mathrm{MD}(\mathbb{U}) > 1$. Then we have disjoint constructible $X, Y \subseteq \mathbb{U}$ such that $\mathrm{MR}(X) \geq \omega$ and $\mathrm{MR}(Y) \geq \omega$. Then the first part of the corollary yields $\mathrm{cl}(X) = \mathbb{U}$ and $\mathrm{cl}(Y) = \mathbb{U}$. But $\mathbb{U}$ is irreducible, so $X$ and $Y$ both contain a nonempty open subset of $\mathbb{U}$, and thus $X \cap Y \neq \emptyset$, a contradiction. $\square$

**More on differentially closed fields.** We mention here some results that we shall not use but which it is good to be aware of. First, DCF being omega-stable, it follows that every $K$ has a so-called *differential closure* $K^{\mathrm{dc}}$, that is, $K \subseteq K^{\mathrm{dc}} \models \mathrm{DCF}$, and every embedding of $K$ into a differentially closed field $E$ extends to an embedding of $K^{\mathrm{dc}}$ into $E$. It can be shown that any two differential closures of $K$ are isomorphic over $K$, but in contrast to algebraic closures of fields, a differential closure of $K$ might have a strictly smaller differential subfield containing $K$ that is also a differential closure of $K$. One can also show that the constant field of a differential closure $K^{\mathrm{dc}}$ of $K$ is the algebraic closure of the constant field of $K$ inside $K^{\mathrm{dc}}$.

## 5. Algebraic Sets

Throughout this section we fix an algebraically closed field $\mathbf{k}$; we shall work in the concrete but rather narrow setting of algebraic subsets of cartesian spaces $\mathbf{k}^n$. The tools we develop here will enable us to introduce in the next section the more general and flexible notion of *algebraic variety.*

For each set $S$, let $\mathbf{k}^S$ be the ring of all functions $f : S \to \mathbf{k}$, with pointwise addition and multiplication of such functions. We consider $\mathbf{k}^S$ as a $\mathbf{k}$-algebra via the ring morphism $\mathbf{k} \to \mathbf{k}^S$ that sends each $c \in \mathbf{k}$ to the $\mathbf{k}$-valued function on $S$ (also indicated by $c$) taking the constant value $c$. Given any non-trivial $\mathbf{k}$-algebra $A$ we identify $\mathbf{k}$ with its image in $A$ via $c \mapsto c \cdot 1 : \mathbf{k} \to A$. By "algebra" we mean "$\mathbf{k}$-algebra" in this section, in particular, an "algebra morphism" is a morphism of $\mathbf{k}$-algebras.

Throughout this section we also fix an algebraic set $X \subseteq \mathbf{k}^m$ with its Zariski topology, induced by the Zariski topology of $\mathbf{k}^m$. This topology is good enough to define some invariants of $X$ like its (Krull) dimension but is too weak for most purposes. To get a better view of $X$ we shall introduce its coordinate ring $\mathbf{k}[X]$, in terms of which we can define its tangent bundle $\mathrm{T}\,X \subseteq \mathbf{k}^{2m}$ and other geometric objects associated to $X$.

First, to each polynomial $f \in \mathbf{k}[T_1, \dots, T_m]$ we associate the polynomial function $f|X : X \to \mathbf{k}$ on $X$ given by $x \mapsto f(x)$. These polynomial functions on $X$ form a subalgebra $\mathbf{k}[X]$ of the algebra $\mathbf{k}^X$; we call $\mathbf{k}[X]$ the *coordinate ring of* $X$. The map

$$f \mapsto f|X \ : \ \mathbf{k}[T_1, \dots, T_m] \to \mathbf{k}[X]$$

is a surjective algebra morphism with kernel $\mathrm{I}(X)$, so induces an algebra isomorphism $\mathbf{k}[T_1, \dots, T_m]/\,\mathrm{I}(X) \ \cong \ \mathbf{k}[X]$. Let $t_i := T_i|X$ for $i = 1, \dots, m$, so $\mathbf{k}[X] = \mathbf{k}[t_1, \dots, t_m]$ as rings if $X \neq \emptyset$.

We often identify a polynomial $f \in \mathbf{k}[T_1, \dots, T_m]$ with the polynomial function $x \mapsto f(x) : \ \mathbf{k}^m \to \mathbf{k}$ on $\mathbf{k}^m$; this is harmless, since $\mathrm{I}(\mathbf{k}^m) = \{0\}$. This identification makes $\mathbf{k}[T_1, \dots, T_m]$ the coordinate ring of the algebraic set $\mathbf{k}^m$ and explains the notation $f|X$ used in defining polynomial functions on $X$. For $a = (a_1, \dots, a_m) \in \mathbf{k}^m$, let

$$\mathfrak{m}_a := \{f \in \mathbf{k}[T_1, \dots, T_m] : \ f(a) = 0\} = (T_1 - a_1, \dots, T_m - a_m)$$

be the corresponding maximal ideal of $\mathbf{k}[T_1, \dots, T_m]$, and note that

$$\mathfrak{m}_a \supseteq \mathrm{I}(X) \iff a \in X.$$

It follows that a point $a = (a_1, \dots, a_m) \in X$ yields the maximal ideal

$$\mathfrak{m}_{X,a} := \{f \in \mathbf{k}[X] : f(a) = 0\} = (t_1 - a_1, \dots, t_m - a_m)\mathbf{k}[X]$$

of $\mathbf{k}[X]$. Also, by part (4) of Corollary 2.3, the above isomorphism

$$\mathbf{k}[T_1, \dots, T_m]/\,\mathrm{I}(X) \;\cong\; \mathbf{k}[X]$$

yields a bijective correspondence

$$a \mapsto \mathfrak{m}_{X,a} \;:\; X \to \{\text{maximal ideals of } \mathbf{k}[X]\}$$

between the points of $X$ and the maximal ideals of its coordinate ring. In particular, if $g_1, \dots, g_n \in \mathbf{k}[X]$ have no common zero in $X$, then there are $f_1, \dots, f_n \in \mathbf{k}[X]$ such that $f_1 g_1 + \dots + f_n g_n = 1$. For $n = 1$ this means that if $g \in \mathbf{k}[X]$ has no zero in $X$, then $1/g \in \mathbf{k}[X]$.

**Regular functions on open sets, and regular maps.** In the next section we define algebraic varieties essentially by glueing algebraic sets along open subsets, with *regular* transition maps as glue. This is one reason to pay attention to open sets and regular maps.

A function $f \in \mathbf{k}[X]$ yields the open subset $X_f := \{x \in X : \ f(x) \neq 0\}$ of $X$, and sets of this form are called *basic open sets in* $X$. Open subsets of $X$ are finite unions of basic open sets in $X$: Let $U \subseteq X$ be open; then

$$X \setminus U = \{x \in X : f_1(x) = \dots = f_n(x)\}, \text{ where } f_1, \dots, f_n \in \mathbf{k}[X],$$

so $U = X_{f_1} \cup \dots \cup X_{f_n}$.

Let $U \subseteq X$ be open. A *regular function* on $U$ is a function $f : U \to \mathbf{k}$ such that each $x \in U$ has an open neighborhood $U_x \subseteq U$ on which $f$ is a rational function: there are $p, q \in \mathbf{k}[X]$ such that $q$ has no zero on $U_x$ and $f(y) = p(y)/q(y)$ for all $y \in U_x$. Regular functions on $U$ are definable in the field $\mathbf{k}$. This is because $U$ is a noetherian space, hence $U$ is compact, so finitely many of the $U_x$ in the definition above will already cover $U$. The regular functions on $U$ are continuous with respect to the Zariski topology on domain and codomain, and are the elements of a subalgebra $\mathcal{O}_X(U)$ of $\mathbf{k}^U$. Note that if $f : U \to \mathbf{k}$ is regular and $f(x) \neq 0$ for all $x \in U$, then $1/f : U \to \mathbf{k}$ is regular. The assignment

$$U \mapsto \mathcal{O}_X(U), \qquad (U \text{ an open set in } X)$$

is the so-called *structure sheaf* $\mathcal{O}_X$ on $X$, but the role of sheafs will become clear only in the more general setting of algebraic varieties. It turns out that the regular functions on $X$ are exactly the polynomial functions on $X$:

**Lemma 5.1.** $\mathcal{O}_X(X) = \mathbf{k}[X]$.

*Proof.* It is obvious that $\mathbf{k}[X] \subseteq \mathcal{O}_X(X)$. For the reverse inclusion, let $f \in \mathcal{O}_X(X)$. By compactness of $X$ we have a covering of $X$ by basic open sets $U_1, \dots, U_n$ in $X$ and for $i = 1, \dots, n$ we have $p_i, q_i \in \mathbf{k}[X]$ such that $q_i$ has no zero in $U_i$ and $f(y) = p_i(y)/q_i(y)$ on $U_i$. Now $U_i = X_{f_i}$ with $f_i \in \mathbf{k}[X]$, so $f_i q_i f = f_i p_i$, not only on $U_i$ but on all of $X$. The functions $f_1 q_1, \dots, f_n q_n$ have no common zero in $X$, so there are $g_1, \dots, g_n \in \mathbf{k}[X]$ such that $g_1 f_1 q_1 + \cdots + g_n q_n f_n = 1$, and then

$$f = (g_1 f_1 q_1 + \cdots + g_n q_n f_n) f = g_1 f_1 p_1 + \cdots + g_n f_n p_n \in \mathbf{k}[X],$$

as claimed. $\square$

For the rest of this section we also fix an algebraic set $Y \subseteq \mathbf{k}^n$. A map

$$\phi = (\phi_1, \dots, \phi_n) : X \to Y, \qquad (\phi_i : X \to \mathbf{k} \text{ for } i = 1, \dots, n)$$

is said to be *regular* if all $\phi_i \in \mathbf{k}[X]$. For example, the identity map $X \to X$ is regular, the inclusion map $(t_1, \dots, t_m) : X \hookrightarrow \mathbf{k}^m$ is regular, and each constant map $X \to Y$ is regular. A regular map $X \to Y$ is continuous. If $Z \subseteq \mathbf{k}^p$ is an algebraic set and $\phi : X \to Y$ and $\psi : Y \to Z$ are regular, then $\psi \circ \phi : X \to Z$ is regular. Thus we have the *category* of algebraic sets and regular maps; an isomorphism between $X$ and $Y$ in this category is a *biregular* map $X \to Y$, that is, a bijective regular map $X \to Y$ whose inverse is a regular map $Y \to X$.

Let $\phi : X \to Y$ be regular. Then it transforms regular functions on $Y$ into regular functions on $X$ by composition with $\phi$. More precisely, let $V \subseteq Y$ be open, and put $U := \phi^{-1}(V)$. Then $\phi$ induces an algebra morphism

$$\phi_V^* : \mathcal{O}_Y(V) \to \mathcal{O}_X(U), \quad \phi_V^*(f) := f \circ (\phi|U).$$

In particular, $\phi^* := \phi_Y^* : \mathbf{k}[Y] \to \mathbf{k}[X]$. If $Z \subseteq \mathbf{k}^p$ is an algebraic set and $\psi : Y \to Z$ are regular, then

$$(\psi \circ \phi)^* = \phi^* \circ \psi^* : \mathbf{k}[Z] \to \mathbf{k}[X].$$

When $X = Y$ and $\phi = \mathrm{id}_X$, then $\phi^*$ is the identity map on $\mathbf{k}[X]$.

**Exercise.** For any algebra morphism $\alpha : \mathbf{k}[Y] \to \mathbf{k}[X]$ there is a unique regular map $\phi : X \to Y$ such that $\phi^* = \alpha$.

**Algebraic sets as intrinsic objects.** We defined algebraic sets as subsets of coordinate spaces $\mathbf{k}^0, \mathbf{k}^1, \mathbf{k}^2, \dots$, but the key features of an algebraic set are those that are invariant under biregular maps: our focus is on properties of the algebraic set $X$ that are independent of its inclusion in the ambient space $\mathbf{k}^m$. These features are encoded in $\mathbf{k}[X]$. Indeed, a biregular map $\phi : X \to Y$ induces an algebra isomorphism $\phi^* : \mathbf{k}[Y] \to \mathbf{k}[X]$, and any algebra isomorphism $\mathbf{k}[Y] \to \mathbf{k}[X]$ has the form $\phi^*$ for a unique biregular $\phi : X \to Y$. As an example of this general philosophy, note that the points of $X$ correspond to the maximal ideals of $\mathbf{k}[X]$; likewise, the closed subsets of $X$ are in bijective correspondence with the radical ideals of $\mathbf{k}[X]$.

The inclusion $X \hookrightarrow \mathbf{k}^m$ is of course a geometric object associated to $X$. What is it in terms of $\mathbf{k}[X]$? This inclusion is the regular map $(t_1, \dots, t_m)$, and specifying this inclusion amounts therefore to specifying the generating system $t_1, \dots, t_m$ of the algebra $\mathbf{k}[X]$. But any other generating system $u_1, \dots, u_n$ of the algebra $\mathbf{k}[X]$ yields also an embedding

$$u = (u_1, \dots, u_n) : \ X \to \mathbf{k}^n,$$

that is, $u(X)$ is closed in $\mathbf{k}^n$ and $u : X \to u(X)$ is biregular. (We leave it to the reader to verify this fact, which is not used later on.)

**Application of Krull's Intersection Theorem.** First a bit of notation. Let $R$ be a ring and let $I_1, \dots, I_e$ be ideals of $R$. Then $I_1 \cdots I_e$ denotes the ideal of $R$ generated by the products $a_1 \cdots a_e$ with $a_1 \in I_1, \dots, a_e \in I_e$, so the elements of $I_1 \cdots I_e$ are the (finite) sums of such products. Note that $I_1 \cdots I_e \subseteq I_1 \cap \cdots \cap I_e$. When $I_1 = \cdots = I_e = I$ we set $I^e := I_1 \cdots I_e$. In particular, $I^0 = R$, $I^1 = I$, and $I^e \supseteq I^{e+1}$, for any ideal $I$ of $R$.

Let $a \in X$, so $\mathfrak{m}_{X,a} = \{f \in \mathbf{k}[X] : \ f(a) = 0\}$; think of the elements of $\mathfrak{m}_{X,a}^e$ as the regular functions on $X$ that *vanish at $a$ with order $\geq e$*. Let $\phi : X \to Y$ be a regular map and let $\phi(a) = b \in Y$. Then $\phi^*(f)(a) = f(b)$ for $f \in \mathbf{k}[Y]$, so $\phi^*(\mathfrak{m}_{Y,b}) \subseteq \mathfrak{m}_{X,a}$, with equality if $\phi^*$ is surjective. Take for example the (regular) inclusion map $\iota : X \hookrightarrow \mathbf{k}^m$. Then $\iota^* : \mathbf{k}[T_1, \dots, T_m] \to \mathbf{k}[X]$ is the restriction map $f \mapsto f|X$, and is surjective by the definition of $\mathbf{k}[X]$. With

$$\mathfrak{m}_a = (T_1 - a_1, \dots, T_m - a_m)\mathbf{k}[T_1, \dots, T_m]$$

this gives $\iota^*(\mathfrak{m}_a) = \mathfrak{m}_{X,a}$, and thus $\iota^*(\mathfrak{m}_a^e) = \mathfrak{m}_{X,a}^e$ for all $e$.

Now, $\mathbf{k}[X]$ and its ideal $\mathfrak{m}_{X,a}$ are $\mathbf{k}$-vector spaces, in general of infinite dimension, but:

**Lemma 5.2.** *$\mathbf{k}[X]/\mathfrak{m}_{X,a}^e$ has finite dimension as a $\mathbf{k}$-vector space.*

*Proof.* The above $\iota^*$ induces a surjective $\mathbf{k}$-algebra morphism

$$\mathbf{k}[T_1, \dots, T_m]/\mathfrak{m}_a^e \to \mathbf{k}[X]/\mathfrak{m}_{X,a}^e,$$

so it is enough to show that $\mathbf{k}[T_1, \dots, T_m]/\mathfrak{m}_a^e$ has finite dimension as a vector space over $\mathbf{k}$. To keep notations simple we just do the case $a = (0, \dots, 0)$. Then $\mathfrak{m}_a = (T_1, \dots, T_m)$ and the elements of $(T_1, \dots, T_m)^e$ are those

$$f = \sum_{\boldsymbol{i}} a_{\boldsymbol{i}} T^{\boldsymbol{i}} \in \mathbf{k}[T_1, \dots, T_m], \quad (\boldsymbol{i} = (i_1, \dots, i_m) \in \mathbb{N}^m)$$

such that $a_{\boldsymbol{i}} = 0$ for all $\boldsymbol{i}$ with $i_1 + \cdots + i_m < e$. . So a basis of the $\mathbf{k}$-linear space $\mathbf{k}[T_1, \dots, T_m]/(T_1, \dots, T_m)^e$ is given by the residue classes

$$T_1^{i_1} \cdots T_m^{i_m} + (T_1, \dots, T_m)^e, \qquad \big((i_1, \dots, i_m) \in \mathbb{N}^m, \ i_1 + \cdots + i_m < e\big).$$

In particular, this vector space has finite dimension. $\square$

In particular, the $\mathbf{k}$-linear subspace $\mathfrak{m}_{X,a}/\mathfrak{m}_{X,a}^2$ of $\mathbf{k}[X]/\mathfrak{m}_{X,a}^2$ has finite dimension. This vector space will later be interpreted as the *cotangent space of $X$ at $a$*.

A key result from Commutative Algebra is the Krull Intersection Theorem, which in one of its forms says: *if $R$ is a noetherian domain and $\mathfrak{m}$ is a maximal ideal of $R$, then $\bigcap_e \mathfrak{m}^e = \{0\}$.*

This has a consequence that we shall use later:

**Lemma 5.3.** *Suppose $Y \subseteq \mathbf{k}^m$ is an irreducible algebraic set, and $a \in X \cap Y$. Then $X \supseteq Y$ if and only if for all $f \in \mathbf{k}[T_1, \dots, T_m]$ and $e$ with $f|X \in \mathfrak{m}^e_{X,a}$ we have $f|Y \in \mathfrak{m}^e_{Y,a}$.*

*Proof.* If $X \supseteq Y$, then the inclusion map $Y \to X$ induces the surjective ring morphism

$$f|X \to f|Y : \mathbf{k}[X] \to \mathbf{k}[Y], \quad (f \in \mathbf{k}[T_1, \dots, T_m]),$$

which maps $\mathfrak{m}_{X,a}$ onto $\mathfrak{m}_{Y,a}$, and thus $\mathfrak{m}^e_{X,a}$ onto $\mathfrak{m}^e_{Y,a}$ for each $e$.

For the converse, assume that for all $f \in \mathbf{k}[T_1, \dots, T_m]$ and $e$ with $f|X \in \mathfrak{m}^e_{X,a}$ we have $f|Y \in \mathfrak{m}^e_{Y,a}$. To obtain $X \supseteq Y$ it suffices to show that $\mathrm{I}(X) \subseteq \mathrm{I}(Y)$. If $f \in \mathrm{I}(X)$, then $f|X = 0$, so $f|X \in \mathfrak{m}^e_{X,a}$ for all $e$, hence $f|Y \in \mathfrak{m}^e_{Y,a}$ for all $e$, and thus $f|Y = 0$ (since $\mathbf{k}[Y]$ is a noetherian domain), that is, $f \in \mathrm{I}(Y)$. $\square$

**Products.** The product $X \times Y \subseteq \mathbf{k}^{m+n}$ is an algebraic set, and it has the following key property: the projection maps $X \times Y \to X$ and $X \times Y \to Y$ are regular, and if $Z \subseteq \mathbf{k}^p$ is an algebraic set and $f : Z \to X$ and $g : Z \to Y$ are regular, so is $(f, g) : Z \to X \times Y$. Also, for $a \in X$ the map

$$y \mapsto (a, y) : Y \to X \times Y$$

is regular, and for $b \in Y$ the map

$$x \mapsto (x, b) : X \to X \times Y$$

is regular. Thus by Lemma 3.2, if $X, Y$ are irreducible, so is $X \times Y$.

Let $T_1, \dots, T_m, U_1, \dots, U_n$ be distinct indeterminates and consider the ideals $\mathrm{I}(X) \subseteq \mathbf{k}[T_1, \dots, T_m]$ and $\mathrm{I}(Y) \subseteq \mathbf{k}[U_1, \dots, U_n]$. For $f \in \mathbf{k}[X]$ and $g \in \mathbf{k}[Y]$ we have the regular function $(x, y) \mapsto f(x)g(y) : X \times Y \to \mathbf{k}$, which for simplicity we denote by $fg$. It is clear that $\mathbf{k}[X \times Y]$ consists of the finite sums of such products $fg$.

