Algebraic Groups

Jay Taylor

Last Updated: 04/05/2015

Introduction

These are the personal notes of the author from a graduate course given jointly with Dr Iulian Simion at the Università degli Studi di Padova in the academic year 2014/2015. The theory of algebraic groups has been exposed time and time again at the graduate level in several text books [Bor91; Hum75; Spr09; Gec03]; so it is not surprising that there is nothing new to be found here. Indeed, the notes follow closely the excellent text of Springer [Spr09] but include parts influenced by [Gec03] and [Hum75].

The author thanks Dr Simion for many useful comments and fruitful discussions about algebraic groups.

Contents

1. Affine Algebraic Geometry

1.1 Notation

Throughout these notes K will denote an algebraically closed field. The n-fold direct product K^n of K will be denoted by $\mathbb{A}^n$ and we refer to this as *affine n-space*. We denote K^n in this way to obfuscate the underlying field structure. If X is any set then we will denote by $\mathrm{Pow}(X)$ the powerset of X, i.e., the set of all subsets of X. Given any subset of $\mathrm{Pow}(X)$ we will always consider this as a poset with respect to the inclusion of subsets.

Note that all rings in these notes will be assumed to be commutative and contain 1. Furthermore, if S is a ring then we will denote by $\mathcal{I}(S) \subseteq \mathrm{Pow}(S)$ the poset of all ideals of S.

1.2 Algebraic Sets and Vanishing Ideals

1.2.1. Affine algebraic geometry is concerned with the study of subsets of affine n-space $V \subseteq \mathbb{A}^n$ which are obtained as the zero-locus of a set of polynomial equations. For example, the parabola

$$V = \{(x, y) \in \mathbb{A}^2 \mid (x-1)^2 - y = 0\}.$$

To make this precise consider the polynomial ring $A = K[X_1, \dots, X_n]$. It is clear that we may naturally identify this as a subalgebra of the K-algebra $\mathrm{Maps}(\mathbb{A}^n, K)$ of all functions $f : \mathbb{A}^n \to K$. Now for any subset $S \subseteq A$ we set

$$\mathbf{V}(S) := \{v \in \mathbb{A}^n \mid f(v) = 0 \text{ for all } f \in S\} \subseteq \mathbb{A}^n,$$

which we call the *algebraic set* defined by S. This construction clearly defines a map $\mathbf{V} : \mathrm{Pow}(A) \to \mathrm{Pow}(\mathbb{A}^n)$.

Lemma 1.2.2. *The map $\mathbf{V}$ satisfies the following properties:*

(a) $\mathbf{V}(\{0\}) = \mathbb{A}^n$ *and* $\mathbf{V}(A) = \varnothing$,

(b) $\mathbf{V}(I) \subseteq \mathbf{V}(J)$ *for any subsets* $J \subseteq I \subseteq A$,

(c) $\mathbf{V}(I \cap J) = \mathbf{V}(I) \cup \mathbf{V}(J)$ *for any two ideals* $I, J \in \mathcal{I}(A)$,

(d) given any (possibly infinite) family $\{I_\lambda \mid \lambda \in \Lambda\} \subseteq \mathrm{Pow}(A)$ *we have*