**Lemma 5.4.** *Let $(f_i)_{i \in I}$ be a basis of the $\mathbf{k}$-linear space $\mathbf{k}[X]$ and $(g_j)_{j \in J}$ a basis of the $\mathbf{k}$-linear space $\mathbf{k}[Y]$. Then $(f_i g_j)_{i \in I, j \in J}$ is a basis of the $\mathbf{k}$-linear space $\mathbf{k}[X \times Y]$.*

*Proof.* Let $i$ range over $I$ and $j$ over $J$ in what follows. Let $(c_{ij})$ be a family of elements of $\mathbf{k}$ with $c_{ij} = 0$ for all but finitely many $(i, j)$, such that $\sum_{i,j} c_{ij} f_i g_j = 0$. Then we have for all $a \in X$,

$$0 = \sum_{ij} c_{ij} f_i(a) g_j = \sum_j \big(\sum_i c_{ij} f_i(a)\big) g_j,$$

in $\mathbf{k}[Y]$, so $\sum_i c_{ij} f_i(a) = 0$ for all $a \in X$ and all $j$. Thus $\sum_i c_{ij} f_i = 0$ for all $j$, so $c_{ij} = 0$ for all $i, j$. $\square$

**Corollary 5.5.** *$\mathrm{I}(X \times Y) \subseteq \mathbf{k}[T_1, \ldots, T_m, U_1, \ldots, U_n]$ is generated by the $F(T) \in \mathrm{I}(X)$ and the $G(U) \in \mathrm{I}(Y)$.*

*Proof.* Let $f \in \mathrm{I}(X \times Y)$. With $\alpha$ and $\beta$ ranging over $\mathbb{N}^m$ and $\mathbb{N}^n$ we have

$$f = \sum_{\alpha,\beta} c_{\alpha\beta} T^\alpha U^\beta$$

with all $c_{\alpha\beta} \in \mathbf{k}$ and $c_{\alpha\beta} \neq 0$ for only finitely many $\alpha, \beta$. Take $F_i \in \mathbf{k}[T_1, \ldots, T_m]$ for $i \in I$ and take $G_j \in \mathbf{k}[U_1, \ldots, U_n]$ for $j \in J$ such that $(F_i|X)$ is a basis of the $\mathbf{k}$-linear space $\mathbf{k}[X]$ and $(G_j|Y)$ is a basis of the $\mathbf{k}$-linear space $\mathbf{k}[Y]$. For all $\alpha, \beta$ we have

$$T^\alpha = f_\alpha + \sum_i a_{i\alpha} F_i, \quad f_\alpha \in \mathrm{I}(X),$$

$$U^\beta = g_\beta + \sum_j b_{j\beta} G_j, \quad g_\beta \in \mathrm{I}(Y).$$

where all $a_{i\alpha}, b_{j\beta} \in \mathbf{k}$ with $a_{i\alpha} \neq 0$ for only finitely many $i$ and $b_{j\alpha} \neq 0$ for only finitely many $j$. The desired result then follows by substitution in the expression for $f$, using also Lemma 5.4. $\square$

**Germs and local rings.** Let $a \in X$ and let $U, V, W$ range over open neighborhoods of $a$ in $X$. The intrinsic features of $X$ near $a$ are encoded in the local ring $\mathcal{O}_{X,a}$ whose elements are the germs of regular functions on open neighborhoods of $a$ in $X$. The precise definition of $\mathcal{O}_{X,a}$ is as follows. We introduce an equivalence relation $\sim_a$ on the disjoint union of the rings $\mathcal{O}_X(U)$: for $f \in \mathcal{O}_X(U)$, $g \in \mathcal{O}_X(V)$,

$$f \sim_a g \ :\Longleftrightarrow\ f|W = g|W \text{ for some } W \subseteq U \cap V.$$

The equivalence class $\gamma_a f$ of $f \in \mathcal{O}_X(U)$ with respect to $\sim_a$ is called the *germ of $f$ at $a$*; for such a germ $\gamma = \gamma_a f$ we set $\gamma(a) := f(a)$. The set of germs of functions in $\bigcup_U \mathcal{O}_X(U)$ is denoted by $\mathcal{O}_{X,a}$, and is made into an algebra in the obvious way, by requiring that for each $U$ the map

$$f \mapsto \gamma_a f : \ \mathcal{O}_X(U) \to \mathcal{O}_{X,a}$$

is an algebra morphism.

Note that $\gamma \mapsto \gamma(a) : \mathcal{O}_{X,a} \to \mathbf{k}$ is a surjective algebra morphism and that if $\gamma \in \mathcal{O}_{X,a}$ and $\gamma(a) \neq 0$, then $\gamma$ is a unit of $\mathcal{O}_{X,a}$. Thus $\mathcal{O}_{X,a}$ is a local ring with maximal ideal $\mathfrak{m}(\mathcal{O}_{X,a}) = \{\gamma \in \mathcal{O}_{X,a} : \ \gamma(a) = 0\}$, and

$$\mathcal{O}_{X,a} = \mathbf{k} \oplus \mathfrak{m}(\mathcal{O}_{X,a}) \qquad \text{(internal direct sum of } \mathbf{k}\text{-linear subspaces).}$$

If $f, g \in \mathbf{k}[X]$ and $g(a) \neq 0$, then $\gamma_a g$ is a unit of $\mathcal{O}_{X,a}$, so $\gamma_a f/\gamma_a g$ denotes an element of $\mathcal{O}_{X,a}$. All elements of $\mathcal{O}_{X,a}$ are of this form, and are thus in some sense quotients of regular functions on $X$.

**Exercise.** The algebra morphism $f \mapsto \gamma_a f : \ \mathbf{k}[X] \to \mathcal{O}_{X,a}$ maps $\mathfrak{m}_{X,a}$ onto $\mathfrak{m}(\mathcal{O}_{X,a})$. If $X$ is irreducible, then $\mathcal{O}_{X,a}$ is a domain, and the algebra morphism $f \mapsto \gamma_a f : \mathbf{k}[X] \to \mathcal{O}_{X,a}$ is injective.

Let $\phi : X \to Y$ be a regular map and put $b = \phi(a)$. Then we have the algebra morphism $\phi_a^* : \mathcal{O}_{Y,b} \to \mathcal{O}_{X,a}$ given by

$$\phi_a^*(\gamma_b g) := \gamma_a\big(\phi_O^*(g)\big) \qquad (g \in \mathcal{O}_Y(O),\ O \text{ open in } Y,\ b \in O),$$

with $\phi_a^*\big(\mathfrak{m}(\mathcal{O}_{Y,b})\big) \subseteq \mathfrak{m}(\mathcal{O}_{X,a})$. When in addition $\psi : Y \to Z$ is regular and $c = \psi(b)$, then

$$(\psi \circ \phi)_a^* = \phi_a^* \circ \psi_b^*.$$

**Tangent spaces.** Fix a point $a = (a_1, \dots, a_m) \in \mathbf{k}^m$. Given a polynomial $F \in \mathbf{k}[T_1, \dots, T_m]$ of degree $\le d$ we expand $F$ around $a$:

$$F(a+v) = F(a) + F_1(v) + F_2(v) + \cdots + F_d(v) \qquad (v \in \mathbf{k}^m),$$

where $F_i(V_1, \dots, V_m) \in \mathbf{k}[V_1, \dots, V_m]$ is homogeneous of degree $i$ and depends on $a$ but not on $v$, for $i = 1, \dots, d$. Here $V_1, \dots, V_m$ are distinct new variables, "new" in the sense of not belonging to $\{T_1, \dots, T_m\}$. In particular,

$$F_1 \;=\; \frac{\partial F}{\partial T_1}(a) \cdot V_1 + \cdots + \frac{\partial F}{\partial T_m}(a) \cdot V_m \in \mathbf{k}V_1 + \cdots + \mathbf{k}V_m$$

is a linear polynomial, also called the *differential of $F$ at $a$* and denoted by $d_aF$. (Think of it as the linear function that best approximates $F - F(a)$ at $a$.) It is easy to check that the map

$$F \mapsto d_aF :\ \mathbf{k}[T_1, \dots, T_m] \to \mathbf{k}V_1 + \cdots + \mathbf{k}V_m$$

is $\mathbf{k}$-linear, with $d_a c = 0$ for $c \in \mathbf{k}$, and satisfies the derivation-like rule

$$d_a(FG) = F(a) \cdot d_aG + G(a) \cdot d_aF, \qquad (F, G \in \mathbf{k}[T_1, \dots, T_m]).$$

We also have the following chain rule.

**Lemma 5.6.** *Let $F_1, \dots, F_n \in \mathbf{k}[T_1, \dots, T_m]$ and $G \in \mathbf{k}[U_1, \dots, U_n]$, and set $H := G(F_1, \dots, F_n) \in \mathbf{k}[T_1, \dots, T_m]$. Then we have for $a \in \mathbf{k}^m$ and $b := (F_1(a), \dots, F_n(a)) \in \mathbf{k}^n$,*

$$d_aH = d_bG(d_aF_1, \dots, d_aF_n) \in \mathbf{k}V_1 + \cdots + \mathbf{k}V_m.$$

One can verify this by checking the identity for $G \in \mathbf{k}$ and for $G = U_j$, $j = 1, \dots, n$, and by showing that the identity is preserved by sums and products of polynomials $G$ for which it holds.

**Exercise.** Let $F \in \mathbf{k}[T_1, \dots, T_m]$ and $a \in \mathbf{k}^m$. Then

$$d_aF = 0 \iff F - F(a) \in \mathfrak{m}_a^2.$$

To express the dependence of $d_aF$ on $a$ we define, for $F \in \mathbf{k}[T_1, \dots, T_m]$,

$$dF := \frac{\partial F}{\partial T_1} \cdot V_1 + \cdots + \frac{\partial F}{\partial T_m} \cdot V_m \in \mathbf{k}[T_1, \dots, T_m]V_1 + \cdots + \mathbf{k}[T_1, \dots, T_m]V_m,$$

the *differential of $F$*, a polynomial in the variables $T_1, \dots, T_m, V_1, \dots, V_m$ which is linear in $V_1, \dots, V_m$. Thus

$$d_aF = dF(a, V_1, \dots, V_m), \qquad V_i = dT_i = d_aT_i, \quad (i = 1, \dots, m).$$

It is in fact traditional to write the new variables $V_1, \dots, V_m$ as $dT_1, \dots, dT_m$.

We now return to our algebraic set $X \subseteq \mathbf{k}^m$, and put $I := \mathrm{I}(X)$. Let $a \in X$. Then we define the *tangent space of $X$ at $a$* by

$$\mathrm{T}_a X := \{v \in \mathbf{k}^m : \ d_a F(v) = 0 \text{ for all } F \in I\},$$

a linear subspace of the vector space $\mathbf{k}^m$ over $\mathbf{k}$. It follows easily from the computation rules for differentials that if $I = (F_1, \dots, F_n)$, then

$$\mathrm{T}_a X = \{v \in \mathbf{k}^m : \ d_a F_1(v) = \cdots = d_a F_n(v) = 0\}.$$

(Think of $a + \mathrm{T}_a X$ as the best linear approximation to $X$ at $a$.) We bundle the tangent spaces of $X$ at its various points into a single object, the *tangent bundle* $\mathrm{T}\, X$ *of* $X$:

$$\mathrm{T}\, X := \{(x, v) \in \mathbf{k}^m \times \mathbf{k}^m : \ x \in X, \ dF(x, v) = 0 \text{ for all } F \in I\},$$

Note that $\mathrm{T}\, X(a) = \mathrm{T}_a X$ for $a \in X$, and that if $I = (F_1, \dots, F_n)$, then $\mathrm{T}\, X$ consists of the points $(x, v) \in \mathbf{k}^m \times \mathbf{k}^m$ such that

$$F_1(x) = \cdots = F_n(x) = 0, \ dF_1(x, v) = \cdots = dF_n(x, v) = 0.$$

In particular, $\mathrm{T}\, X$ is an algebraic set in $\mathbf{k}^m \times \mathbf{k}^m = \mathbf{k}^{2m}$.

**The case of a hypersurface.** A *hypersurface $H$ in* $\mathbf{k}^m$ is the zero set

$$H = \mathrm{Z}(F) \subseteq \mathbf{k}^m$$

of a single polynomial $F \in \mathbf{k}[T_1, \dots, T_m]$, $F \notin \mathbf{k}$. Let $H$ be an *irreducible* hypersurface in $\mathbf{k}^m$, so $H = \mathrm{Z}(F)$ where $F \in \mathbf{k}[T_1, \dots, T_m]$ is irreducible. Then $\mathrm{I}(H) = (F)$, so for $a \in H$,

$$\mathrm{T}_a H = \{v \in \mathbf{k}^m : \ \frac{\partial F}{\partial T_1}(a) v_1 + \cdots + \frac{\partial F}{\partial T_m}(a) v_m \ = \ 0\},$$

so $\mathrm{T}_a H$ has dimension $m - 1$ iff $\frac{\partial F}{\partial T_i}(a) \neq 0$ for some $i$, and $\mathrm{T}_a H = \mathbf{k}^m$ otherwise. We claim that the closed subset

$$\{a \in H : \ \mathrm{T}_a H = \mathbf{k}^m\} = \{a \in H : \ \frac{\partial F}{\partial T_1}(a) = \cdots = \frac{\partial F}{\partial T_m}(a) = 0\}$$

of $H$ is a proper subset of $H$. To see why this is so, assume first that $\mathbf{k}$ has characteristic 0. Since $F \notin \mathbf{k}$ we can take $i \in \{1, \dots, m\}$ such that $T_i$ occurs in $F$; viewing $F$ as a polynomial in $T_i$ with coefficients in $\mathbf{k}[T_1, \dots, T_{i-1}, T_{i+1}, \dots, T_m]$ we get that $\frac{\partial F}{\partial T_i} \neq 0$ (using the characteristic 0 assumption) and $\frac{\partial F}{\partial T_i}$ has lower degree in $T_i$ than $F$. Since $F$ is irreducible, it follows that $\frac{\partial F}{\partial T_i} \notin (F) = \mathrm{I}(H)$, so there is $a \in H$ such that $\frac{\partial F}{\partial T_i}(a) \neq 0$. When $\mathbf{k}$ has positive characteristic one needs to choose $i$ with a little more care, and this case is left as an exercise.

**The dimension of a tangent space.** Suppose that $\mathrm{I}(X) = (F_1, \ldots, F_n)$. Then $\mathrm{T}_a X$ consists of all $v = (v_1, \ldots, v_m) \in \mathbf{k}^m$ such that

$$\begin{aligned} \frac{\partial F_1}{\partial T_1}(a)v_1 + \cdots + \frac{\partial F_1}{\partial T_m}(a)v_m &= 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \frac{\partial F_n}{\partial T_1}(a)v_1 + \cdots + \frac{\partial F_n}{\partial T_m}(a)v_m &= 0. \end{aligned}$$

The matrix of this system of linear equations is the so-called *jacobian matrix*

$$\mathrm{J}(F_1, \ldots, F_n)(a) := \big(\frac{\partial F_i}{\partial T_j}(a)\big),$$

an $n \times m$-matrix with entries in $\mathbf{k}$, so

$$\dim \mathrm{T}_a(X) + \operatorname{rank}\big(\mathrm{J}(F_1, \ldots, F_n)(a)\big) = m.$$

Consider any $n \times m$-matrix

$$A = (a_{ij}) \qquad (1 \le i \le n,\ 1 \le j \le m)$$

with entries in a field. A *minor of $A$* is a square submatrix

$$(a_{ij})_{i \in I, j \in J} \qquad I \subseteq \{1, \ldots, n\},\ J \subseteq \{1, \ldots, m\},\ |I| = |J|,$$

and the *size* of this minor is the number $|I| = |J| \le \min(m, n)$. Recall that the rank of $A$ equals the largest $r \in \mathbb{N}$ such that $A$ has a minor of size $r$ with nonzero determinant.

**Lemma 5.7.** *Suppose $X$ is irreducible. Then there is $d \in \{0, \ldots, m\}$ and a proper closed subset* $\mathrm{Sing}(X)$ *of $X$ such that*

(1) $\dim \mathrm{T}_a X > d$ *for all* $a \in \mathrm{Sing}(X)$*;*
(2) $\dim \mathrm{T}_a X = d$ *for all* $a \in X \setminus \mathrm{Sing}(X)$.

*Proof.* Take $r \in \mathbb{N}$ to be the maximum value of $\operatorname{rank}\big(\mathrm{J}(F_1, \ldots, F_n)(a)\big)$ as $a$ ranges over $X$, and take $d \in \mathbb{N}$ such that $d + r = m$. It follows from the considerations above that for all $a \in X$ we have $\dim \mathrm{T}_a X \ge d$ and that $\dim \mathrm{T}_a X > d$ iff all minors of size $r$ of $\mathrm{J}(F_1, \ldots, F_n)(a)$ have vanishing determinant. $\square$

The set $\mathrm{Sing}(X)$ defined in this lemma is called the *singular locus of $X$*, and its points are called *singular points of $X$*; the nonsingular points of $X$ are also called *simple points of $X$*, and if $a$ is a simple point of $X$, we also say that $X$ is *smooth at $a$*. It is an important fact that the number $d$ defined by this lemma equals $\dim X$: this is clear when $X$ is an irreducible hypersurface in $\mathbf{k}^m$, and will be proved later by reduction to this case.

**Functoriality of the tangent space construction.** A reminder about terminology: Let $K$ be a field and $V$ a finite-dimensional $K$-vector space. Then $V^*$ denotes the dual vector space of $K$-linear functions $V \to K$. Recall that $V^*$ has the same $K$-vector space dimension as $V$. For $\mathbf{k} = K$ and $a \in X$, the dual $(\mathrm{T}_a X)^*$ of the tangent space $\mathrm{T}_a X$ of $X$ at $a$ is also denoted by $\mathrm{T}_a^* X$ and called the *cotangent space of $X$ at $a$*.

Returning to algebraic sets, let $a \in X$ and define for $f \in \mathbf{k}[X]$ the $\mathbf{k}$-linear function $d_a f : \mathrm{T}_a X \to \mathbf{k}$ to be $d_a F|\,\mathrm{T}_a X$ with $F \in \mathbf{k}[T_1, \dots, T_m]$ such that $F|X = f$. (This makes sense, since if $F, G \in \mathbf{k}[T_1, \dots, T_m]$ and $F|X = G|X$, then $F - G \in \mathrm{I}(X)$, so $d_a F|\,\mathrm{T}_a X \ = \ d_a G|\,\mathrm{T}_a X$.) Thus $d_a f \in \mathrm{T}_a^* X$ for $f \in \mathbf{k}[X]$ and the map $f \mapsto d_a f : \mathbf{k}[X] \to \mathrm{T}_a^* X$ is $\mathbf{k}$-linear and satisfies

$$d_a(fg) = f(a) d_a g + g(a) d_a f \qquad (f, g \in \mathbf{k}[X].$$

Let $Y \subseteq \mathbf{k}^n$ be a second algebraic set, let $f = (f_1, \dots, f_n) : X \to Y$ be a regular map, and let $b = f(a)$.

**Lemma 5.8.** *If $v \in \mathrm{T}_a X$, then $(d_a f_1(v), \dots, d_a f_n(v)) \in \mathrm{T}_b Y$.*

*Proof.* Take $F_1, \dots, F_n \in \mathbf{k}[T_1, \dots, T_m]$ with $F_i|X = f_i$ for $i = 1, \dots, m$, and let $G \in \mathrm{I}(Y)$. Then $H := G(F_1, \dots, F_m) \in \mathrm{I}(X)$, so by the earlier chain rule we have, for $v \in \mathrm{T}_a X$,

$$0 = d_a H(v) = d_b G(d_a f_1(v), \dots, d_a f_n(v)),$$

which yields the desired result. $\square$

We define $d_a f := (d_a f_1, \dots, d_a f_n) : \mathrm{T}_a X \to \mathrm{T}_b Y$, a $\mathbf{k}$-linear map, and we bundle these maps as $a$ varies into a single map

$$\mathrm{T} f : \ \mathrm{T} X \to \mathrm{T} Y, \qquad \mathrm{T} f(x, v) := (f(x), d_x f(v)).$$

It is easy to check that $\mathrm{T} f : \mathrm{T} X \to \mathrm{T} Y$ is a regular map.

Suppose $Z \subseteq \mathbf{k}^p$ is also an algebraic set and $g = (g_1, \dots, g_p) : Y \to Z$ is a regular map, and $c = g(b)$. Then the earlier chain rule yields

$$d_a(g \circ f) \ = \ d_b g \circ d_a f, \qquad \mathrm{T}(g \circ f) = (\mathrm{T}\, g) \circ (\mathrm{T} f).$$

Note that if $m = n$ and $X \subseteq Y$, then $\mathrm{T}_a X \subseteq \mathrm{T}_a Y \subseteq \mathbf{k}^m$, and the inclusion map $\iota : X \hookrightarrow Y$ yields the inclusion maps

$$d_a \iota : \ \mathrm{T}_a X \hookrightarrow \mathrm{T}_a Y, \qquad \mathrm{T}\,\iota : \ \mathrm{T} X \hookrightarrow \mathrm{T} Y.$$

**Corollary 5.9.** *Let $a \in X, b \in Y$. Then*

$$\mathrm{T}_{(a,b)}(X \times Y) \ = \ (\mathrm{T}_a X) \times (\mathrm{T}_b Y) \subseteq \mathbf{k}^m \times \mathbf{k}^n = \mathbf{k}^{m+n}.$$

*Proof.* Let $T_1, \dots, T_m, U_1, \dots, U_n$ be distinct variables. Take polynomials $F_1, \dots, F_p \in \mathbf{k}[T_1, \dots, T_m]$ and $G_1, \dots, G_q \in \mathbf{k}[U_1, \dots, U_n]$ such that

$$\mathrm{I}(X) = (F_1, \dots, F_p)\mathbf{k}[T_1, \dots, T_m], \qquad \mathrm{I}(Y) = (G_1, \dots, G_q)\mathbf{k}[U_1, \dots, U_n].$$

Then by Corollary 5.5

$$\mathrm{I}(X \times Y) \ = \ (F_1, \dots, F_p, G_1, \dots, G_q)\mathbf{k}[T_1, \dots, T_m, U_1, \dots, U_n],$$

from which the desired result follows. $\square$

**The basic duality.** Let $K$ be a field and $V$ and $W$ finite-dimensional $K$-vector spaces. A *dual pairing* of $V$ and $W$ is a function

$$(v,w) \mapsto \langle v,w\rangle : \; V \times W \to K$$

with the following properties:

(i) $\langle\ ,\ \rangle$ is $K$-bilinear, that is, $\langle v,-\rangle : W \to K$ and $\langle -,w\rangle : V \to K$ are $K$-linear for all $v \in V$ and $w \in W$;

(ii) if $v \in V$ and $\langle v,w\rangle = 0$ for all $w \in W$, then $v = 0$, and if $w \in W$ and $\langle v,w\rangle = 0$ for all $v \in V$, then $w = 0$.

Such a dual pairing yields the injective $K$-linear maps

$$v \mapsto \langle v,-\rangle : \; V \to W^*, \qquad w \mapsto \langle -,w\rangle : \; W \to V^*,$$

and since $V$ and $V^*$ have the same finite $K$-vector space dimension, as well as $W$ and $W^*$, it follows that these two maps are actually $K$-linear isomorphisms, and that $V$ and $W$ have the same $K$-vector space dimension.

Let $a \in X$. We have the $\mathbf{k}$-bilinear map

$$d_a : \; \mathfrak{m}_{X,a} \times \mathrm{T}_a X \to \mathbf{k}, \qquad d_a(f,v) := d_a f(v)$$

and since $d_a f(v) = 0$ for $f \in \mathfrak{m}^2_{X,a}$, this gives a $\mathbf{k}$-bilinear map

$$(f + \mathfrak{m}^2_{X,a}, v) \mapsto d_a f(v) : \; (\mathfrak{m}_{X,a}/\mathfrak{m}^2_{X,a}) \times \mathrm{T}_a X \; \to \mathbf{k} \quad (f \in \mathfrak{m}_{X,a}),$$

which we also denote by $d_a$. Here both vector spaces $\mathfrak{m}_{X,a}/\mathfrak{m}^2_{X,a}$ and $\mathrm{T}_a X$ are finite dimensional.

**Lemma 5.10.** *The map* $d_a : \; (\mathfrak{m}_{X,a}/\mathfrak{m}^2_{X,a}) \times \mathrm{T}_a X \; \to \mathbf{k}$ *is a dual pairing of the* $\mathbf{k}$*-linear spaces* $\mathfrak{m}_{X,a}/\mathfrak{m}^2_{X,a}$ *and* $\mathrm{T}_a X$*.*

*Proof.* Let $v \in \mathrm{T}_a X$ be such that $d_a f(v) = 0$ for all $f \in \mathfrak{m}_{X,a}$. For $f = t_i - a_i$, $1 \le i \le m$, we have $f \in \mathfrak{m}_{X,a}$, so

$$d_a f(v) = d_a(T_i - a_i)(v) = d_a T_i(v) = v_i = 0,$$

hence $v = 0$. Next, let $f \in \mathfrak{m}_{X,a}$ be such that $d_a f(v) = 0$ for all $v \in \mathrm{T}_a X$. Take $F, F_1, \dots, F_n \in \mathbf{k}[T_1, \dots, T_m]$ such that

$$F|X = f, \qquad \mathrm{I}(X) = (F_1, \dots, F_n).$$

Then $d_a F$ vanishes on $\mathrm{T}_a X = \{v \in \mathbf{k}^m : \; d_a F_1(v) = \cdots = d_a F_n(v) = 0\}$, so

$$d_a F = c_1 d_a F_1 + \cdots + c_n d_a F_n, \qquad c_1, \dots, c_n \in \mathbf{k}.$$

With $G := F - (c_1 F_1 + \cdots + c_n F_n)$ this yields $d_a G = 0$ and $G(a) = 0$, so $G \in \mathfrak{m}^2_a$ by an earlier exercise, and thus $f = G|X \in \mathfrak{m}^2_{X,a}$. $\square$

**Corollary 5.11.** $\dim \mathrm{T}_a X \; = \; \dim(\mathfrak{m}_{X,a}/\mathfrak{m}^2_{X,a})$.

**Intrinsic tangent spaces.** Let $a$ be a point in $X$. Our definition of $\mathrm{T}_a X$ used the inclusion of $X$ in $\mathbf{k}^m$. It is important that a more intrinsic definition is available. The idea is to think of a tangent vector $v \in \mathrm{T}_a X \subseteq \mathbf{k}^m$ as the operation $D_v$ of taking the derivative at $a$ in the $v$-direction,

$$D_v : \mathbf{k}[X] \to \mathbf{k}, \quad D_v(f) = d_a f(v) \qquad (\text{“the } v\text{-derivation”}).$$

More precisely, this operation is a *derivation on $X$ at $a$*; this is by definition a $\mathbf{k}$-linear map $D : \mathbf{k}[X] \to \mathbf{k}$ such that

$$D(fg) = f(a)D(g) + g(a)D(f) \quad \text{ for all } f, g \in \mathbf{k}[X].$$

Let $\mathrm{Der}(\mathbf{k}[X], a)$ be the set of derivations on $X$ at $a$; it is a $\mathbf{k}$-vector space with respect to the pointwise addition and scalar multiplication operations.

**Lemma 5.12.** *The map*

$$v \mapsto D_v : \ \mathrm{T}_a X \to \mathrm{Der}(\mathbf{k}[X], a)$$

*is an isomorphism of* $\mathbf{k}$*-vector spaces.*

*Proof.* It is easy to check that this map is $\mathbf{k}$-linear. Injectivity of this map means that if $v \in \mathrm{T}_a X$ and $d_a f(v) = 0$ for all $f \in \mathbf{k}[X]$, then $v = 0$; this was established in the beginning of the proof of Lemma 5.10. Surjectivity: let $D$ be a derivation on $X$ at $a$, and set $v := \big(D(t_1), \dots, D(t_m)\big) \in \mathbf{k}^m$. Then one checks easily that $v \in \mathrm{T}_a X$ and $D = D_v$. $\square$

This lemma suggests an intrinsic redefinition of $\mathrm{T}_a X$ as the $\mathbf{k}$-vector space $\mathrm{Der}(\mathbf{k}[X], a)$. A key point is how this translates under regular maps. Let $\phi : X \to Y$ be a regular map, $b = \phi(a)$. One verifies easily that then for $v \in \mathrm{T}_a X$ and $w := d_a\phi(v) \in \mathrm{T}_b Y$ we have

$$D_w \ = \ D_v \circ \phi^* \ \in \mathrm{Der}(\mathbf{k}[Y], b).$$

It is desirable to be even more intrinsic by defining $\mathrm{T}_a X$ purely in terms of the *local* algebra $\mathcal{O}_{X,a}$.

Towards this goal, define an *evaluation* on an algebra $A$ to be an algebra morphism $\chi : A \to \mathbf{k}$. An *algebra with evaluation* is a pair $(A, \chi)$ where $A$ is an algebra and $\chi$ is an evaluation on $A$. Let $(\mathbf{k}[X], a)$ denote the algebra $\mathbf{k}[X]$ with evaluation $f \mapsto f(a)$. The only evaluation on $\mathcal{O}_{X,a}$ is $\gamma \mapsto \gamma(a)$, so we consider $\mathcal{O}_{X,a}$ as an algebra with evaluation in the only way possible. Let $(A, \chi)$ be an algebra with evaluation. Then $\mathrm{Der}(A, \chi)$ is the set of all $\mathbf{k}$-linear maps $D : A \to \mathbf{k}$ such that $D(fg) = \chi(f)D(g) + \chi(g)D(f)$ for all $f, g \in A$. Then $\mathrm{Der}(A, \chi)$ is a $\mathbf{k}$-vector space with respect to the pointwise addition and scalar multiplication operations.

This yields in particular the $\mathbf{k}$-vector space $\mathrm{Der}(\mathcal{O}_{X,a})$, whose elements are the $\mathbf{k}$-linear maps $D : \mathcal{O}_{X,a} \to k$ such that

$$D(\beta\gamma) = \beta(a)D(\gamma) + \gamma(a)D(\beta), \quad (\beta, \gamma \in \mathcal{O}_{X,a}).$$

**Lemma 5.13.** *For each $D \in \mathrm{Der}(\mathbf{k}[X], a)$ there is a unique $D_a \in \mathrm{Der}(\mathcal{O}_{X,a})$ such that $D_a(\gamma_a f) = D(f)$ for all $f \in \mathbf{k}[X]$. The map*

$$D \mapsto D_a : \mathrm{Der}(\mathbf{k}[X], a) \to \mathrm{Der}(\mathcal{O}_{X,a})$$

*is an isomorphism of* $\mathbf{k}$*-linear spaces.*

In particular, each tangent vector $v \in \mathrm{T}_a X$ yields an element

$$D_{v,a} := (D_v)_a \in \mathrm{Der}(\mathcal{O}_{X,a}).$$

We now define the *intrinsic tangent space of $X$ at $a$* to be the $\mathbf{k}$-vector space $\mathrm{Der}(\mathcal{O}_{X,a})$. When we use words like "the intrinsic tangent space $\mathrm{T}_a X$" we mean that we identify the tangent space $\mathrm{T}_a X \subseteq \mathbf{k}^m$ with the intrinsic tangent space of $X$ at $a$ via the $\mathbf{k}$-linear isomorphism

$$v \mapsto D_{v,a} : \ \mathrm{T}_a X \to \mathrm{Der}(\mathcal{O}_{X,a}).$$

If $\phi : X \to Y$ is a regular map and $b = \phi(a)$, $v \in \mathrm{T}_a X$ and $w := d_a\phi(v) \in \mathrm{T}_b Y$, then

$$D_{w,b} = D_{v,a} \circ \phi_b^* \in \mathrm{Der}(\mathcal{O}_{Y,b}).$$

**Fields of definition.** Let $K$ a subfield of $\mathbf{k}$. Then $K$ is said to be a *field of definition of $X$* if $K$ is a field of definition of its ideal $\mathrm{I}(X)$, that is, $\mathrm{I}(X)$ is generated as an ideal of $\mathbf{k}[T_1, \dots, T_m]$ by polynomials in $K[T_1, \dots, T_m]$. Note that if $K$ is a field of definition of $X$, then $X$ is defined over $K$ in $\mathbf{k}$, in the sense of model theory. The converse is true if $K$ is perfect, in particular, if $\mathbf{k}$ has characteristic zero:

**Proposition 5.14.** *Suppose $K$ is perfect. Then $K$ is a field of definition of $X$ if and only if $X$ is defined over $K$ in the sense of model theory.*

*Proof.* Let $X$ be defined over $K$. Then $\sigma(X) = X$ for all $\sigma \in \mathrm{Aut}(\mathbf{k}|K)$, so with $I := \mathrm{I}(X)$ we have $\sigma(I) = I$ for all $\sigma \in \mathrm{Aut}(\mathbf{k}|K)$. Take $a \in \mathbf{k}^n$ such that $\mathbb{F}(a)$ is the smallest field of definition of $I$, where $\mathbb{F}$ is the prime field of $\mathbf{k}$. Then $\sigma(I) = I \ \Leftrightarrow \ \sigma(a) = a$, for all $\sigma \in \mathrm{Aut}(\mathbf{k})$, and thus $\sigma(a) = a$ for all $\sigma \in \mathrm{Aut}(\mathbf{k}|K)$. Since $K$ is perfect, it is the fixed field of $\mathrm{Aut}(\mathbf{k}|K)$, so $a \in K^n$, and thus $\mathbb{F}(a) \subseteq K$. $\square$

We cannot omit in this result the assumption that $K$ is perfect. To see why, suppose $K$ is not perfect. Then $K$ has characteristic $p > 0$ and we can take $a \in K$ such that $a \neq b^p$ for all $b \in K$. Then the set

$$X := \{x \in \mathbf{k} : \ x^p = a\} = \{a^{1/p}\} \subseteq \mathbf{k}$$

is defined over $K$ in the sense of model theory, but $X$ does not have $K$ as a field of definition. This is because

$$\mathrm{I}(X) \cap K[T_1] \ = \ (T_1^p - a)K[T_1]$$

but $T_1 - a^{1/p} \in \mathrm{I}(X) \setminus (T_1^p - a)\mathbf{k}[T_1]$.

## 6. Algebraic varieties and algebraic groups

The basic features of algebraic sets in spaces $\mathbf{k}^m$ can be seen as direct consequences of simple facts about polynomials. We now turn to algebraic varieties that are in general not given as subsets of spaces $\mathbf{k}^m$, but are obtained by glueing algebraic sets. We first describe glueing very generally.

**k-spaces.** Till further notice, $\mathbf{k}$ is any set. A $\mathbf{k}$-space is by definition a pair $(X, \mathcal{F})$ where $X$ is a space and $\mathcal{F}$ a *sheaf* of $\mathbf{k}$-valued functions on $X$, that is, $\mathcal{F}$ assigns to each open $U \subseteq X$ a subset $\mathcal{F}(U)$ of the set $\mathbf{k}^U$ of functions $f : U \to \mathbf{k}$ such that:

(Sh1) if $U \subseteq V$ with open $V \subseteq X$, then the restriction map $f \mapsto f|U$ maps $\mathcal{F}(V)$ into $\mathcal{F}(U)$;

(Sh2) if $(U_i)$ is a covering of $U$ by open subsets and $f : U \to \mathbf{k}$ has the property that $f|U_i \in \mathcal{F}(U_i)$ for all $i$, then $f \in \mathcal{F}(U)$.

**Example.** Suppose $\mathbf{k}$ is an algebraically closed field and $X \subseteq \mathbf{k}^m$ is an algebraic set. Then $(X, \mathcal{O}_X)$ is a $\mathbf{k}$-space, as is easily verified.

Below we let $(X, \mathcal{F})$, $(Y, \mathcal{G})$, and $(Z, \mathcal{H})$ denote $\mathbf{k}$-spaces. A *morphism* $(X, \mathcal{F}) \to (Y, \mathcal{G})$ (of $\mathbf{k}$-spaces) is a continuous map $\alpha : X \to Y$ such that for each open $V \subseteq Y$ and $U := \alpha^{-1}(V)$,

$$g \in \mathcal{G}(V) \implies g \circ (\alpha|U) \in \mathcal{F}(U).$$

For such $\alpha$ and $U, V$ we denote the operation $g \mapsto g \circ (\alpha|U) : \mathcal{G}(V) \to \mathcal{F}(U)$ by $\alpha_V^*$. The identity map $\mathrm{id}_X$ on $X$ is a morphism $(X, \mathcal{F}) \to (X, \mathcal{F})$, and if $\alpha : (X, \mathcal{F}) \to (Y, \mathcal{G})$ and $\beta : (Y, \mathcal{G}) \to (Z, \mathcal{H})$ are morphisms, so is

$$\beta \circ \alpha : (X, \mathcal{F}) \to (Z, \mathcal{H}).$$

Thus the $\mathbf{k}$-spaces with their morphisms form a category with the above identity maps as identity morphisms and where composition of morphisms is given by composition of maps. A morphism $\alpha$ as above is an isomorphism in this category iff $\alpha$ is a homeomorphism and $\alpha_V^*$ is a bijection for each open $V \subseteq X$.

Suppose $\mathbf{k}$ is a ring. For any set $U$, consider $\mathbf{k}^U = \{f : U \to \mathbf{k}\}$ as a ring with pointwise defined addition and multiplication. Adding to the above definition of "$\mathbf{k}$-space" the requirement that $\mathcal{F}(U)$ is a subring of $\mathbf{k}^U$ for each open $U \subseteq X$, makes $(X, \mathcal{F})$ into a *ringed* $\mathbf{k}$-*space*. (The restriction map $\mathcal{F}(V) \to \mathcal{F}(U)$ in (Sh1) above is then a ring morphism.) If $(X, \mathcal{F})$ and $(Y, \mathcal{G})$ are ringed $\mathbf{k}$-spaces and $\alpha : (X, \mathcal{F}) \to (Y, \mathcal{G})$ is a morphism of $\mathbf{k}$-spaces, then $\alpha$ is automatically a morphism of ringed $\mathbf{k}$-spaces in the sense that each $\alpha_V^*$ is a ring morphism.

**Example.** Let $\mathbf{k}$ be an algebraically closed field. If $X \subseteq \mathbf{k}^m$ is an algebraic set, then $(X, \mathcal{O}_X)$ is clearly a ringed $\mathbf{k}$-space. If $X \subseteq \mathbf{k}^m$ and $Y \subseteq \mathbf{k}^n$ are algebraic sets, then the regular maps $X \to Y$ are exactly the morphisms $(X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$.

Let $(X, \mathcal{F})$ be a $\mathbf{k}$-space and let $U \subseteq X$ be open. Then we define the sheaf $\mathcal{F}|U$ of $\mathbf{k}$-valued functions on $U$ by:

$$(\mathcal{F}|U)(V) := \mathcal{F}(V) \quad \text{for open } V \subseteq U.$$

Then the inclusion $U \hookrightarrow X$ is a morphism $(U, \mathcal{F}|U) \to (X, \mathcal{F})$. Let $(Y, \mathcal{G})$ be a second $\mathbf{k}$-space, $\alpha : X \to Y$ a map, and $V$ an open subset of $Y$ with $\alpha(X) \subseteq V$. Then the following are equivalent:

(i) $\alpha$ is a morphism $(X, \mathcal{F}) \to (V, \mathcal{G}|V)$;
(ii) $\alpha$ is a morphism $(X, \mathcal{F}) \to (Y, \mathcal{G})$;
(iii) for each $x \in X$ there is an open neighborhood $U$ of $x$ in $X$ such that $\alpha|U : (U, \mathcal{F}|U) \to (Y, \mathcal{G})$ is a morphism.

We shall use this fact without mentioning it in what follows.

**Example.** Let $\mathbf{k}$ be an algebraically closed field, $X \subseteq \mathbf{k}^m$ an algebraic set, and $U := X_f$ a basic open set, $f \in \mathbf{k}[X]$. Then

$$Y := \{(x, t) \in \mathbf{k}^{m+1} : f(x)t = 1\}$$

is an algebraic set in $\mathbf{k}^{m+1}$, and the regular map $(x, t) \mapsto x : Y \to X$ has image $U$ and gives an isomorphism $(Y, \mathcal{O}_Y) \to (U, \mathcal{O}_X|U)$ of $\mathbf{k}$-spaces.

**Lemma 6.1.** (Glueing $\mathbf{k}$-spaces). *Let $(U_i)$ be a covering of a set $X$ by subsets, and suppose for each $i$ there is given a topology $t_i$ on $U_i$ and a sheaf $\mathcal{F}_i$ of $\mathbf{k}$-valued functions on $(U_i, t_i)$ such that for all $i, j$,*

(a) *$U_i \cap U_j$ is open in $(U_i, t_i)$ and in $(U_j, t_j)$ and the topologies on $U_i \cap U_j$ induced by $t_i$ and $t_j$ are the same;*
(b) *$\mathcal{F}_i|U_i \cap U_j \;=\; \mathcal{F}_j|U_i \cap U_j$.*

*Then there is a unique pair $(t, \mathcal{F})$ consisting of a topology $t$ on $X$ and a sheaf $\mathcal{F}$ of $\mathbf{k}$-valued functions on $(X, t)$ such that for each $i$ the set $U_i$ is open in $(X, t)$, the topology on $U_i$ induced by $t$ is $t_i$, and $\mathcal{F}|U_i = \mathcal{F}_i$.*

*Proof.* Let $t$ be the topology on $X$ whose open sets are the $U \subseteq X$ such that $U \cap U_i$ is open in $(U_i, t_i)$ for each $i$. For each $t$-open $U \subseteq X$, let

$$\mathcal{F}(U) := \{f : U \to \mathbf{k} : \; f|U \cap U_i \in \mathcal{F}_i(U \cap U_i) \text{ for all } i\}.$$

It is easy to check that $(t, \mathcal{F})$ has the desired properties. $\square$

Let $(X, \mathcal{F})$ be a $\mathbf{k}$-space and $Y$ a subspace of $X$. Then we obtain a $\mathbf{k}$-space $(Y, \mathcal{F}|Y)$ as follows. For an open subset $U$ of $Y$, a function $f : U \to \mathbf{k}$ belongs to $(\mathcal{F}|Y)(U)$ iff for each $x \in U$ there is an open neighborhood $U_x$ of $x$ in $X$ with a function $f_x \in \mathcal{F}(U_x)$ such that $f|U \cap U_x = f_x|U \cap U_x$. Note that the inclusion $Y \hookrightarrow X$ is a morphism $(Y, \mathcal{F}|Y) \to (X, \mathcal{F})$, and that if $Z$ is a subspace of $Y$ (and hence of $X$), then $(\mathcal{F}|Y)|Z = \mathcal{F}|Z$.

This construction is particularly relevant when $Y$ is closed in $X$. If $Y$ is open in $X$, this sheaf $\mathcal{F}|Y$ coincides with the sheaf $\mathcal{F}|Y$ defined earlier in that case. If $\mathbf{k}$ is a ring and $(X, \mathcal{F})$ is a ringed $\mathbf{k}$-space, then $(Y, \mathcal{F}|Y)$ is a ringed $\mathbf{k}$-space.

**Example.** Let $\mathbf{k}$ be an algebraically closed field, $X \subseteq \mathbf{k}^m$ an algebraic set, and $Y$ a closed subset of $X$. Then $Y$ is an algebraic set and $\mathcal{O}_Y = \mathcal{O}_X|Y$.

**Geometric k-spaces.** In this subsection $\mathbf{k}$ is a field.

A *geometric* $\mathbf{k}$*-space* is a ringed $\mathbf{k}$-space $(X, \mathcal{F})$ such that for every open $U$ in $X$,

(i) all constant functions $U \to \mathbf{k}$ belong to $\mathcal{F}(U)$;
(ii) if $a \in U$, $f \in \mathcal{F}(U)$, and $f(a) \neq 0$, then there is an open $V \subseteq U$ such that $a \in V$ and $f|V$ is a unit of $\mathcal{F}(V)$ (so $f(x) \neq 0$ for all $x \in V$).

Note that if $(X, \mathcal{F})$ is a geometric $\mathbf{k}$-space and $Y$ is a subspace of $X$, then $(Y, \mathcal{F}|Y)$ is also a geometric $\mathbf{k}$-space. If $(X, \mathcal{F})$ is a ringed $\mathbf{k}$-space and $(U_i)$ is a covering of $X$ by open subsets such that each $(U_i, \mathcal{F}|U_i)$ is a geometric $\mathbf{k}$-space, then $(X, \mathcal{F})$ is a geometric $\mathbf{k}$-space.

Let $(X, \mathcal{F})$ be a geometric $\mathbf{k}$-space. For open $U \subseteq X$ we consider the ring $\mathcal{F}(U)$ as a $\mathbf{k}$-algebra via the ring morphism $\mathbf{k} \to \mathcal{F}(U)$ that assigns to each $c \in \mathbf{k}$ the constant function on $U$ with value $c$. If $U \subseteq X$ is open and $U \neq \emptyset$, then we identify $\mathbf{k}$ with a subring of $\mathcal{F}(U)$ via this ring morphism.

Let $a \in X$ and let $U, V, W$ range over open neighborhoods of $a$ in $X$. The behaviour of $X$ near $a$ is encoded in the $\mathbf{k}$-algebra $\mathcal{F}_a$ whose elements are the germs of functions in the various $\mathbf{k}$-algebras $\mathcal{F}(U)$. The precise definition of $\mathcal{F}_a$ is as follows. Introduce an equivalence relation $\sim_a$ on the disjoint union of the sets $\mathcal{F}(U)$: for $f \in \mathcal{F}(U)$, $g \in \mathcal{F}(V)$,

$$f \sim_a g \;:\Longleftrightarrow\; f|W = g|W \text{ for some } W \subseteq U \cap V.$$

The equivalence class $\gamma_a f$ of $f \in \mathcal{F}(U)$ with respect to $\sim_a$ is called the *germ of $f$ at $a$*; for such a germ $\gamma = \gamma_a f$ we set $(\gamma_a f)(a) := f(a)$. The set of germs of functions in $\bigcup_U \mathcal{F}(U)$ is denoted by $\mathcal{F}_a$, and is made into a $\mathbf{k}$-algebra by requiring that for each $U$ the map

$$f \mapsto \gamma_a f : \; \mathcal{F}(U) \to \mathcal{F}_a$$

is a $\mathbf{k}$-algebra morphism. We identify the $\mathbf{k}$-algebras $\mathcal{F}_a$ and $(\mathcal{F}|U)_a$ in the obvious way: for $V \subseteq U$ and $f \in \mathcal{F}(V) = (\mathcal{F}|U)(V)$,

$$\gamma_a f \text{ (in } \mathcal{F}_a) \;=\; \gamma_a f \text{ (in } (\mathcal{F}|U)_a).$$

Note that $\gamma \mapsto \gamma(a) : \mathcal{F}_a \to \mathbf{k}$ is a $\mathbf{k}$-algebra morphism, and that if $\gamma \in \mathcal{F}_a$ and $\gamma(a) \neq 0$, then $\gamma$ is a unit of $\mathcal{F}_a$. It follows that $\mathcal{F}_a$ is a local $\mathbf{k}$-algebra with maximal ideal $\mathfrak{m}(\mathcal{F}_a) = \{\gamma \in \mathcal{F}_a : \; \gamma(a) = 0\}$, and

$$\mathcal{F}_a = \mathbf{k} \oplus \mathfrak{m}(\mathcal{F}_a) \qquad \text{(internal direct sum of } \mathbf{k}\text{-linear subspaces)},$$

Note that $\gamma \mapsto \gamma(a) : \mathcal{F}_a \to \mathbf{k}$ is the unique evaluation on the $\mathbf{k}$-algebra $\mathcal{F}_a$; we view $\mathcal{F}_a$ as a $\mathbf{k}$-algebra with evaluation in the only way possible. This allows us to define the (intrinsic) tangent space $\mathrm{T}_a(X, \mathcal{F})$ of $(X, \mathcal{F})$ at $a$ to be the $\mathbf{k}$-linear space

$$\mathrm{T}_a(X, \mathcal{F}) := \mathrm{Der}(\mathcal{F}_a).$$

In particular, $\mathrm{T}_a(X,\mathcal{F}) = \mathrm{T}_a(U,\mathcal{F}|U)$. These constructions are functorial: Let a morphism $\phi : (X,\mathcal{F}) \to (Y,\mathcal{G})$ into a geometric **k**-space $(Y,\mathcal{G})$ be given, and let $b = \phi(a)$. Then we have the **k**-algebra morphism

$$\phi_a^* : \mathcal{G}_b \to \mathcal{F}_a, \quad \phi_a^*(\gamma_b g) := \gamma_a\big(\phi_O^*(g)\big) \quad (g \in \mathcal{G}(O),\ O \text{ open in } Y,\ b \in O),$$

with $\phi_a^*\big(\mathfrak{m}(\mathcal{G}_b)\big) \subseteq \mathfrak{m}(\mathcal{F}_a)$, so we can define the **k**-linear map

$$d_a\phi : \mathrm{T}_a(X,\mathcal{F}) \to \mathrm{T}_b(Y,\mathcal{G}), \quad d_a\phi(v) := v \circ \phi_a^*.$$

When in addition $\psi : (Y,\mathcal{G}) \to (Z,\mathcal{H})$ is a morphism into the geometric **k**-space $(Z,\mathcal{H})$ and $c = \psi(b)$, then

$$(\psi \circ \phi)_a^* = \phi_a^* \circ \psi_b^*, \quad d_a(\psi \circ \phi) = (d_b\psi) \circ (d_a\phi).$$

We bundle these tangent spaces into a single object

$$\mathrm{T}(X,\mathcal{F}) := \bigcup_{a \in X} \{a\} \times \mathrm{T}_a(X,\mathcal{F}) \qquad (\text{the tangent bundle of } (X,\mathcal{F})),$$

and for $\phi : (X,\mathcal{F}) \to (Y,\mathcal{G})$ as above we define the map

$$\mathrm{T}\,\phi :\ \mathrm{T}(X,\mathcal{F}) \to \mathrm{T}(Y,\mathcal{G}), \quad \mathrm{T}\,\phi(a,v) = \big(\phi(a), d_a\phi(v)\big).$$

Again, we have functoriality: with $\phi$ and $\psi$ as above,

$$\mathrm{T}(\psi \circ \phi) = (\mathrm{T}\,\psi) \circ (\mathrm{T}\,\phi).$$

**Affine models and Products.** In this subsection we take the sets

$$\mathbf{k}^0 = \{0\},\ \mathbf{k}^1 = \mathbf{k},\ \mathbf{k}^2, \mathbf{k}^3, \dots$$

to be mutually disjoint. We assume that certain subsets of $\mathbf{k}^n$, for $n = 0, 1, 2, \dots$, have been singled out, which we shall call *affine sets*, and that to each affine set $X$ a topology $t_X$ and a sheaf $\mathcal{F}_X$ of **k**-valued functions on $(X, t_X)$ is associated, so $(X, t_X, \mathcal{F}_X)$ is a **k**-space. These distinguished **k**-spaces will be referred to as *affine models*. Since an affine model $(X, t_X, \mathcal{F}_X)$ is uniquely determined by its underlying affine set $X$ we also indicate it just by $X$. A **k**-space is said to be *affine* if it is isomorphic to an affine model. A **k**-space $(X,\mathcal{F})$ is said to be *locally affine* if each $x \in X$ has an open neighborhood $U$ such that $(U,\mathcal{F}|U)$ is affine. Unless specified otherwise, "morphism" means "morphism of **k**-spaces".

We now make three further assumptions about affine sets $X \subseteq \mathbf{k}^m$:

(C) all constant functions $X \to \mathbf{k}$ belong to $\mathcal{F}_X(X)$;
(LA) if $U \subseteq X$ is open, then the **k**-space $(U, \mathcal{F}_X|U)$ is locally affine;
(Pr) if $Y \subseteq \mathbf{k}^n$ is also an affine set, then $X \times Y \subseteq \mathbf{k}^{m+n}$ is an affine set, the projection maps $X \times Y \to X$ and $X \times Y \to Y$ are morphisms and whenever $Z$ is an affine set and $f : Z \to X$ and $g : Z \to Y$ are morphisms, then $(f,g) : Z \to X \times Y$ is a morphism.

It is clear from (C) and (LA) that for any locally affine $\mathbf{k}$-space $(X, \mathcal{F})$ all constant functions $X \to \mathbf{k}$ belong to $\mathcal{F}(X)$. It also follows from (LA) that if $(X, \mathcal{F})$ is a locally affine $\mathbf{k}$-space and $U$ is an open subset of $X$, then $(U, \mathcal{F}|U)$ with the induced topology on $U$ is a locally affine $\mathbf{k}$-space, which for simplicity we just denote by $U$ if the ambient $(X, \mathcal{F})$ is clear from the context. By an *affine open part* of a locally affine $\mathbf{k}$-space $(X, \mathcal{F})$ we mean an open $U \subseteq X$ that is affine as a $\mathbf{k}$-space. With the notations of (Pr), the affine set $X \times Y$ with the projection maps to $X$ and $Y$ is a product of $X$ and $Y$ in the full subcategory of affine $\mathbf{k}$-spaces of the category of $\mathbf{k}$-spaces; it is even a product in the full subcategory of locally affine $\mathbf{k}$-spaces, as is easily verified.

**Example.** Let $\mathbf{k}$ be an algebraically closed field. Taking as affine models the $(X, \mathcal{O}_X)$ where $X \subseteq \mathbf{k}^m$ is an algebraic set with its Zariski topology, $m = 0, 1, 2, \dots$, the assumptions above are satisfied. To see why (LA) holds, let $X \subseteq \mathbf{k}^m$ be an algebraic set and $U = X_f$ a *basic* open set in $X$, $f \in \mathbf{k}[X]$. Then we saw earlier that $(U, \mathcal{O}_X|U) \cong (Y, \mathcal{O}_Y)$ where

$$Y := \{(x, t) \in \mathbf{k}^{m+1} : \ x \in X, \ f(x) \cdot t = 1\}$$

is an algebraic set in $\mathbf{k}^{m+1}$, so $(U, \mathcal{O}_X|U)$ is affine.

Let $(X, \mathcal{F})$ and $(Y, \mathcal{G})$ be locally affine $\mathbf{k}$-spaces. A *set-like product of* $(X, \mathcal{F})$ *and* $(Y, \mathcal{G})$ is a locally affine $\mathbf{k}$-space $(X \times Y, t, \mathcal{H})$, where $t$ is a topology on the cartesian product $X \times Y$, and $\mathcal{H}$ is a sheaf of $\mathbf{k}$-valued functions on $(X \times Y, t)$ such that the projection maps to $X$ and $Y$ are morphisms

$$(X \times Y, t, \mathcal{H}) \to (X, \mathcal{F}), \qquad (X \times Y, t, \mathcal{H}) \to (Y, \mathcal{G}),$$

and for each locally affine $\mathbf{k}$-space $(Z, \mathcal{K})$ and morphisms

$$f : (Z, \mathcal{K}) \to (X, \mathcal{F}), \qquad g : (Z, \mathcal{K}) \to (Y, \mathcal{G})$$

the map $(f, g) : Z \to X \times Y$ is a morphism $(Z, \mathcal{K}) \to (X \times Y, t, \mathcal{H})$.

Suppose $(X \times Y, t, \mathcal{H})$ and $(X \times Y, t', \mathcal{H}')$ are both set-like products of $(X, \mathcal{F})$ and $(Y, \mathcal{G})$. Then the identity on $X \times Y$ must be an isomorphism $(X \times Y, t, \mathcal{H}) \to (X \times Y, t', \mathcal{H}')$, so $t = t'$ and $\mathcal{H} = \mathcal{H}'$. Because of this uniqueness we put $\mathcal{H} := \mathcal{F} \odot \mathcal{G}$ and let $(X \times Y, \mathcal{F} \odot \mathcal{G})$ denote $(X \times Y, t, \mathcal{H})$, leaving out $t$ for simplicity.

If $U \subseteq X$ and $V \subseteq Y$ are open, then $U \times V \subseteq X \times Y$ is open, by the continuity of the projection maps $X \times Y \to X$ and $X \times Y \to Y$. But the topology $t$ on $X \times Y$ is not necessarily the product topology. We have already noted that any two affine $\mathbf{k}$-spaces have a set-like product (which is not just locally affine, but even affine).

**Lemma 6.2.** *Suppose the locally affine* $\mathbf{k}$*-spaces* $(X, \mathcal{F})$ *and* $(Y, \mathcal{G})$ *have a set-like product, and let* $U \subseteq X$ *and* $V \subseteq Y$ *be open. Then* $(U, \mathcal{F}|U)$ *and* $(V, \mathcal{G}|V)$ *have a set-like product, namely* $(U \times V, (\mathcal{F} \odot \mathcal{G})|U \times V)$*, the topology on* $U \times V$ *being induced by that of* $X \times Y$.

**Proposition 6.3.** *Let $(X, \mathcal{F})$ and $(Y, \mathcal{G})$ be locally affine* $\mathbf{k}$*-spaces. Then $(X, \mathcal{F})$ and $(Y, \mathcal{G})$ have a set-like product.*

*Proof.* Let $(U_i)_{i \in I}$ be a covering of $X$ by affine open parts, and let $(V_j)_{j \in J}$ be a covering of $Y$ by affine open parts. Let $i$ and $j$ range over $I$ and $J$, respectively, and put $\mathcal{F}_i := \mathcal{F}|U_i$, $\mathcal{G}_j := \mathcal{G}|V_j$. Consider each $U_i \times V_j \subseteq X \times Y$ with the unique topology $t_{ij}$ and sheaf $\mathcal{F}_i \odot \mathcal{G}_j$ making $(U_i \times V_j, t_{ij}, \mathcal{F}_i \odot \mathcal{G}_j)$ the set-like product of $(U_i, \mathcal{F}_i)$ with $(V_j, \mathcal{G}_j)$. Now, for $i_1, i_2 \in I$ and $j_1, j_2 \in J$, the set

$$(U_{i_1} \times V_{j_1}) \cap (U_{i_2} \times V_{j_2}) = (U_{i_1} \cap U_{i_2}) \times (V_{j_1} \cap V_{j_2})$$

is open in $(U_{i_1} \times V_{j_1}, t_{i_1 j_1})$ and by the previous lemma, the induced topology and the restriction of the sheaf $\mathcal{F}_{i_1} \odot \mathcal{G}_{j_1}$ make it the set-like product of $(U_{i_1} \cap U_{i_2}, \mathcal{F}|U_{i_1} \cap U_{i_2})$ with $(V_{j_1} \cap V_{j_2}, \mathcal{G}|V_{j_1} \cap V_{j_2})$. But the same is true for the topology induced by $U_{i_2} \times V_{j_2}$ and the restriction of the sheaf $\mathcal{F}_{i_2} \odot \mathcal{G}_{j_2}$. This allows us to apply the Glueing Lemma 6.1: equip $X \times Y$ with a topology $t$ and a sheaf $\mathcal{H}$ making $(X \times Y, t, \mathcal{H})$ a $\mathbf{k}$-space and such that for all $i$ and $j$, $U_i \times V_j$ is open in $X \times Y$ and

$$(U_i \times V_j, t_{ij}, \mathcal{F}_i \odot \mathcal{G}_j) = (U_i \times V_j, t|U_i \times V_j, \mathcal{H}|U_i \times V_j).$$

This already makes $(X \times Y, t, \mathcal{H})$ a locally affine $\mathbf{k}$-space. Let now $(Z, \mathcal{K})$ be a locally affine $\mathbf{k}$-space and let $f : (Z, \mathcal{H}) \to (X, \mathcal{F})$ and $g : (Z, \mathcal{H}) \to (Y, \mathcal{G})$ be morphisms. Then for all $i, j$ the set $f^{-1}(U_i) \cap g^{-1}(V_j) = Z_{ij}$ is open in $Z$ and the maps $f|Z_{ij} : \ Z_{ij} \to (U_i, \mathcal{F}_i)$ and $g|Z_{ij} : \ Z_{ij} \to (V_j, \mathcal{G}_j)$ are morphisms so that

$$(f, g)|Z_{ij} : \ (Z_{ij}, \mathcal{K}) \to (U_i \times V_j, \mathcal{F}_i \odot \mathcal{G}_j)$$

is a morphism. Since we have the inclusion morphisms

$$(U_i \times V_j, \mathcal{F}_i \odot \mathcal{G}_j) \to (X \times Y, t, \mathcal{H})$$

and $Z = \bigcup_{i,j} Z_{ij}$, the map $(f, g) : (Z, \mathcal{K}) \to (X \times Y, t, \mathcal{H})$ is a morphism. $\square$

**Lemma 6.4.** *Let $(X, \mathcal{F})$ and $(Y, \mathcal{G})$ be locally affine spaces and $b \in Y$. Then the constant map $X \to \{b\} \subseteq Y$ is a morphism $(X, \mathcal{F}) \to (Y, \mathcal{G})$, and the map $x \mapsto (x, b) : \ X \to X \times Y$ is a morphism $(X, \mathcal{F}) \to (X \times Y, \mathcal{F} \odot \mathcal{G})$.*

**Prevarieties.** In the rest of this section $\mathbf{k}$ is an algebraically closed field and our affine models are just the algebraic sets $X$ with their Zariski topology and their structure sheaf $\mathcal{O}_X$. Since every algebraic set with this topology and sheaf is a geometric $\mathbf{k}$-space, all locally affine $\mathbf{k}$-spaces are geometric $\mathbf{k}$-spaces. If $(X, \mathcal{F})$ is a locally affine $\mathbf{k}$-space and $x \in X$, then $\{x\}$ is closed in $X$, since $X \setminus \{x\}$ is open in $X$.

A *prevariety* is a locally affine $\mathbf{k}$-space with a *finite* covering by affine open subsets; equivalently, it is a *noetherian* locally affine $\mathbf{k}$-space. Every open subset of a prevariety is also a prevariety. Likewise for closed subsets: if $(X, \mathcal{F})$ is a prevariety and $Y$ is a closed subset of $X$, then $(Y, \mathcal{F}|Y)$ (with the induced topology on $Y$) is a prevariety.

We denote the sheaf of a prevariety $X$ by $\mathcal{O}_X$ and the set-like product of prevarieties $X, Y$ by $X \times Y$. If $X, Y$ are prevarieties, so is $X \times Y$; if $X$ and $Y$ are irreducible prevarieties, so is $X \times Y$. The affine model $\mathbf{k}^n$ is also referred to as *affine $n$-space* and denoted by $\mathbb{A}^n$. (It would be more accurate to denote it by $\mathbb{A}^n(\mathbf{k})$, but as long as $\mathbf{k}$ remains fixed this abuse of notation is harmless.) We identify in the usual way the product $\mathbb{A}^m \times \mathbb{A}^n$ of prevarieties with the prevariety $\mathbb{A}^{m+n}$.

**Exercise.** Let $X$ be a prevariety. The irreducible affine open parts of $X$ form a basis for the topology of $X$. A morphism $X \to \mathbb{A}^1$ is the same as a function $f \in \mathcal{O}_X(X)$. Given functions $\phi_1, \dots, \phi_n : X \to \mathbf{k}$, the map $\phi = (\phi_1, \dots, \phi_n) : X \to \mathbf{k}^n$ is a morphism $X \to \mathbb{A}^n$ iff $\phi_1, \dots, \phi_n \in \mathcal{O}_X(X)$.

**Projective Spaces.** The projective space $\mathbb{P}^n$ has as its points the lines $\mathbf{k}a \subseteq \mathbb{A}^{n+1}$ through the origin, with

$$a = (a_0, \dots, a_n) \in \mathbb{A}^{n+1}, \quad a_i \neq 0 \text{ for some } i.$$

We denote such a line $\mathbf{k}a$ also by $[a_0 : a_1 : \cdots : a_n]$. The symbol : is meant to indicate that only the ratios between the $a_i$ matter: if $a_0, \dots, a_n \in \mathbf{k}$ are not all zero, and $b_0, \dots, b_n \in \mathbf{k}$ are not all zero, then

$$[a_0 : a_1 : \cdots : a_n] = [b_0 : b_1 : \cdots : b_n] \iff \text{there is } \lambda \in \mathbf{k}^\times \text{ with } a_i = \lambda b_i \text{ for } i = 0, \dots, n.$$

Suppose the polynomial $F \in \mathbf{k}[T_0, \dots, T_n]$ is homogeneous of degree $d$. Then

$$F(\lambda a) = \lambda^d F(a) \ \text{ for } \lambda \in \mathbf{k} \text{ and } a \in \mathbf{k}^{n+1},$$

so we can define that a point $p = [a_0 : \cdots : a_n] \in \mathbb{P}^n$ is a *zero of* $F$ if $F(a_0, \dots, a_n) = 0$, since this depends only on $p$ and not on the choice of $a_0, \dots, a_n$. (But there is no such thing as a function $p \mapsto F(p) : \mathbb{P}^n \to \mathbf{k}$.) For each set $S$ of homogeneous polynomials in $\mathbf{k}[T_0, \dots, T_n]$ we set

$$\mathrm{Z}(S) := \{p \in \mathbb{P}^n : \ p \text{ is a zero of every } F \in S\},$$

and we note that there is a finite subset $S_0$ of $S$ such that $\mathrm{Z}(S) = \mathrm{Z}(S_0)$. Thus the sets $\mathrm{Z}(S)$ are the closed sets of a noetherian topology on $\mathbb{P}^n$, the *Zariski topology of* $\mathbb{P}^n$.

For $i = 0, \dots, n$ we have the open subset $U_i := \mathbb{P}^n \setminus \mathrm{Z}(T_i)$ of $\mathbb{P}^n$ and the bijection $h_i : \mathbb{A}^n \to U_i$ given by

$$h_i(a_1, \dots, a_n) = [a_1 : \cdots : a_i : 1 : a_{i+1} : \cdots : a_n].$$

We claim that $h_i$ is a homeomorphism. Consider for example

$$h = h_0 : \mathbb{A}^n \to U_0, \quad h(a_1, \dots, a_n) = [1 : a_1 : \cdots : a_n].$$

Then for $F \in \mathbf{k}[T_1, \dots, T_n]$ of total degree $\leq d$ its homogenization

$$G(T_0, \dots, T_n) := T_0^d F(T_1/T_0, \dots, T_n/T_0) \in \mathbf{k}[T_0, \dots, T_n]$$

is homogeneous of degree $d$, and for all $a \in \mathbb{A}^n$,

$$a \text{ is a zero of } F \iff h(a) \text{ is a zero of } G.$$

Conversely, if $G \in \mathbf{k}[T_0, \ldots, T_n]$ is homogeneous of degree $d$, then

$$F := G(1, T_1, \ldots, T_n) \in \mathbf{k}[T_1, \ldots, T_n]$$

is of total degree $\leq d$ and $G = T_0^d F(T_1/T_0, \ldots, T_n/T_0)$.

Note that $\mathbb{P}^n = U_0 \cup \cdots \cup U_n$. In order to make $\mathbb{P}^n$ into a prevariety we now equip each $U_i$ with the induced topology and the sheaf $\mathcal{O}_i$ of $\mathbf{k}$-valued functions such that we have an isomorphism $h_i : \mathbb{A}^n \cong (U_i, \mathcal{O}_i)$. Let us check that the conditions of the glueing lemma are satisfied. This is trivial for $n = 0$ (in which case $U_0 = \mathbb{P}^0$ is just a point), so let $n > 0$. Then $\mathcal{O}_0 | U_0 \cap U_1 = \mathcal{O}_1 | U_0 \cap U_1$ because

$$h_0^{-1}(U_0 \cap U_1) = h_1^{-1}(U_0 \cap U_1) = \{(x_1, \ldots, x_n) \in \mathbf{k}^n : x_1 \neq 0\}$$

is a basic open set in $\mathbb{A}^n$, and the transition maps

$$h_1^{-1} \circ h_0 : h_0^{-1}(U_0 \cap U_1) \to h_1^{-1}(U_0 \cap U_1),$$
$$h_0^{-1} \circ h_1 : h_1^{-1}(U_0 \cap U_1) \to h_0^{-1}(U_0 \cap U_1)$$

are both given by $(x_1, \ldots, x_n) \mapsto (\frac{1}{x_1}, \frac{x_2}{x_1}, \ldots, \frac{x_n}{x_1})$, and are thus isomorphisms of prevarieties. Of course, all this works in the same way with $h_i$ and $h_j$ instead of $h_0$ and $h_1$. Thus the conditions of the glueing lemma 6.1 are satisfied. We equip $\mathbb{P}^n$ with the unique sheaf $\mathcal{O}$ of $\mathbf{k}$-valued functions on $\mathbb{P}^n$ such that $\mathcal{O} | U_i = \mathcal{O}_i$ for $i = 0, \ldots, n$; this makes $\mathbb{P}^n$ a prevariety. It has the $U_i$ as affine open parts, and each $U_i$ is an isomorphic copy of $\mathbb{A}^n$ via $h_i$.

What we defined to be $\mathbb{P}^n$ is more properly denoted by $\mathbb{P}^n(\mathbf{k})$, but as long as $\mathbf{k}$ is fixed, this abuse of notation is harmless.

**Exercise**. With the notations above, we have

(1) $\mathbb{P}^n$ is irreducible of dimension $n$;

(2) if $n > 0$, then we have an isomorphism

$$[0 : a_1 : \cdots : a_n] \mapsto [a_1 : \cdots : a_n] \ : \ \mathbb{P}^n \setminus U_0 \ \to \ \mathbb{P}^{n-1};$$

(3) a set $X \subseteq \mathbb{A}^m \times \mathbb{P}^n$ is closed in the prevariety $\mathbb{A}^m \times \mathbb{P}^n$ iff there are polynomials $f_1, \ldots, f_N \in \mathbf{k}[T_1, \ldots, T_m, U_0, \ldots, U_n]$, homogeneous in $(U_0, \ldots, U_n)$, such that for all $a \in \mathbb{A}^m$ and all $b \in \mathbb{A}^{n+1}$ with $b \neq 0$ and $p = [b_0 : \cdots : b_n] \in \mathbb{P}^n$,

$$(a, p) \in X \iff f_1(a, b) = \cdots = f_N(a, b) = 0.$$

**Tangent spaces and smoothness.** Let $X$ be a prevariety. Since $X$ is in particular a geometric $\mathbf{k}$-space, we have for $a \in X$ the tangent space $\mathrm{T}_a X$, a $\mathbf{k}$-vector space of *finite* dimension, since $\mathrm{T}_a X = \mathrm{T}_a U$ where $U$ is an affine open part of $X$ with $a \in U$. We are going to show that if $X$ is irreducible of dimension $d$, then $\dim \mathrm{T}_a X = d$ for all $a \in X$ outside some proper closed subset $\mathrm{Sing}(X)$ of $X$. The key fact is as follows.

**Lemma 6.5.** *Suppose the algebraic set $X \subseteq \mathbf{k}^m$ is irreducible of dimension $d$. Then some nonempty affine open part of $X$ is isomorphic to a nonempty affine open part of an irreducible hypersurface $H$ in $\mathbf{k}^{d+1}$.*

*Proof.* The coordinate ring $\mathbf{k}[X] = \mathbf{k}[t_1, \dots, t_m]$ is a domain and its fraction field $\mathbf{k}(t_1, \dots, t_m)$ has transcendence degree $d$ over $\mathbf{k}$. Then by standard facts in Lang's *Algebra* (X, 6.8, and VII, 6.1 and their proofs),

$$\mathbf{k}(t_1, \dots, t_m) = \mathbf{k}(y_1, \dots, y_d, y_{d+1}), \qquad y_1, \dots, y_{d+1} \in \mathbf{k}[t_1, \dots, t_m]$$

where $y_1, \dots, y_d$ is a transcendence basis of $\mathbf{k}(t_1, \dots, t_m)$ over $\mathbf{k}$ and $y_{d+1}$ is separably algebraic over $\mathbf{k}(y_1, \dots, y_d)$. Take an irreducible polynomial $F \in \mathbf{k}[Y_1, \dots, Y_{d+1}]$ such that $F(y_1, \dots, y_{d+1}) = 0$; this gives the irreducible hypersurface $H = \mathrm{Z}(F)$ in $\mathbf{k}^{d+1}$. For $i = 1, \dots, d+1$, take a polynomial $f_i \in \mathbf{k}[T_1, \dots, T_m]$ such that $y_i = f_i(t_1, \dots, t_m)$. This gives a regular map

$$\phi : X \to H, \quad \phi(a) = (f_1(a), \dots, f_{d+1}(a)).$$

Next, take polynomials $g_1, \dots, g_m, g \in \mathbf{k}[Y_1, \dots, Y_{d+1}]$ such that

$$g(y_1, \dots, y_{d+1}) \neq 0, \quad t_j = g_j(y_1, \dots, y_{d+1})/g(y_1, \dots, y_{d+1}) \quad (j = 1, \dots, m).$$

Then $V := \{b \in H : g(b) \neq 0\}$ is nonempty open in $H$, and we have a morphism

$$\psi : V \to X, \quad \psi(b) = \left(\frac{g_1(b)}{g(b)}, \dots, \frac{g_m(b)}{g(b)}\right).$$

It is easy to check that $\phi \circ \psi = \mathrm{id}_V$. Put $U := \phi^{-1}(V)$, so $U$ is open in $X$ and $\psi(V) \subseteq U$. Next one checks that $\psi \circ (\phi|U) = \mathrm{id}_U$, so $U \cong V$. Since $V$ is affine, so is $U$. $\square$

In the next proof we use the "local character of closedness": if $(U_i)$ is a covering of a space $X$ by open sets in $X$ and $Y \subseteq X$, then $Y$ is closed in $X$ iff $Y \cap U_i$ is closed in $U_i$ for each $i$.

**Corollary 6.6.** *Suppose the prevariety $X$ is irreducible and $\dim X = d$. Then there is a proper closed subset $\mathrm{Sing}(X)$ of $X$ such that $\dim \mathrm{T}_a X = d$ for all $a \in X \setminus \mathrm{Sing}(X)$, and $\dim \mathrm{T}_a X > d$ for all $a \in \mathrm{Sing}(X)$.*

*Proof.* If $X$ is affine, this follows from the lemma above and the description of tangent spaces of hypersurfaces in the previous section.

In general, take nonempty affine open parts $U_1, \dots, U_n$ of $X$ that cover $X$. Then $U_i$ is irreducible and $\dim U_i = d$ for all $i$, and $\mathrm{Sing}(U_i) \cap U_j = U_i \cap \mathrm{Sing}(U_j)$ for all $i, j$. from which it follows that

$$\mathrm{Sing}(X) := \mathrm{Sing}(U_1) \cup \dots \cup \mathrm{Sing}(U_n)$$

is closed in $X$. $\square$

Let $X$ be an irreducible prevariety. The set $\mathrm{Sing}(X)$ defined in Corollary 6.6 is called the *singular locus of* $X$, and its points are called *singular points of* $X$; the nonsingular points of $X$ are also called *simple points of* $X$, and if $a$ is a simple point of $X$, we also say that $X$ is *smooth at* $a$. Thus in some sense $X$ is smooth at almost all its points. We say that $X$ is *smooth* if $\mathrm{Sing}(X) = \emptyset$.

**Tangent bundles.** Let $X$ be a prevariety. Since $X$ is a geometric $\mathbf{k}$-space, $\mathrm{T}\,X$ is defined as a set. We make $\mathrm{T}\,X$ into a prevariety as follows.

First consider the case that $X$ is affine. Take an affine model $X'$ with an isomorphism $\phi : X' \to X$. Then $\phi$ induces a bijection $\mathrm{T}\,\phi : \mathrm{T}\,X' \to \mathrm{T}\,X$. Now $\mathrm{T}\,X'$ as defined in section 5 is naturally an affine model, and we now equip $\mathrm{T}\,X$ with the topology on $\mathrm{T}\,X$ and sheaf of $\mathbf{k}$-valued functions on $\mathrm{T}\,X$ that makes $\mathrm{T}\,\phi$ into an isomorphism of $\mathbf{k}$-spaces. (This topology and sheaf is independent of the choice of $X'$ and $\phi$.)

Next consider the general case, and take a covering $(U_i)_{i\in I}$ of $X$ by affine open parts, with finite $I$, so, as sets,

$$\mathrm{T}\,X = \bigcup_i \mathrm{T}\,U_i, \quad \mathrm{T}\,U_i \cap \mathrm{T}\,U_j = \mathrm{T}(U_i \cap U_j).$$

Each $\mathrm{T}\,U_i$ has been made into a prevariety, and it is easy to check that the conditions of the glueing lemma 6.1 are satisfied with $\mathrm{T}\,X$ and the $\mathrm{T}\,U_i$ in place of $X$ and the $U_i$. We now give $\mathrm{T}\,X$ the topology that makes each $\mathrm{T}\,U_i$ into an open subset and induces on $\mathrm{T}\,U_i$ its given topology. We also equip $\mathrm{T}\,X$ with the sheaf of $\mathbf{k}$-valued functions on $\mathrm{T}\,X$ whose restriction to each $\mathrm{T}\,U_i$ is the structure sheaf of the prevariety $\mathrm{T}\,U_i$. This makes $\mathrm{T}\,X$ into a prevariety. If $\phi : X \to Y$ is a morphism of $X$ into a prevariety $Y$, then $\mathrm{T}\,\phi : \mathrm{T}\,X \to \mathrm{T}\,Y$ is a morphism of prevarieties.

**Varieties.** A *variety* is a prevariety $X$ whose diagonal

$$\Delta(X) := \{(x, y) \in X \times X : \ x = y\}$$

is closed in the prevariety $X \times X$. This condition is a substitute for being hausdorff. Any affine space $\mathbb{A}^m$ is a variety. Any open subset and any closed subset of a variety is a variety. The set-like product $X \times Y$ of varieties $X, Y$ is a variety. By a *curve* we shall mean a variety of dimension 1.

Let $X$ be a variety. If $Y$ is a locally closed subset of $X$, then $Y$ with the induced topology and sheaf $\mathcal{O}_X|Y$ is itself a variety, and unless specified otherwise we consider $Y$ as a variety in this way, and this makes the inclusion map $Y \hookrightarrow X$ into a morphism. A *subvariety* of $X$ is a locally closed subset of $X$ viewed as a variety in this way.

We leave it to the reader to show that each projective space $\mathbb{P}^n$ is a variety. A variety is said to be *projective* if it is isomorphic to a closed subvariety of some projective space $\mathbb{P}^n$.

**Exercise.** Let $X$ be a prevariety and $Y$ a variety. Then

(i) If $f, g : X \to Y$ are morphisms, then $\{x \in X : \ f(x) = g(x)\}$ is closed in $X$.

(ii) If $f : X \to Y$ is a morphism, then its graph

$$\Gamma(f) := \{(x, y) \in X \times Y : \ f(x) = y\}$$

is closed in $X \times Y$, and $x \mapsto (x, f(x)) : X \to \Gamma(f)$ is an isomorphism.

**Complete varieties.** A *complete variety* is a variety $X$ such that for each $m$ the projection map $\mathbb{A}^m \times X \to \mathbb{A}^m$ maps each closed subset of $\mathbb{A}^m \times X$ onto a closed subset of $\mathbb{A}^m$. The variety $\mathbb{A}^1$ is not complete: the image

$$\{(x, y) \in \mathbb{A}^2 : xy = 1\} \qquad \text{s closed subset of } \mathbb{A}^2$$

under the projection map $(x, y) \mapsto x : \mathbb{A}^2 \to \mathbb{A}^1$ is $\{x \in \mathbb{A}^1 : x \neq 0\}$, which is not closed in $\mathbb{A}^1$. Completeness is a substitute for compactness: while varieties are compact as a topological space, this is not so useful in the absence of being hausdorff. It is a key fact that projective spaces $\mathbb{P}^n$ are complete. (There is a short proof of this, using the exercise above characterizing closed subsets of $\mathbb{A}^m \times \mathbb{P}^n$, and some model theory; this will be handed out.) It follows from item (2) in the next lemma that every projective variety is complete.

In the next lemma $X$ and $Y$ are varieties.

**Lemma 6.7.** *Suppose $X$ is complete variety. Then*

(1) *the projection map $X \times Y \to Y$ maps each closed subset of $X \times Y$ onto a closed subset of $Y$;*
(2) *each closed subvariety of $X$ is complete;*
(3) *if $Y$ is complete, so is $X \times Y$;*
(4) *if $\phi : X \to Y$ is a morphism, then $\phi(X)$ is closed in $Y$ and complete;*
(5) *if $X$ is a subvariety of $Y$, then $X$ is closed in $Y$;*
(6) *if $X$ is irreducible, then $\mathcal{O}_X(X) = \mathbf{k}$ and every morphism of $X$ into an affine variety is constant.*

*Proof.* Item (1) holds for $Y = \mathbb{A}^n$, and thus for any affine variety $Y$. The general case can be reduced to this case by taking affine open parts $Y_1, \ldots, Y_m$ of $Y$ that cover $Y$. Items (2) and (3) are easy consequences of the definition and (1). As to (4), let $\phi : X \to Y$ be a morphism. Then $\phi(X)$ is the image of the closed subset $\Gamma(f)$ of $X \times Y$ under the projection map $X \times Y \to Y$, so $f(X)$ is closed in $Y$. To get completeness of $f(X)$, suppose $Z \subseteq f(X) \times \mathbb{A}^n$ is closed. Then the inverse image $Z'$ of $Z$ under the morphism

$$(f, \mathrm{id}_{\mathbb{A}^n}) : X \times \mathbb{A}^n \to f(X) \times \mathbb{A}^n$$

is closed in $X \times \mathbb{A}^n$, and the image of $Z$ under the projection map

$$f(X) \times \mathbb{A}^n \to \mathbb{A}^n$$

equals the image of $Z'$ under the projection map $X \times \mathbb{A}^n \to \mathbb{A}^n$, and this image is therefore closed in $\mathbb{A}^n$. Item (5) follows from (4) by considering the inclusion morphism $X \hookrightarrow Y$. As to (6), let $X$ be irreducible and $f \in \mathcal{O}_X(X)$. Then $f(X) \subseteq \mathbb{A}^1$ is closed by (5), and irreducible, so either $f(X)$ has just one point, or $f(X) = \mathbb{A}^1$. But $f(X)$ is also complete by (5), and $\mathbb{A}^1$ is not complete, so $f$ must be constant. It follows that any morphism from $X$ into an affine variety is constant. $\square$

**Lemma 6.8.** *Let $X, Y$ be irreducible varieties with $X$ complete, and suppose $\phi : X \times Y \to Z$ is a morphism into a variety $Z$ such that $\phi(-, b) : X \to Z$*

*is constant for some $b \in Y$. Then $\phi(-,y) : X \to Z$ is constant for every $y \in Y$.*

*Proof.* Take $b \in Y$ and $c \in Z$ such that $\phi(x,b) = c$ for all $x \in X$. Take an affine open neighborhood $U$ of $c$ in $Z$. Then

$$P := \{(x,y) \in X \times Y : \ \phi(x,y) \notin U\}$$

is closed in $X \times Y$, so its image $Q$ under the projection map $X \times Y \to Y$ is closed in $Y$. We have $b \in Y \setminus Q$, and if $y \in Y \setminus Q$, then the morphism $\phi(-,y) : X \to Z$ takes its values in the affine variety $U$, so $\phi(-,y)$ is constant by (6) of Lemma 6.7. Let $x, x' \in X$. Then $\{y \in Y : \ \phi(x,y) = \phi(x',y\}$ is closed in $Y$ and contains the nonempty open subset $Y \setminus Q$ of $Y$, and thus equals $Y$. □

**Algebraic groups.** An *algebraic group* is a prevariety $G$ equipped with a distinguished element 1, and morphisms $\iota : G \to G$ and $\mu : G \times G \to G$ such that $(G; 1, \iota, \mu)$ is a group; in practice we shall write $x^{-1}$ and $xy$ instead of $\iota(x)$ and $\mu(x,y)$ for $x, y \in G$. Note that then $G$ is actually a variety, since $\Delta(G)$ is the inverse image of the closed set $\{1\} \subseteq G$ under the morphism

$$(x,y) \mapsto \mu(x, \iota(y)) : G \times G \to G.$$

Let $G$ and $H$ be algebraic groups. An *algebraic group morphism $G \to H$* is a morphism $G \to H$ of varieties that is also a group morphism. We consider the set-like product $G \times H$ as an algebraic group in the obvious way by taking the product group as the underlying group.

**Lemma 6.9.** *Suppose $G$ is an algebraic group. Then*

(1) *for each $g \in G$ the maps*

$$x \mapsto gx : G \to G, \quad x \mapsto xg : G \to G, \quad x \mapsto gxg^{-1} : G \to G$$

*are isomorphisms of varieties;*

(2) *if $G$ is irreducible, then $G$ is a smooth variety;*

(3) *each closed subgroup of $G$ is an algebraic group;*

(4) *if $G'$ is any subgroup of $G$, then its closure in $G$ is also a subgroup;*

(5) *if $G'$ is a subgroup of $G$ and a constructible set in $G$, then $G'$ is a closed subgroup of $G$.*

*Proof.* Items (1) and (3) are clear from earlier results, and (2) follows from (1) and the fact that if $G$ is irreducible, then $G$ is smooth at some point of $G$ by Corollary 6.6. Item (4) is an easy exercise. As to (5), let $G'$ be a subgroup of $G$ and a constructible set in $G$. Let $H$ be the closure of $G'$ in $G$. Then $H$ is a closed subgroup of $G$ by (4), and $\dim(H \setminus G') < \dim H$ by results in the section on noetherian spaces. Suppose that $G' \neq H$, and take $h \in H$, $h \notin G'$. Then $hG' \subseteq H \setminus G'$, but $\dim hG' = \dim G'$, and we have a contradiction. □

**Examples of algebraic groups.** To specify an algebraic group we usually indicate just the underlying variety and the group multiplication, since the latter determines the group inversion and group identity.

(1) $\mathbb{A}^1$ with the usual addition is an algebraic group, referred to as the *additive group* and denoted by $\mathbb{G}_{\mathrm{a}}$.
(2) the basic open subvariety $\mathbb{A}^1\setminus\{0\}$ of $\mathbb{A}^1$ with the usual multiplication is an algebraic group, referred to as the *multiplicative group* and denoted by $\mathbb{G}_{\mathrm{m}}$.
(3) View an $n \times n$-matrix over $\mathbf{k}$ as an element of $\mathbf{k}^{n^2}$ in the usual way. Then the basic open subvariety $\mathrm{GL}_n(\mathbf{k})$ of $\mathbb{A}^{n^2}$ with the usual matrix multiplication is an algebraic group, the *general linear group* $\mathbb{GL}_n$. For $n = 1$ this is just $\mathbb{G}_{\mathrm{m}}$.
(4) The closed subgroup $\mathrm{SL}_n(\mathbf{k}) := \{A \in \mathbb{GL}_n : \det(A) = 1\}$ of $\mathbb{GL}_n$ is an algebraic group, the *special linear group* $\mathbb{SL}_n$.

These algebraic groups are all affine as varieties.

**Proposition 6.10.** *Let $G$ be an algebraic group. Then*

(1) *$G$ has a unique irreducible component $G^0$ that contains $1$;*
(2) *$G^0$ is a closed normal subgroup of $G$ of finite index in $G$;*
(3) *$G^0$ is the connected component of $1$ in $G$;*
(4) *any closed subgroup of $G$ of finite index in $G$ contains $G^0$.*

*Proof.* Let $X$ and $Y$ be irreducible components of $G$ containing 1. Then the set $XY \subseteq G$ is the image of $X \times Y$ under a morphism $G \times G \to G$, so $XY$ is irreducible, hence $\mathrm{cl}(XY)$ is irreducible. But $X \subseteq \mathrm{cl}(XY)$ and $Y \subseteq \mathrm{cl}(XY)$, so $X = Y = \mathrm{cl}(XY)$. Thus $XX = X$; it is also clear that $X = X^{-1}$. So $X$ is a closed subgroup $G^0$ of $G$. By (1) of Lemma 6.9 we see in the same way that $gG^0g^{-1} = G^0$ for each $g \in G$, so $G^0$ is a normal subgroup. It also follows that the cosets $gG^0$ of $G^0$ in $G$ are exactly the irreducible components of $G$, so there can only be finitely many cosets of $G^0$ in $G$, that is, $G^0$ has finite index in $G$. Since $G^0$ is irreducible, it is connected. The complement of $G^0$ is a finite union of cosets $gG^0$, so is closed in $G$, and thus $G^0$ is open in $G$. It follows that $G^0$ is the connected component of 1. This argument also shows that any closed subgroup of $G$ of finite index in $G$ is open as well as closed in $G$, and thus must contain the connected component $G^0$ of 1. $\square$

It follows that for algebraic groups, *connected* is the same as *irreducible*; the preferred terminology is *connected algebraic group.* Note that the connected components of an algebraic group $G$ are the cosets $gG^0$ of $G^0$, and that these are also its irreducible components.

An algebraic group is said to be *linear* if it is isomorphic as algebraic group to a closed subgroup of $\mathbb{GL}_n$ for some $n$. Closed subgroups of linear algebraic groups are clearly linear algebraic groups, and it is also easy to see that if $G$ and $H$ are linear algebraic groups, then $G \times H$ is a linear algebraic group. Linear algebraic groups are clearly affine varieties. We shall not use this fact, but the converse is also true: affine algebraic groups are linear.

An *algebraic torus* is an algebraic group isomorphic as algebraic group to a power $\mathbb{G}_{\mathrm{m}}^n$ of the multiplicative group. In particular, an algebraic torus is a linear algebraic group, since $\mathbb{G}_{\mathrm{m}}^n$ is isomorphic as algebraic group to the closed subgroup of $\mathbb{GL}_n$ consisting of the diagonal $n \times n$-matrices over $\mathbf{k}$ with nonzero determinant.

Let $T$ be an algebraic torus of dimension $d$; so $T$ is isomorphic as algebraic group to $\mathbb{G}_{\mathrm{m}}^d$. In particular, $T$ is commutative and connected. If in addition $\mathbf{k}$ has characteristic 0, then for each $n > 0$ the $n$-torsion subgroup

$$T[n] := \{g \in T : g^n = 1\}$$

of $T$ is isomorphic as a group to $(\mathbb{Z}/n\mathbb{Z})^d$.

An *abelian variety* is by definition a complete connected algebraic group. If $A$ is an abelian variety, so is every closed connected subgroup. Note that if $A$ and $B$ are abelian varieties, so is $A \times B$.

Abelian varieties are amazing objects and very different from linear algebraic groups, although there are resemblances to algebraic tori.

**Lemma 6.11.** *Let $A$ be an abelian variety. Then $A$ is commutative, and every morphism $A \to G$ of varieties into an algebraic group $G$ sending $1_A$ to $1_G$ is an algebraic group morphism.*

*Proof.* Apply Lemma 6.8 with $X = Y = Z = A$, $\phi(x,y) = xyx^{-1}$, and $b = 1$, to get commutativity. The second statement is proved likewise with $X = Y = A$ and $Z = G$ and a suitable map that the reader can guess. $\square$

**Corollary 6.12.** *If the abelian varieties $A$ and $B$ are isomorphic as varieties, then they are isomorphic as algebraic groups. If $X$ is a variety and $e \in X$, then there is at most one group operation $X \times X \to X$ that makes $X$ into an abelian variety with identity element $e$.*

Abelian varieties of dimension 1 are called *elliptic curves* for complicated historical reasons. It is traditional to use additive notation when dealing with abelian varieties, and we shall do so in what follows.

**Examples of elliptic curves.** Assume that characteristic($\mathbf{k}$) $\neq 2, 3$ and consider a polynomial $T^3 + aT + b$ ($a, b \in \mathbf{k}$) with three distinct zeros in $\mathbf{k}$. Then we have the irreducible algebraic set $C \subseteq \mathbb{A}^2$ defined by the equation $y^2 = x^3 + ax + b$, that is, its points are the $(x,y) \in \mathbb{A}^2$ satisfying this equation. Identifying $\mathbb{A}^2$ with the affine open part $U_2$ of the projective plane $\mathbb{P}^2$ via $(x,y) \mapsto [x : y : 1]$, the closure $E := \mathrm{cl}(C)$ of $C$ in $\mathbb{P}^2$ is defined by the homogeneous equation

$$y^2 z = x^3 + axz^2 + bz^3,$$

that is, its points are the $[x : y : z] \in \mathbb{P}^2$ satisfying this equation. Setting $z = 0$ in this equation we see that $E$ has just one point not in $C$, namely the point $O = [0 : 1 : 0]$. It is easy to check that $E$ is a smooth projective irreducible curve. It is a remarkable fact, but less easy to prove, that there is a unique group operation $+ : E \times E \to E$ that makes $E$ into an abelian variety with zero element $O$; this addition operation can be visualized as follows: if $L$ is a line in $\mathbb{A}^2$ that intersects $C$ in three distinct points $P, Q, R$, then $P + Q + R = O$; for any point $P = (x, y) \in C$ we have $-P = (x, -y)$. Thus by our definition of an elliptic curve, $E$ with this addition operation is an elliptic curve.

A *semiabelian variety* is a commutative algebraic group $G$ for which there exist an algebraic torus $T$ and an abelian variety $A$ with an exact sequence

$$1 \to T \to G \to A \to 0$$

of algebraic group morphisms. In particular, algebraic tori and abelian varieties are semiabelian varieties.

**Constructible sets and groups.** For model theorists it is natural to work in the category of constructible sets rather than that of varieties, because constructible sets in varieties are basically the same as the definable relations on $\mathbf{k}$. By EI, the quotient of a constructible set by a constructible equivalence relation is again a constructible set in a natural way, but in general the quotient of a variety by a closed equivalence relation is not a variety in a natural way. Fortunately, in characteristic zero, constructible groups are equivalent to algebraic groups as explained below, and forming quotients of algebraic groups by closed normal subgroups can be reduced to forming quotients of constructible groups by constructible normal subgroups. Below we fill in the above sketch.

In this subsection $X, Y, Z$ are varieties. By a constructible set we mean here a pair $(C, X)$ where $C$ is a constructible set in $X$, referring to it as "the constructible set $C \subseteq X$" or "the constructible set $C$ in $X$" and indicating it just by $C$ if we don't wish to mention its ambient variety $X$. Given constructible sets $C \subseteq X$ and $D \subseteq Y$, a *constructible map* $C \to D$ is a map $f : C \to D$ whose graph is a constructible subset of $X \times Y$. Note that if $f : C \to D$ is a constructible bijection, then $f^{-1} : D \to C$ is constructible. A variety $X$ is viewed as a constructible set in itself. Note that a morphism $X \to Y$ is constructible. The next two lemmas are easy consequences of the definitions and QE. The way QE comes in is via its obvious consequence that if $X$ and $Y$ are affine and $C \subseteq X \times Y$ is constructible, then the image of $C$ under the projection map $X \times Y \to Y$ is constructible in $Y$.

**Lemma 6.13.** *Let $C \subseteq X$, $D \subseteq Y$, $E \subseteq Z$ be constructible sets. Then*

1. *if $f : C \to D$ is constructible, then $f(C) \subseteq Y$ is constructible;*
2. *$C \times D \subseteq X \times Y$ is constructible, and whenever $f : E \to C$ and $g : E \to D$ are constructible, so is $(f, g) : E \to C \times D$;*
3. *if $f : C \to D$ is constructible and $D' \subseteq D$ is constructible in $Y$, then $f^{-1}(D') \subseteq X$ is constructible;*
4. *if the relation $R \subseteq C \times D$ is constructible in $X \times Y$, then*

$$R(C) := \{y \in D : (c, y) \in R \text{ for some } c \in C\}$$

*is constructible in* $Y$*;*

(5) *if* $f : C \to D$ *and* $g : D \to E$ *are constructible, so is* $g \circ f : C \to E$.

*Proof.* The main fact here is (1); we leave the rest to the reader. Let $f$ be as in (1); so its graph $\Gamma(f) \subseteq X \times Y$ is constructible. Let $\pi : X \times Y \to Y$ be the projection map, so $f(C) = \pi(\Gamma(f))$. Let $U$ be an affine open part of $X$ and $V$ an affine open part of $Y$, and put

$$C_{U,V} := \Gamma(f) \cap (U \times V),$$

a constructible subset of $U \times V$. By the observation preceding the lemma the set $\pi(C_{U,V})$ is constructible in $Y$. Covering $X$ and $Y$ by finitely many affine open parts, we obtain in this way $f(C)$ as a finite union of constructible sets $\pi(C_{U,V})$ in $Y$, so $f(C)$ is constructible in $Y$. □

**Lemma 6.14.** *There is a constructible bijection* $b : X \to b(X)$ *between* $X$ *and a constructible set* $b(X) \subseteq \mathbf{k}^n$*, for some* $n$*.*

*Proof.* Let $U_1, \ldots, U_m$ be a covering of $X$ by affine open parts. Take $n$, disjoint algebraic sets $V_1, \ldots, V_m \subseteq \mathbf{k}^n$, and isomorphisms

$$h_1 : \ U_1 \to V_1, \ldots, h_m : \ U_m \to V_m.$$

Put $Y_i = h_i\big(U_i \setminus (U_1 \cup \cdots \cup U_{i-1})\big)$ for $i = 1, \ldots, m$. Then $Y := Y_1 \cup \cdots \cup Y_m$ is a constructible set in $\mathbf{k}^n$. Let $b : X \to Y$ be the constructible bijection that agrees with $h_i$ on $U_i \setminus (U_1 \cup \cdots \cup U_{i-1})$ for $i = 1, \ldots, m$. □

By these two lemmas there is no significant difference between constructible sets and definable relations on $\mathbf{k}$. Thus by EI,

**Lemma 6.15.** *Let* $E$ *be a constructible equivalence relation on a constructible set* $C \subseteq X$*, that is,* $E$ *is an equivalence relation on* $C$ *and is constructible in* $X \times X$*. Then there is a constructible set* $D$ *and a surjective constructible map* $f : C \to D$ *such that*

$$E(a,b) \iff f(a) = f(b), \qquad \text{for all } a, b \in C.$$

Let $C, E, f, D$ be as in this lemma, and suppose $g : C \to C'$ is a constructible map into a constructible set $C'$ such that $g(a) = g(b)$ for all $(a,b) \in E$. Then the unique map $h : D \to C'$ such that $h(f(a)) = g(a)$ for all $a \in C$ is constructible.

**Lemma 6.16.** *Suppose* $\mathbf{k}$ *has characteristic* $0$*.*

(1) *If* $\phi : X \to Y$ *is constructible, then there is a nonempty open subset* $U$ *of* $X$ *such that* $\phi|U : \ U \to Y$ *is a morphism;*

(2) *Let* $G$ *and* $H$ *be algebraic groups and* $\phi : \ G \to H$ *a constructible group morphism. Then* $\phi$ *is an algebraic group morphism.*

*Proof.* For (1) we can assume that $X$ is irreducible. Take affine open parts $V_1, \ldots, V_n$ of $Y$ that cover $Y$. Then the constructible sets

$$\phi^{-1}(V_1), \ldots, \phi^{-1}(V_n) \subseteq X$$

cover $X$, so some $\phi^{-1}(V_i)$ contains a nonempty open subset of $X$. Replacing $X$ by such a nonempty open subset and $Y$ by some $V_i$ we reduce to the case that $Y$ is affine. Shrinking $X$ further we can assume also that $X$ is affine. This gives a reduction to the case that $X$ is an irreducible closed set in $\mathbf{k}^m$ and $Y = \mathbf{k}^n$. It remains to use the characterization of definable functions in $\mathbf{k}$ as piecewise rational functions. Item (2) follows easily. □

A *constructible group* is a constructible set $G$ (in some $X$) together with a distinguished element 1, and constructible maps

$$\iota : G \to G \quad \text{and} \quad \mu : G \times G \to G$$

such that $(G; 1, \iota, \mu)$ is a group. Algebraic groups are constructible groups in the obvious way.

**Theorem 6.17.** *If $G$ is a constructible group, then there is a constructible group isomorphism $G \to G^{\mathrm{a}}$ onto an algebraic group $G^{\mathrm{a}}$.*

*Proof.* This follows from a result of A. Weil. A proof is given in *Weil's group chunk theorem: a topological setting.* □

The proof is a little easier when $\mathbf{k}$ has characteristic 0, and we shall only use the theorem for that case in the next section.

**Corollary 6.18.** *Suppose $\mathbf{k}$ has characteristic 0. Let $G$ be an algebraic group and $N$ a closed normal subgroup. Then there is a unique structure of variety on $G/N$ that makes the quotient group $G/N$ an algebraic group and the canonical map $G \to G/N$ a morphism of algebraic groups.*

Assume $\mathbf{k}$ has characteristic 0. With $G$ and $N$ as in the above corollary we shall consider $G/N$ as an algebraic group as specified there. In particular, if $A$ is an abelian variety and $B$ is a closed subgroup of $A$, then $A/B$ is again an abelian variety.

We finish this section with a result related to Weil's theorem. We shall need it in the proof of "Mordell-Lang for function fields of characteristic zero".

**Lemma 6.19.** *Let $G$ be a connected algebraic group, $S$ a constructible set in $G$, and $f : S \to H$ a constructible map into an algebraic group $H$, and $D$ a dense subgroup of $G$, such that $D \subseteq S$ and $f|D : D \to H$ is a group morphism $D \to H$. Then there is an algebraic group morphism $\phi : G \to H$ such that $\phi|D = f|D$.*

*Proof.* The constructible subset

$$\{(x, y) \in S \times S : \ xy \in S, \ f(xy) = f(x)f(y)\}$$

of $G \times G$ contains the dense subset $D \times D$ of $G \times G$, so it contains a nonempty open subset $O$ of $G \times G$. Since $S$ is dense in $G$ we can take a nonempty open set $X$ in $G$ such $X \subseteq S$ and $f|X : X \to H$ is a morphism of varieties and

$X$ is contained in the image of $O$ under both projection maps $G \times G \to G$. Replacing $X$ by $X \cap X^{-1}$ we can assume that $X = X^{-1}$. Put

$$U := \{(x, y) \in O \cap (X \times X) : \ xy \in X\},$$

a nonempty open subset of $G \times G$ such that for each $x \in X$ there are $y, z \in G$ with $(z, x) \in U$. It follows that $X$ with the multiplication of $G$ restricted to $U$ and the inversion of $G$ restricted to $X$ is a group chunk, with $G$ and the inclusion map $X \to G$ as a realization of this group chunk. Note that $f(xy) = f(x)f(y)$ for all $(x, y) \in U$, so by Lemma 7 in *Weil's group chunk theorem: a topological setting* there is a group morphism $\phi : G \to H$ such that $\phi|X = f|X$. We claim that $\phi|D = f|D$. Let $a \in D$ and note that $\{x \in X : ax^{-1} \in X\}$ is a nonempty open subset of $G$, which gives $b \in D \cap X$ with $ab^{-1} \in D \cap X$. Then $\phi(a) = \phi(ab^{-1})\phi(b) = f(ab^{-1})f(b) = f(a)$. Since $\phi|X : X \to H$ is a morphism (of varieties), $\phi$ is an algebraic group morphism. $\square$

**Further results on algebraic groups.** When we later deal with "Mordell-Lang for function fields of characteristic 0" we need some basic facts on algebraic groups that we state here without proof. In this subsection we assume that $\mathbf{k}$ has characteristic 0.

**Fact 1.** If $T$ is an algebraic torus and $N$ a closed subgroup of $T$, then $T/N$ is an algebraic torus.

From this we easily derive:

**Corollary 6.20.** *If $A$ is a semiabelian variety and $N$ a closed subgroup of $A$, then $A/N$ is a semiabelian variety.*

*Proof.* Let $A$ be a semiabelian variety, and take a closed subgroup $T$ of $A$ such that $T$ is a torus and $A/T$ is an abelian variety. let $N$ be a closed subgroup of $A$. Then $T/(N \cap T)$ is an algebraic torus and we have an obvious exact sequence

$$0 \longrightarrow T/(N \cap T) \longrightarrow A/N \longrightarrow A/(N + T) \longrightarrow 0$$

of algebraic group morphisms. Since $A/(N + T)$ is an abelian variety, $A/N$ is a semiabelian variety. $\square$

**Exercise.** The closed subgroups of $\mathbf{k}^m = \mathbb{G}_{\mathrm{a}}^m$ are exactly the $\mathbf{k}$-linear subspaces of $\mathbf{k}^m$. The algebraic group morphisms $\mathbb{G}_{\mathrm{a}}^m \to \mathbb{G}_{\mathrm{a}}^n$ are exactly the $\mathbf{k}$-linear maps $\mathbf{k}^m \to \mathbf{k}^n$.

By an *algebraic vector group* we mean an algebraic group that is isomorphic as algebraic group to $\mathbb{G}_{\mathrm{a}}^n$ for some $n$. If $G$ is an algebraic vector group, then $G$ is connected, and (using additive terminology for $G$) each nonzero $g \in G$ is contained in a closed subgroup of $G$ isomorphic as algebraic group to $\mathbb{G}_{\mathrm{a}}$.

**Lemma 6.21.** *Let $G$ be an algebraic vector group and $T$ an algebraic torus.*

(1) *There is no nontrivial algebraic group morphisms $G \to T$.*

(2) *There is no nontrivial algebraic group morphisms $T \to G$.*
(3) *There is no nontrivial algebraic group morphisms $G \to A$ with $A$ a semiabelian variety.*

*Proof.* For (1), use that there is no nontrivial algebraic group morphism $\mathbb{G}_{\mathrm{a}} \to \mathbb{G}_{\mathrm{m}}$. For (2), use that there is no nontrivial algebraic group morphism $\mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{a}}$. Let $\phi : G \to A$ be an algebraic group morphisms with $A$ a semiabelian variety. Let $T$ be a closed subgroup of $A$ such that $T$ is an algebraic torus and $A/T$ is an abelian variety. Composing $\phi$ with the canonical morphism $A \to A/T$ gives a morphism $G \to A/T$, whose image is closed subgroup of $A/T$. This image is a complete variety, but is also an algebraic vector group, so it is trivial. Hence $\phi(G) \subseteq T$, and thus $\phi$ is trivial by (1). □

**Fact 2.** If $G$ is a connected commutative linear algebraic group, then $G$ is isomorphic as algebraic group to $\mathbb{G}_{\mathrm{a}}^m \times \mathbb{G}_{\mathrm{m}}^n$ for some $m, n$.

**Fact 3.** If $G$ is a connected algebraic group, then there is a closed normal subgroup $N$ of $G$ such that $N$ is a connected linear algebraic group and $G/N$ is an abelian variety. (Chevalley's Theorem.)

**Corollary 6.22.** *Suppose $G$ is a connected commutative algebraic group. Then $G$ is a semiabelian variety iff $G$ has no nontrivial algebraic vector group as a closed subgroup.*

*Proof.* It follows from Lemma 6.21 that if $G$ is a semiabelian variety, then $G$ has no nontrivial algebraic vector group as a closed subgroup. For the converse, assume $G$ has no nontrivial algebraic vector group as a closed subgroup. Take $N$ as in Fact 3. Then $N$ is a connected commutative linear algebraic group, so $N$ is an algebraic torus by Fact 2 and the assumption on $G$. Hence $G$ is a semiabelian variety. □

Here is an immediate consequence:

**Corollary 6.23.** *If $A$ is a semiabelian variety and $B$ is a closed connected subgroup of $A$, then $B$ is also a semiabelian variety.*

**Fact 4.** If $A$ is a semiabelian variety, then for each $n > 0$ the $n$-torsion subgroup $A[n] := \{a \in A : na = 0\}$ is finite, and the torsion subgroup

$$\mathrm{t}(A) := \bigcup_{n>0} A[n]$$

is dense in $A$.

**Corollary 6.24.** *Suppose the semiabelian variety $A$ is defined over the algebraically closed subfield $K$ of $\mathbf{k}$. Then any connected closed subgroup of $A$ is defined over $K$.*

*Proof.* Let $B$ be a connected closed subgroup of $A$ defined over $K$. In particular, $B$ is a semiabelian variety by Corollary 6.24. Also,

$$\mathrm{t}(B) \subseteq \mathrm{t}(A) \subseteq A(K),$$

so each point in $\mathrm{t}(B)$ is fixed under the action of $\mathrm{Aut}(\mathbf{k}|K)$ on $A$. But $\mathrm{t}(B)$ is dense in $B$, so $B$ is invariant under this action, and thus $B$ is defined over $K$. □

## 7. Definable sets of finite Morley rank in differentially closed fields

As before, "differential field" means "differential field of characteristic 0" and $K$ will denote a differential field. We also let $\mathbf{k}$ be an *algebraically closed* differential field. Terminology and notation like "closed", "open", "irreducible", "dense", "dim", refers to the relevant Zariski topology, not to the $\partial$-topology.

For $a = (a_1, \ldots, a_m) \in K^m$ we set $\partial a := (\partial a_1, \ldots, \partial a_m) \in K^m$.

A simple device in the study of differential equations is to eliminate higher derivatives by introducing new variables. For example, an equation

$$f(x, x', x'') = 0$$

is equivalent to the system of equations

$$f(x, y, z) = 0, \ y = x', \ z = y',$$

in the sense that solutions to the original equation correspond bijectively to solutions of the new system. In general we hope to reduce *differential* equations as much as possible to *algebraic* equations. This hope can be realized to a large extent in the setting of differentially closed fields, for definable sets of finite Morley rank. The method we follow comes from a paper by Pillay and Ziegler, and also applies to difference equations.

**A criterion for extending derivations.** Let $a_1, \ldots, a_m, b_1, \ldots, b_m$ be elements in an extension field $E$ of $K$. When is there a derivation $d$ of $E$ that extends the derivation $\partial$ of $K$ such that $d(a_1) = b_1, \ldots, d(a_m) = b_m$? Lemma 4.2 yields the necessary condition that for all $f \in K[T_1, \ldots, T_m]$ with $f(a) = 0$ we have

$$f^{\partial}(a) + \sum_{i=1}^{m} \frac{\partial f}{\partial T_i}(a) \cdot b_i = 0.$$

It turns out that this condition is also sufficient.

**Proposition 7.1.** *Suppose for all $f \in K[T_1, \ldots, T_m]$ with $f(a) = 0$ we have*

$$f^{\partial}(a) + \sum_{i=1}^{m} \frac{\partial f}{\partial T_i}(a) \cdot b_i = 0.$$

*Then there is a derivation $d$ of $E$ that extends the derivation $\partial$ of $K$ such that $d(a_1) = b_1, \ldots, d(a_m) = b_m$.*

*Proof.* The assumption allows us to define a map $d : K[a] \to E$ by

$$d(f(a)) = f^{\partial}(a) + \sum_{i=1}^{m} \frac{\partial f}{\partial T_i}(a) \cdot b_i \quad (f \in K[T_1, \dots, T_m]).$$

Moreover, $d$ is easily seen to be a derivation of $K$ into $E$ extending $\partial$. The exercises concerning this extended notion of derivation early in Section 4 then show that $d$ can be extended to a derivation of $E$. $\square$

**Remarks.** For the conclusion of this proposition to hold it suffices that the identity in the proposition holds for all $f$ in a set of generators of the ideal $\{g \in K[T_1, \dots, T_m] : \ g(a) = 0\}$ of $K[T_1, \dots, T_m]$.

When $E = K(a_1, \dots, a_m)$, there is just one extension $d$ as in the proposition, and this case is covered by a theorem in Lang's *Algebra*. For our purpose, however, we prefer not to require $b_1, \dots, b_m \in K(a_1, \dots, a_m)$.

**Torsors and prolongations.** Fix distinct variables $T_1, \dots, T_m, V_1, \dots, V_m$. For $F \in \mathbf{k}[T_1, \dots, T_m]$ and $a \in \mathbf{k}^m$ we set

$$\tau_a(F)(V_1, \dots, V_m) := F^{\partial}(a) + \sum_{i=1}^{m} \frac{\partial F}{\partial T_i}(a) V_i \in \mathbf{k}[V_1, \dots, V_m], \quad \text{so}$$

$$\tau_a F = F^{\partial}(a) + d_a F \in \mathbf{k} + \mathbf{k}V_1 + \dots + \mathbf{k}V_m, \quad F(a)' = (\tau_a F)(\partial a).$$

For $F, G \in \mathbf{k}[T_1, \dots, T_m]$ and $a \in \mathbf{k}^m$ we have

$$\tau_a(F + G) = \tau_a(F) + \tau_a(G), \quad \tau_a(FG) = F(a) \cdot \tau_a(G) + G(a) \cdot \tau_a(F).$$

We also have the following chain rule.

**Lemma 7.2.** *Let $F_1, \dots, F_n \in \mathbf{k}[T_1, \dots, T_m]$ and $G \in \mathbf{k}[U_1, \dots, U_n]$, and set $H := G(F_1, \dots, F_n) \in \mathbf{k}[T_1, \dots, T_m]$. Then we have for $a \in \mathbf{k}^m$ and $b := (F_1(a), \dots, F_n(a)) \in \mathbf{k}^n$,*

$$\tau_a(H) = \tau_b(G)\big(\tau_a(F_1), \dots, \tau_a(F_n)\big) \in \mathbf{k} + \mathbf{k}V_1 + \dots + \mathbf{k}V_m.$$

Let $X \subseteq \mathbf{k}^m$ be an algebraic set. Then we define, for $a \in X$,

$$\tau_a X := \{v \in \mathbf{k}^m : \ \tau_a(F)(v) = 0 \ \text{ for all } F \in \mathrm{I}(X)\},$$

the *torsor* of $X$ at $a$. If $\mathrm{I}(X) = (F_1, \dots, F_n)$, then in the definition above one can replace "for all $F \in \mathrm{I}(X)$" by "for $F = F_1, \dots, F_n$". The next lemma is now obvious.

**Lemma 7.3.** *Let $a \in X$. Then $\partial a \in \tau_a(X)$ and thus $\tau_a X = \partial a + \mathrm{T}_a X$.*

We bundle the spaces $\tau_a X$ as $a$ varies over $X$ into a single algebraic subset

$$\tau X := \{(x, v) \in \mathbf{k}^m \times \mathbf{k}^m : \ x \in X, \ \tau_x(F)(v) = 0 \ \text{ for all } F \in \mathrm{I}(X)\}$$

of $\mathbf{k}^{2m}$. We call $\tau X$ the *prolongation* of $X$, and consider it as a variety over $X$ via the regular map

$$\pi_X : \ \tau X \to X, \quad \pi_X(x, v) = x.$$

Let $f \in \mathbf{k}[X]$ and choose $F \in \mathbf{k}[T_1, \ldots, T_m]$ with $f = F|X$. For $a \in X$ the function

$$\tau_a F|\tau_a X : \tau_a X \to \mathbf{k}$$

does not depend on $F$, so we can define $\tau_a f := \tau_a F|\tau_a X$. Then

$$f(a)' \;=\; (\tau_a f)(\partial a) \qquad \text{for all } a \in X.$$

Suppose $Y \subseteq \mathbf{k}^n$ is a second algebraic set, $f = (f_1, \ldots, f_n) : X \to Y$ is a regular map, $a \in X$ and $b = f(a)$. The chain rule (Lemma 7.2) yields:

**Lemma 7.4.** *If $v \in \tau_a X$, then $(\tau_a f_1(v), \ldots, \tau_a f_n(v)) \in \tau_b Y$.*

We define $\tau_a f := (\tau_a f_1, \ldots, \tau_a f_n) : \tau_a X \to \tau_b Y$, an affine map between affine spaces over $\mathbf{k}$. Note that then

$$(\tau_a f)(\partial a) = \partial b.$$

We bundle the maps $\tau_a f$ as $a$ varies into a single regular map

$$\tau f : \; \tau X \to \tau Y, \qquad \tau f(x, v) := (f(x), \tau_x f(v)).$$

Suppose $Z \subseteq \mathbf{k}^p$ is a third algebraic set and $g = (g_1, \ldots, g_p) : Y \to Z$ is a regular map, and $c = g(b)$. Then the chain rule Lemma 7.2 yields

$$\tau_a(g \circ f) \;=\; \tau_b g \circ \tau_a f, \qquad \tau(g \circ f) = (\tau g) \circ (\tau f).$$

Note that if $m = n$ and $X \subseteq Y$, then $\tau_a X \subseteq \tau_a Y \subseteq \mathbf{k}^m$, and the inclusion map $\iota : X \hookrightarrow Y$ yields the inclusion maps

$$\tau_a \iota : \; \tau_a X \hookrightarrow \tau_a Y, \qquad \tau\iota : \; \tau X \hookrightarrow \tau Y.$$

**Lemma 7.5.** *Suppose $\mathbf{k}$ is differentially closed, $X \subseteq \mathbf{k}^m$ is an irreducible algebraic set, $U$ is a nonempty open set in $X$, and $Y$ is a closed irreducible subset of $\tau X$ such that $\pi_X(Y) \supseteq U$. Then there is $a \in U$ such that $(a, \partial a) \in Y$.*

*Proof.* Take a $|\mathbf{k}|^+$-saturated algebraically closed field extension $\Omega$ of $\mathbf{k}$ and take a point $x \in X(\Omega)$ such that $\operatorname{trdeg}_{\mathbf{k}} \mathbf{k}(x) = \dim X$, so for all $F \in \mathbf{k}[T_1, \ldots, T_m]$ we have

$$F(x) = 0 \iff F \in \mathrm{I}(X).$$

Hence $x \in U(\Omega)$, so we can take a point $(x, y) \in Y(\Omega)$. Then $\tau_x(F)(y) = 0$ for all $F \in \mathbf{k}[T_1, \ldots, T_m]$ with $F(x) = 0$. It follows that there is a derivation $d$ on $\Omega$ that extends $\partial$ such that $d(x) = y$. Since $\mathbf{k}$ is existentially closed as a differential field, there is $(a, b) \in Y$ such that $a \in U$ and $b = \partial(a)$. $\square$

**Algebraic $\partial$-sets.** These are algebraic sets with a section into their prolongation. To be precise, an *algebraic $\partial$-set in $\mathbf{k}^m$* is a pair $(X, s)$ where $X \subseteq \mathbf{k}^m$ is an algebraic set and $s : X \to \tau(X)$ is a regular map such that $\pi_X \circ s = \mathrm{id}_X$.

Let $(X, s)$ be an algebraic $\partial$-set in $\mathbf{k}^m$. Then we obtain a derivation $\partial_s$ on the coordinate ring $\mathbf{k}[X]$ as follows. A regular function $f \in \mathbf{k}[X]$ yields the regular map $\tau f : \tau X \to \tau\mathbf{k} = \mathbf{k}^2$, so we have a regular map

$$\tau f \circ s = (f, \partial_s f) : X \to \mathbf{k}^2, \qquad \partial_s(f) \in \mathbf{k}[X].$$

Explicitly, take $s_{m+1}, \ldots, s_{2m} \in \mathbf{k}[X]$ such that

$$s(x) = (x, s_{m+1}(x), \ldots, s_{2m}(x)) \qquad \text{for all } x \in X.$$

Then for $f \in \mathbf{k}[X]$ and $x \in X$,

$$(\partial_s f)(x) \ = \ (\tau_x f)(s_{m+1}(x), \ldots, s_{2m}(x)).$$

The map $\partial_s : \mathbf{k}[X] \to \mathbf{k}[X]$ is a derivation on $\mathbf{k}[X]$, and it extends the derivation $\partial$ on $\mathbf{k}$ if $X \neq \emptyset$. We let $\mathbf{k}[X, s]$ be the differential ring $(\mathbf{k}[X], \partial_s)$.

**Lemma 7.6.** *Let $a \in X$ be such that $s(a) = (a, \partial a)$. Then $\mathfrak{m}_{X,a}$ is a differential ideal of $\mathbf{k}[X]$, and so is every power $\mathfrak{m}_{X,a}^e$.*

*Proof.* Let $f \in \mathbf{k}[X]$. Then $f(a)' = (\tau_a f)(\partial a) = (\partial_s f)(a)$. ☐

Let $(X, s)$ and $(Y, t)$ be algebraic $\partial$-sets in $\mathbf{k}^m$ and $\mathbf{k}^n$. A *regular map* $(X, s) \to (Y, t)$ is a regular map $\phi : X \to Y$ such that

$$t \circ \phi \ = \ \tau\phi \circ s.$$

It is easy to check that then $\phi^* : \mathbf{k}[Y, t] \to \mathbf{k}[X, s]$ is a differential ring morphism.

The identity map on $X$ is a regular map $(X, s) \to (X, s)$. If $(Z, u)$ is a third algebraic $\partial$-set in $\mathbf{k}^p$ and $\phi : (X, s) \to (Y, t)$ and $\psi : (Y, t) \to (Z, u)$ are regular maps, so is $\psi \circ \phi : (X, s) \to (Z, u)$.

**Types of finite order.** In this subsection $\mathbb{U}$ is a big *differentially closed* field and $K$ and $\mathbf{k}$ are small differential subfields of $\mathbb{U}$ (with $\mathbf{k}$ algebraically closed). Given an algebraic $\partial$-set $(X, s)$ in $\mathbb{U}^m$ we put

$$(X, s)^\partial := \{x \in X : \ s(x) = (x, \partial x)\},$$

a definable subset of $\mathbb{U}^m$, and $(X, s)$ is said to be *defined over* $K$ if $X$ and $s$ are defined over $K$ in the *algebraically closed field* $\mathbb{U}$ (forgetting $\partial$). Also, "generic point" in this subsection is with respect to $\mathbb{U}$ as a big *algebraically closed field*.

**Lemma 7.7.** *Let $(X, s)$ be an algebraic $\partial$-set in $\mathbb{U}^m$. Suppose that $X$ is irreducible, and $(X, s)$ is defined over $K$. Then*

(1) *$(X, s)^\partial$ is dense in $X$;*
(2) *$(X, s)^\partial$ contains a generic point $a$ of $X$ over $K$;*
(3) *for $a$ as in* (2) *we have $K(a) = K\langle a\rangle$, and $\dim X = \operatorname{trdeg}_K K\langle a\rangle$;*
(4) *$\operatorname{tp}(a|K)$ (in $\mathbb{U}$) is independent of the choice of $a$ as in* (2).

*Proof.* Let $U$ be a nonempty open subset of $X$; for (1) we need to show that there is an $x \in U$ such that $s(x) = (x, \partial x)$. Let $Y$ be the closure in $\tau(X)$ of the constructible set $s(X) \subseteq \tau(X)$. Then $Y$ is a closed irreducible set in $\tau(X)$, and $\dim(Y \setminus s(X)) < \dim Y = \dim X$. Thus the constructible set $\pi(Y \setminus s(X)) \subseteq X$ has dimension $< \dim X$. Hence by shrinking $U$ we can arrange that $U$ is disjoint from $\pi(Y \setminus s(X))$. By the previous lemma we get $x \in U$ with $(x, \partial x) \in Y$, and then $(x, \partial x) \in s(X)$, that is $s(x) = (x, \partial x)$.

For (2), we note that by (1) we can take $a \in (X, s)^\partial$ outside all proper closed subsets of $X$ defined over $K$. Then $a$ is a generic point of $X$ over $K$. For (3) and (4), let $a, b \in (X, s)^\partial$ be generic points of $X$ over $K$. Then we have a field isomorphism $i : K(a) \to K(b)$ over $K$ that sends $a$ to $b$, and since $s(a) = (a, \partial a)$ and $s(b) = (b, \partial b)$, we have $K(a) = K\langle a \rangle$, $K(b) = K\langle b \rangle$, and $i$ a differential field isomorphism. In particular, $\mathrm{tp}(a|K) = \mathrm{tp}(b|K)$, and $\dim X = \mathrm{trdeg}_K K\langle a \rangle$. $\square$

For $a \in \mathbb{U}^m$ we say that $a$ has *finite order* over $K$ if $\mathrm{trdeg}_K K\langle a \rangle$ is finite, and then we define $\mathrm{ord}(a|K)$ to be this transcendence degree. Note that if $a \in \mathbb{U}^m$ and $b \in \mathbb{U}^n$ are interdefinable in $\mathbb{U}$ over $K$ and $a$ is of finite order over $K$, then $b$ is too, and $\mathrm{ord}(a|K) = \mathrm{ord}(b|K)$.

**Lemma 7.8.** *Suppose $a \in \mathbb{U}^m$ has finite order over $K$, and $K$ is algebraically closed. Then there is an algebraic $\partial$-set $(X, s)$ in some $\mathbb{U}^n$ such that*

(1) *$X$ is irreducible, and $(X, s)$ is defined over $K$;*
(2) *there is a generic point $b \in (X, s)^\partial$ of $X$ over $K$ such that $a$ and $b$ are interdefinable in $\mathbb{U}$ over $K$.*

*Proof.* Take $e$ such that $K\langle a \rangle$ is algebraic over $K(a, \partial a, \ldots, \partial^e a)$. Increasing $e$ by 1 we get $K\langle a \rangle = K(a, \partial a, \ldots, \partial^e a)$. Replacing $a$ by $(a, \partial a, \ldots, \partial^e a)$ and $m$ by $(e+1)m$ (and renaming) yields $K\langle a \rangle = K(a)$. Let $a = (a_1, \ldots, a_m)$, and take polynomials $f_1, \ldots, f_m, g \in K[T_1, \ldots, T_m]$ such that $g(a) \neq 0$ and $\partial a_i = f_i(a)/g(a)$. Put $b := (a_1, \ldots, a_m, 1/g(a)) \in \mathbb{U}^n$ where $n := m + 1$. Then $a$ and $b$ are interdefinable over $K$, and we have polynomials $s_1, \ldots, s_n \in K[T_1, \ldots, T_n]$ such that $\partial b_i = s_i(b)$ for $i = 1, \ldots, n$. Let

$$I := \{f \in K[T_1, \ldots, T_n] : \ f(b) = 0\},$$

a prime ideal of $K[T_1, \ldots, T_n]$, and put $X := \mathrm{Z}(I) \subseteq \mathbb{U}^n$, a $K$-irreducible $K$-algebraic set. Since $K$ is algebraically closed, $X$ is not just $K$-irreducible, but even irreducible, and $b$ is a generic point of $X$ over $K$. Define $s : X \to \mathbb{U}^{2n}$ by $s(x) = (x, s_1(x), \ldots, s_n(x))$. Then $s(b) = (b, \partial b) \in \tau(X)$, and thus $s(X) \subseteq \tau(X)$ since $\tau(X)$ is defined over $K$ and $b$ is a generic point of $X$ over $K$. Thus $s : X \to \tau(X)$ is a regular map with $\pi \circ s = \mathrm{id}_X$, and $(X, s)$ and $b$ have the desired properties. $\square$

Note that by part (3) of Lemma 7.7 we have $\dim X = \mathrm{ord}(b|K) = \mathrm{ord}(a|K)$ for $(X, s)$ and $b$ as in the above lemma.

**Corollary 7.9.** *Let $K$ be algebraically closed and $a \in \mathbb{U}^m$. Then*

(1) *$a$ has finite order over $K$ iff* $\mathrm{MR}(a|K)$ *is finite.*
(2) *if $a$ has finite order over $K$, then* $\mathrm{MR}(a|K) \le \mathrm{ord}(a|K)$.

*Proof.* Suppose $\mathrm{MR}(a|K) < \omega$. Then $\mathrm{MR}(a_i|K) < \omega$ for all $i$, so $a_i$ has finite order over $K$ for all $i$, by the results at the end of Section 4 on differential prime ideals of $K[Y]_{\mathrm{d}}$ where $Y$ is a single variable. Hence $a$ has finite order over $K$.

For the converse and for (2), assume $a$ has finite order over $K$. By Lemma 7.8 we reduce to the case that $a \in (X,s)^\partial$ with $(X,s)$ an algebraic $\partial$-set in $\mathbb{U}^m$ defined over $K$ such that $X$ is irreducible and $a$ is a generic point of $X$ over $K$. For $y \in (X,s)^\partial$, let $Y$ be the algebraic locus of $y$ over $K$, that is

$$Y := \{x \in \mathbb{U}^m : \ f(x) = 0 \text{ for all } f \in K[T_1,\dots,T_m] \text{ with } f(y) = 0\}.$$

Then $Y \subseteq X$, $y$ is a generic point of $Y$ over $K$, and $s(y) = (y, \partial y) \in \tau Y$, so $s(Y) \subseteq \tau Y$, and thus $(Y, s|Y)$ is an algebraic $\partial$-set defined over $K$ with $y \in (Y, s|Y)^\partial$, so $\dim Y = \mathrm{ord}(y|K) \le \mathrm{ord}(a|K)$. Thus we can assume inductively that for all $y \in (X,s)^\partial$,

$$\mathrm{ord}(y|K) < \mathrm{ord}(a|K) \implies \mathrm{MR}(y|K) \le \mathrm{ord}(y|K) < \mathrm{ord}(a|K) = \dim X.$$

But all $y \in (X,s)^\partial$ with $\mathrm{ord}(y|K) = \mathrm{ord}(a|K)$ realize the same type as $a$ in $\mathbb{U}$ over $K$, by (4) of lemma 7.7, so $\mathrm{MR}(y|K) = \mathrm{MR}(a|K) \le \dim X$ for all such $y$. $\square$

**Linear differential equations.** A $\partial$-*module over* $K$ is a pair $(V,d)$ where $V$ is a $K$-vector space and $d : V \to V$ is an additive map such that

$$d(\lambda v) = \partial(\lambda)v + \lambda d(v) \text{ for all } \lambda \in K,\ v \in V.$$

Note that then $d$ is $C_K$-linear. The *dimension* of a $\partial$-module over $K$ is the dimension of its underlying $K$-vector space. All $\partial$-modules below are over $K$, unless specified otherwise.

**Lemma 7.10.** *Given any $K$-linear map $A : K^n \to K^n$ we have the $\partial$-module $(K^n, \partial - A)$ where $\partial$ acts coordinatewise. Conversely, if $(K^n, d)$ is a $\partial$-module, then $d = \partial - A$ for some $K$-linear map $A : K^n \to K^n$.*

*Proof.* This is straightforward. For the second part, check that $A := \partial - d$ is $K$-linear. $\square$

Let $(K^n, \partial - A)$ be as in this lemma. Identify $A$ with its $n \times n$-matrix with respect to the standard basis, and think of $x \in K^n$ as a column vector $x = (x_1, \dots, x_n)^{\mathrm{t}}$ with components $x_i \in K$. Then the $\partial$-module $(K^n, \partial - A)$ corresponds to the equation $\partial x = Ax$, the matrix form of a system of $n$ linear differential equations. Its solutions are the $x \in K^n$ satisfying this equation.

More generally, given a $\partial$-module $(V,d)$, put

$$V(d) := \{v \in V : \ d(v) = 0\},$$

so $V(d)$ is a $C_K$-linear subspace of $V$. A *submodule* of a $\partial$-module $(V,d)$ is a $K$-linear subspace $W$ of $V$ such that $d(W) \subseteq W$, and is viewed as the $\partial$-module $(W, d|W)$. Given $\partial$-modules $(V,d)$ and $(V',d')$, a $\partial$-*morphism*

$$\phi : (V,d) \to (V',d')$$

is a $K$-linear map $\phi : V \to V'$ such that $\phi(d(v)) = d'(\phi(v))$ for all $v \in V$; note that then the kernel and image of $\phi$ are submodules of $(V,d)$ and $(V',d')$, respectively.

For a submodule $W$ of a $\partial$-module $(V,d)$, the *quotient module* $(V/W, d/W)$, or just $(V/W,d)$ for simplicity, is the $\partial$-module with $V/W$ as its underlying $K$-vector space, with $d(v+W) := d(v) + W$. Note that then the canonical map $V \to V/W$ is a $\partial$-morphism $(V,d) \to (V/W,d)$.

The next result says that, up to isomorphism, there is just one $\partial$-module of dimension $n$ over a differentially closed field. As always, $\mathbb{U}$ denotes a differentially closed field.

**Lemma 7.11.** *Let $(V,d)$ be a $\partial$-module over $\mathbb{U}$ of finite dimension.*

(1) *$V$ has a basis $b_1,\dots,b_n$ with $b_1,\dots,b_n \in V(d)$;*
(2) *let $b_1,\dots,b_n$ be as in (1) and let $e_1,\dots,e_n$ be the standard basis of the $\mathbb{U}$-vector space $\mathbb{U}^n$. Then the $\mathbb{U}$-linear map $\phi : V \to \mathbb{U}^n$ with $\phi(b_i) = e_i$ for $i = 1,\dots,n$ is a $\partial$-isomorphism $(V,d) \to (\mathbb{U}^n, \partial)$;*
(3) *with $b_1,\dots,b_n$ as in (1) we have $V(d) = Cb_1 + \cdots + Cb_n$.*

*Proof.* We can assume $V = \mathbb{U}^n$ and $d = \partial - A$ where $A : \mathbb{U}^n \to \mathbb{U}^n$ is $\mathbb{U}$-linear. Take $X = \mathbb{A}^{n^2} = \mathbb{U}^{n^2}$, the set of $n \times n$-matrices over $\mathbb{U}$. Then

$$\tau X = \mathrm{T}\, X = \mathbb{U}^{2n^2},$$

and we have the algebraic $\partial$-set $(X,s)$ defined over $\mathbf{Q}$, where

$$s : X \to \tau(X), \qquad s(B) = (B, AB).$$

Part (1) of Lemma 7.7 gives $B \in (X,s)^\partial$ with $\det(B) \neq 0$. Then $AB = \partial B$, and so the columns $b_1,\dots,b_n$ of $B$ are linearly independent and satisfy

$$Ab_i = \partial b_i, \quad i = 1,\dots,n.$$

This proves (1). For (2) and (3), let $b_1,\dots,b_n$ be as in (1), and let $v \in V$. With $v = a_1b_1 + \cdots + a_nb_n$ (all $a_i \in \mathbb{U}$), this gives

$$d(v) = \partial(a_1)b_1 + \cdots + \partial(a_n)b_n.$$

□

**Corollary 7.12.** *Let $W$ be a submodule of the $\partial$-module $(\mathbb{U}^n, \partial)$ over $\mathbb{U}$. Then the definable set $W \subseteq \mathbb{U}^n$ is defined over $C$.*

*Proof.* By the previous lemma the $\mathbb{U}$-vector space $W$ has a basis $b_1,\dots,b_m$ with $\partial(b_i) = 0$ for all $i$, that is, $b_i \in C^n$ for all $i$. □

Consider an algebraic $\partial$-set $(X, s)$ in $\mathbf{k}^m$. Then $(\mathbf{k}[X], \partial_s)$ is a $\partial$-module over $\mathbf{k}$. Consider a point $a \in X$ such that $s(a) = (a, \partial a)$, and an integer $e \geq 1$. Then we have a differential ideal $\mathfrak{m}^e_{X,a}$ of $\mathbf{k}[X, s]$. This ideal is a $\partial$-submodule of $(\mathbf{k}[X], \partial_s)$, and thus yields a finite-dimensional quotient $\partial$-module over $\mathbf{k}$, namely

$$\mathbf{k}[X, s]_{a,e} \ := \ \big(\mathbf{k}[X]/\mathfrak{m}^e_{X,a},\ \partial_s\big).$$

Let $(Y, t)$ be a second algebraic $\partial$-set in $\mathbf{k}^n$, let $\phi : (X, s) \to (Y, t)$ be a regular map, and let $\phi(a) = b$. Then $t(b) = (b, \partial b)$, and so we have the $\partial$-module $\mathbf{k}[Y, t]_{b,e}$ over $\mathbf{k}$, and $\phi^* : \mathbf{k}[Y] \to \mathbf{k}[X]$ induces a $\partial$-morphism

$$\phi^*_{a,e} : \mathbf{k}[Y, t]_{b,e} \to \mathbf{k}[X, s]_{a,e}, \quad \phi^*_{a,e}(g + \mathfrak{m}^e_{Y,b}) := \phi^*(g) + \mathfrak{m}^e_{X,a} \ \text{ for } g \in \mathbf{k}[Y].$$

**Theorem 7.13.** *Let $a \in \mathbb{U}^m$ and suppose $\mathrm{MR}(a|K)$ is finite where $K$ is a small algebraically closed differential subfield of $\mathbb{U}$. Let $L$ also be a small algebraically closed differential subfield of $\mathbb{U}$ with $K \subseteq L$, and let the finite tuple $b$ in $\mathbb{U}$ be a canonical base of $\mathrm{tp}(a|L)$. Then there are finite tuples $c$ in $C$ and $d$ in $\mathbb{U}$ such that*

$$b \underset{Ka}{\perp} d,$$

*$b$ is definable over $Kacd$.*

*Proof.* By Lemma 7.8 we can reduce to the case that $a \in (X, s)^\partial$ where $(X, s)$ is an algebraic $\partial$-set in $\mathbb{U}^m$ defined over $K$ such that $X$ is irreducible and $a$ is a generic point of $X$ over $K$. Let

$$\mathfrak{p} := \{F \in L[T_1, \dots, T_m] :\ F(a) = 0\},$$

a prime ideal of $L[T_1, \dots, T_m]$, and put

$$Y := \mathrm{Z}(\mathfrak{p}) = \{x \in \mathbb{U}^m :\ F(x) = 0 \text{ for all } F \in \mathfrak{p}\},$$

an irreducible algebraic set in $\mathbb{U}^m$ defined over $L$, with $a$ as generic point over $L$. Then $Y \subseteq X$ and $s(a) = (a, \partial a)$, so $s(a) \in \tau Y$, hence $s(Y) \subseteq \tau Y$. This gives a $\partial$-set $(Y, s|Y)$ in $\mathbb{U}^m$ and the inclusion map $Y \hookrightarrow X$ is a regular map $(Y, s|Y) \to (X, s)$. By Lemma 7.8 we have

$$\dim X = \mathrm{ord}(a|K), \qquad \dim Y = \mathrm{ord}(a|L).$$

**Claim.** Let $\sigma \in \mathrm{Aut}(\mathbb{U}|K)$. Then

$$\sigma(\mathrm{tp}(a|L)) = \mathrm{tp}(a|L) \iff \sigma(Y) = Y.$$

To prove this claim, note first that $(Y, s|Y)^\partial \in \mathrm{tp}(a|L)$. If $\sigma(Y) = Y$, then $(Y, s|Y)^\partial \in \sigma(\mathrm{tp}(a|L))$, so $\sigma(\mathrm{tp}(a|L)) = \mathrm{tp}(a|L)$

Next, assume $\sigma(\mathrm{tp}(a|L)) = \mathrm{tp}(a|L)$. Then $Y \cap \sigma(Y) \in \mathrm{tp}(a|L)$, and $Y \cap \sigma(Y)$ is an algebraic set in $\mathbb{U}^m$, so $\sigma(Y) = Y$.

It follows from this claim that $b$ codes $Y$ in $\mathbb{U}$ over $K$.

Let $e$ take positive integer values. For each $e$, put

$$V_e := \mathbb{U}[X, s]_{a,e}, \quad W_e := \mathbb{U}[Y, s|Y]_{a,e},$$

finite-dimensional $\partial$-modules over $\mathbb{U}$, and let $p_e : V_e \to W_e$ be the natural $\partial$-module morphism given by

$$p_e(f + \mathfrak{m}^e_{X,a}) \;=\; (f|Y) + \mathfrak{m}^e_{Y,a} \qquad (f \in \mathbb{U}[X]).$$

Let $V_e$ and $W_e$ have dimension $k(e)$ and $l(e)$ as vector spaces over $\mathbb{U}$. Pick $f_{e1}, \dots, f_{ek(e)} \in \mathbb{U}[X]$ such that their images in $V_e$ form a basis of $V_e$ as vector space over $\mathbb{U}$, and $f_{e1}, \dots, f_{ek(e)} : X \to \mathbb{U}$ are defined over $Ka$ in the algebraically closed field $\mathbb{U}$. (The reader should check this is possible.) Likewise, pick $g_{e1}, \dots, g_{el(e)} \in \mathbb{U}[Y]$ such that $g_{e1}, \dots, g_{el(e)} : Y \to \mathbb{U}$ are defined over $L(a)$ in the algebraically closed field $\mathbb{U}$ and the images of $g_{e1}, \dots, g_{el(e)}$ in $W_e$ form a basis of $W_e$ as vector space over $\mathbb{U}$. Note that then the matrix of $p_e$ with respect to these bases has entries in $L(a)$.

By Krull's Intersection Theorem, $Y$ is determined by the sequence

$$\ker(p_e), \quad e = 1, 2, \dots.$$

As it stands, this is vague, but here is a way to make this precise. Let $\mathrm{Aut}(\mathbb{U}|Ka)$ act on $V_e$ in the natural way; then we have for all $\sigma \in \mathrm{Aut}(\mathbb{U}|Ka)$,

$$\sigma(Y) = Y \iff \sigma(\ker p_e) = \ker p_e \text{ for all } e.$$

Let $I_e : V_e \to \mathbb{U}^{k(e)}$ be the $\mathbb{U}$-linear isomorphism that maps the basis $f_{e1}, \dots, f_{ek(e)}$ onto the standard basis of the $\mathbb{U}$-vector space $\mathbb{U}^{k(e)}$. Note that for all $\sigma \in \mathrm{Aut}(\mathbb{U}|Ka)$ and all $e$ we have

$$\sigma(\ker p_e) = \ker p_e \iff \sigma(I_e(\ker p_e)) = I_e(\ker p_e),$$

and thus for all $\sigma \in \mathrm{Aut}(\mathbb{U}|Ka)$,

$$\sigma(b) = b \iff \sigma(I_e(\ker p_e)) = I_e(\ker p_e) \text{ for all } e,$$

This gives a single $e$ such that for all $\sigma \in \mathrm{Aut}(\mathbb{U}|Ka)$,

$$\sigma(b) = b \iff \sigma(I_e(\ker p_e)) = I_e(\ker p_e).$$

We fix such an $e$ in what follows, and put

$$V := V_e, \quad k := k(e), \quad E := I_e(\ker(p_e)),$$

so the definable set $E \subseteq \mathbb{U}^k$ is coded by $b$ over $Ka$. Up till this point we only used the vectorspace structure of $V$, but we are now going to use that it is a $\partial$-module over $\mathbb{U}$. Let $d_1, \dots, d_k$ be the standard basis of the $C$-vectorspace $C^k \subseteq \mathbb{U}^k$. Lemma 7.11 yields a basis $h_1, \dots, h_k$ of the $\mathbb{U}$-vector space $V$ such that all $h_i \in V(\partial_s)$ and the $\mathbb{U}$-linear map

$$J : V \to \mathbb{U}^k, \quad J(h_i) \;=\; d_i \text{ for } i = 1, \dots, k$$

is an isomorphism $(V, \partial_s) \to (\mathbb{U}^k, \partial)$ of $\partial$-modules over $\mathbb{U}$. Then we have the submodule $J(\ker(p_e))$ of the $\partial$-module $(\mathbb{U}^k, \partial)$, so this submodule is defined over $C$ by Corollary 7.12. Using also $I_e$ it follows that $E \subseteq \mathbb{U}^k$ is defined over $Kac$. Thus $b$ is defined over $Kac$. $\square$

Recall that if $X \subseteq C^n \subseteq \mathbb{U}^n$ is definable in $\mathbb{U}$, then $X$ is definable in the algebraically closed field $C$. It follows that if $G \subseteq C^n \subseteq \mathbb{U}^n$ is a definable group in $\mathbb{U}$, then $G$ is a constructible group in the sense of the algebraically closed field $C$, and thus constructibly isomorphic to an algebraic group in $C$. In the next result and its proof "constructible" is in the sense of the algebraically closed field $C$, and $A$ denotes a small parameter set in $\mathbb{U}$.

**Proposition 7.14.** *Let $G \subseteq \mathbb{U}^m$ be a definable group in $\mathbb{U}$ such that* $\mathrm{MR}(G)$ *is finite. Suppose the small parameter set $A$ in $\mathbb{U}$ and $g \in G$ are such that*

(i) *$G$ and its group operation are $A$-definable;*
(ii) *$p := \mathrm{tp}(g|A) \in \mathrm{St}(G|A)$ is stationary, and* $\mathrm{stab}_G(p) = \{1\}$*;*

*Then the subgroup $G(p,g)$ of $G$ generated by $g^{-1}p(G)$ is a connected definable subgroup of $G$, and is definably isomorphic in $\mathbb{U}$ to a constructible group $H \subseteq C^n$.*

*Proof.* With $A$, $g$, and $p = \mathrm{tp}(g|A)$ as in the hypothesis, the set $g^{-1}p(G)$ is indecomposable (with respect to $G$), so by the Zilber indecomposability theorem the group $G(p,g)$ is a connected definable subgroup of $G$ and we have $N \in \mathbb{N}$ such that every element of $G(p,g)$ has the form $g^{-1}h_1 \cdots g^{-1}h_N$ with $h_1, \dots, h_N \in p(G)$. By results related to the previous theorem we obtain a small parameter set $B \supseteq A$ in $\mathbb{U}$ such that $g$ is $B$-definable and every $h \in p(G)$ is $B$-definable over $C$. It follows that all elements of $G(p,g)$ are $B$-definable over $C$; then each element of $G(p,g)$ has the form $f(c)$ for some partial $B$-definable map $f : C^e \rightharpoonup \mathbb{U}^m$ and some $e \in \mathbb{N}$ with $c \in \mathrm{domain}(f)$. Hence, by saturation there is a single $A$-definable map $f : Y \to \mathbb{U}^m$ with definable $Y \subseteq C^e$ $(e \in \mathbb{N})$ such that $G(p,g) = f(Y)$. Then the equivalence relation on $Y$ given by $f(y_1) = f(y_2)$ is a constructible set in $C^{2e}$, so by EI there is a constructible map $h : Y \to C^n$ for some $n$ such that for all $y_1, y_2 \in Y$ we have $f(y_1) = f(y_2) \Leftrightarrow h(y_1) = h(y_2)$. This gives a definable bijection

$$G(p,g) \to H := h(Y) \subseteq C^n, \quad f(y) \mapsto h(y) \text{ for } y \in G.$$

We now make $H$ into a definable group in $\mathbb{U}$ such that this bijection becomes a group isomorphism. By the remark preceding the theorem $H$ is a constructible group in the algebraically closed field $C$. $\square$

**Lemma 7.15.** *Let $G$ be a definable subgroup of $\mathbb{G}_{\mathrm{a}}^n(\mathbb{U})$ (which is just $\mathbb{U}^n$ with componentwise addition). Then $G$ is a $C$-linear subspace of $\mathbb{U}^n$.*

*Proof.* The set $\{c \in C : cG \subseteq G\}$ is a definable subgroup of $\mathbb{G}_{\mathrm{a}}(C)$ and contains $\mathbb{Z}$, so is infinite. Since $C$ is strongly minimal, it follows that this set is all of $C$. $\square$

Consider the logarithmic derivative map $\ell : (\mathbb{U}^\times)^n \to \mathbb{U}^n$ given by

$$\ell(x_1, \dots, x_n) \;=\; \big(\frac{x_1'}{x_1}, \dots, \frac{x_n'}{x_n}\big).$$

It is a definable group morphism $\mathbb{G}_{\mathrm{m}}^n(\mathbb{U}) \to \mathbb{G}_{\mathrm{a}}^n(\mathbb{U})$ whose kernel is

$$(C^{\times})^n = \mathbb{G}_{\mathrm{m}}^n(C),$$

which has Morley rank $n$ in $\mathbb{U}$. More generally, we have the following result due to Buium. In stating this and later results we shall violate our convention that $A$ and $B$ denote small parameter sets in our monster model $\mathbb{U}$. Instead they will denote semiabelian varieties, and we shall use additive notation for the group operations of a semiabelian variety.

**Lemma 7.16.** *Let $A$ be a semiabelian variety in $\mathbb{U}$. Then there is a group morphism $\mu : A \to \mathbb{G}_{\mathrm{a}}^n(\mathbb{U})$, definable in $\mathbb{U}$, such that $\ker(\mu)$ is a connected definable subgroup of $A$ of finite Morley rank.*

An abelian (additively written) group $\Gamma$ is said to be of *finite rank* if $\Gamma$ has a finitely generated subgroup $\Gamma'$ such that for all $\gamma \in \Gamma$ there is $n > 0$ with $n\gamma \in \Gamma'$. (This notion of finite rank has nothing to do with Morley rank.) In particular, every finitely generated abelian group has finite rank, but the (additive) group $\mathbb{Q}^n$ has also finite rank, as well as the (multiplicative) group of roots of unity in any field.

**Corollary 7.17.** *Let $A$ be a semiabelian variety in $\mathbb{U}$ and let $\Gamma$ be a subgroup of $A$ of finite rank. Then there is a connected definable subgroup $H$ of $A$ such that $\Gamma \subseteq H$ and $H$ has finite Morley rank.*

*Proof.* Take $\mu$ as in Lemma 7.16. Then $\mu(A)$ is a $C$-linear subspace of $\mathbb{U}^n$ by Lemma 7.15, so $\mu(\Gamma)$ generates a finite-dimensional $C$-linear subspace $V$ of $\mu(A)$. Then $V$ is definable in $\mathbb{U}$ of finite Morley rank, and also a connected definable subgroup of $\mathbb{G}_{\mathrm{a}}^n(\mathbb{U})$. Put $H := \mu^{-1}(V)$, a definable subgroup of $A$ containing $\Gamma$. Since $\mu(H)$ is a $C$-linear subspace of $\mathbb{U}^n$ and contains $\Gamma$ we have $\mu(H) = V$. This gives an exact sequence

$$0 \longrightarrow \ker(\mu) \longrightarrow H \longrightarrow V \longrightarrow 0$$

of definable groups and definable group morphisms. It follows easily that $H$ is of finite Morley rank and connected as a definable group in $\mathbb{U}$. $\square$

We can now state the main Mordell-Lang type result for function fields of characteristic 0. In what follows we fix algebraically closed fields $K$ and $L$ of characteristic 0 with $K \subseteq L$.

**Theorem 7.18.** *Let $A = A(L)$ be a semiabelian variety in $L$, let $\Gamma$ be a subgroup of $A$ of finite rank, and $X$ an irreducible closed set in $A$ such that $\Gamma \cap X$ is dense in $X$.*

*Then $X$ comes from $K$ as follows: there is a closed subgroup $A'$ of $A$, a semiabelian variety $B$ in $K$, a closed irreducible $Y \subseteq B$, and a surjective algebraic group morphism $\phi : A' \to B(L)$ such that $X = a + \phi^{-1}\big(Y(L)\big)$ for some $a \in A$. If $X$ has trivial stabilizer in $A$, then we can arrange that $\phi$ is an algebraic group isomorphism.*

Before we begin the proof, note that the theorem holds trivially for $K = L$ with $A = A' = B$, $X = Y$, $\phi = \mathrm{id}_A$ and $a = 0 \in A$. Also, the strongest version of the theorem is when $K$ is as small as possible, that is, when $K$ is the algebraic closure of $\mathbb{Q}$ in $L$.

*Proof.* Let $S := \{a \in A : a + X = X\}$ be the stabilizer of $X$ in $A$. It is a constructible and therefore closed subgroup of $A$, and $X$ is a union of cosets of $S$. Then $A/S$ is also a semiabelian variety. Let $\Gamma/S$ and $X/S$ be the images of $\Gamma$ and $X$ under the canonical map $A \to A/S$. Then $X/S$ is a closed irreducible set in $A/S$, $(\Gamma/S) \cap (X/S)$ is dense in $X/S$, and $X/S$ has trivial stabilizer in $A/S$. By replacing $A$, $\Gamma$ and $X$ by their images $A/S$, $\Gamma/S$, and $X/S$ we reduce to the case that $X$ has trivial stabilizer in $A$. (The reader should verify the details of this reduction.)

As noted before the proof, we can assume $K \neq L$. Then $(L, K)$ is a model of the theory of algebraically closed fields of characteristic 0 with a predicate for a proper algebraically closed subfield. This theory is complete, and $(\mathbb{U}, C)$ is also a model of it (where we forget $\partial$). So by taking $\mathbb{U}$ sufficiently big we can arrange that $(L, K)$ is an elementary submodel of the model $(\mathbb{U}, C)$ of this theory. Replacing $A(L)$ by $A(\mathbb{U})$ and $X$ by $X(\mathbb{U})$ we reduce to the case that $L = \mathbb{U}$ and $K = C$. (The reader should check the details of this reduction.)

By Corollary 7.17 we can take a connected definable subgroup $G$ of $A$ of finite Morley rank such that $\Gamma \subseteq G$. Then $G \cap X$ is dense in $X$. Among the definable subsets of $G \cap X$ that are dense in $X$, let $P$ be one of least Morley rank. Then $P = P_1 \cup \cdots \cup P_d$, $d = \mathrm{MD}(P)$, where all $P_i$ are definable with the same Morley rank as $P$ and with Morley degree 1. Then some $P_i$ is dense in $X$, so by replacing $P$ by a suitable $P_i$ we can assume that $P$ has Morley degree 1. Let $m := \mathrm{MR}(P)$, and let $G$ and $P$ be defined over the small algebraically closed differential subfield $\mathbf{k}$ of $\mathbb{U}$.

Take the unique $p \in \mathrm{St}(G|\mathbf{k})$ such that $\mathrm{MR}(p) = m$ and $P \in p$. Then $p$ is stationary and $p(G) \subseteq P \subseteq G \cap X$.

*Claim 1.* $\mathrm{stab}_G(p) = \{0\}$.

To prove this claim, let $g \in \mathrm{stab}_G(p)$. Then $\mathrm{MR}\big((g + P) \cap P\big) = m$, hence $P = \big((g + P) \cap P\big) \cup Q$ with definable $Q \subseteq P$ and $\mathrm{MR}(Q) < m$, so $Q$ is not dense in $X$. Hence $(g + P) \cap P$ is dense in $X$, so $g + X = X$, and thus $g = 0$.

*Claim 2.* The set $p(G)$ is dense in $X$.

Suppose otherwise. Then $p(G) \subseteq Z$ where $Z$ is a proper closed subset of $X$. Then $P \cap Z$ is not dense in $X$, so $\mathrm{MR}(P \cap Z) < m$. Since $p(G) \subseteq P \cap Z$, this yields $\mathrm{MR}(p) < m$, a contradiction.

Take any $g \in p(G)$, and let $G(p, g)$ be the subgroup of $G$ generated by $p(G) - g$. It follows from Claim 1 and Proposition 7.14 that $G(p, g)$ is a connected definable subgroup of $G$ and that we have a connected definable group $H \subseteq C^m$ in the algebraically closed field $C$ and a group isomorphism

$h : H \to G(p, g)$ that is definable in $\mathbb{U}$. Let $B := H^{\mathrm{a}}$, an algebraic group in $C$. Then $B(\mathbb{U})$ is the corresponding algebraic group in $\mathbb{U}$.

By Lemmas 4.15 and 6.19 we have an algebraic group morphism $B(\mathbb{U}) \to A$ extending $h : H \to G(p, g)$; we denote this extension also by $h$. Since $B(\mathbb{U})$ is connected, its image $A' := h(B(\mathbb{U}))$ is a connected closed subgroup of $A$, and thus a semiabelian variety.

*Claim 3.* $h : B(\mathbb{U}) \to A'$ is an algebraic group isomorphism.

We first show that $B$ is a semiabelian variety. Let $N$ be an algebraic vector group with respect to $C$ and a closed subgroup of $B$. Then $N(\mathbb{U})$ is an algebraic vector group with respect to $\mathbb{U}$ and a closed subgroup of $B(\mathbb{U})$, so $h|N(\mathbb{U})$ is trivial. Since $h$ is injective on $B$ it follows that $N$ is trivial. This argument shows that $B$ is a semiabelian variety. Then by Corollary 6.24 the connected component $\ker(h)^0$ of $\ker(h)$ is defined over $C$, so is trivial, since $h$ is injective on $B$. Hence $\ker(h)$ is finite, so $\ker(h) \subseteq \mathrm{t}(B(\mathbb{U})) = \mathrm{t}(B)$, and thus $\ker(h)$ is trivial.

Since $p(G) - g$ is dense in $X - g$ and $p(G) - g \subseteq G(p, g) \subseteq A'$ we have $X - g \subseteq A'$. The set $h^{-1}(p(G) - g) \subseteq B$ is dense in the closed irreducible subset $h^{-1}(X - g)$ of $B(\mathbb{U})$, so $h^{-1}(X - g)$ is defined over $C$, that is,

$$h^{-1}(X - g) = Y(\mathbb{U})$$

where $Y$ is a closed irreducible subset of $B$. Then $X - g = h(Y(\mathbb{U})$, and we have established the desired result with $\phi = h^{-1} : A' \to B(\mathbb{U})$. □

For abelian varieties we turn this into a more attractive result as follows. Let $A = A(L)$ be an abelian variety in $L$. We say that $A$ *has no $K$-trace* if $A$ has no nontrivial abelian subvariety isomorphic (as algebraic group) to $B(L)$ for any abelian variety $B$ in $K$. It can be shown that then there is no surjective algebraic group morphism $A' \to B(L)$ for any closed subgroup $A'$ of $A$ and any nontrivial abelian variety $B$ in $K$.

**Corollary 7.19.** *Let $A = A(L)$ be an abelian variety in $L$ with no $K$-trace, let $\Gamma$ be a finitely generated subgroup of $A$, and let $X$ be a closed subset of $A$. Then $\Gamma \cap X$ is a finite union of cosets in $A$ of subgroups of $A$.*

*Proof.* Let $X_1, \ldots, X_m$ be the irreducible components of the closure of $\Gamma \cap X$ in $X$. Then $\Gamma \cap X_i$ is dense in $X_i$ for all $i$, so by replacing $X$ by each of the $X_i$ we reduce to the case that $X$ is irreducible and $\Gamma \cap X$ is dense in $X$.

Then Theorem 7.18 and the $K$-trace assumption yield a closed subgroup $A'$ of $A$ such that $X = a + A'$ with $a \in A$. If $\Gamma \cap X \neq \emptyset$, we can take $a \in \Gamma \cap X$, and then $\Gamma \cap X = a + (A' \cap \Gamma)$. □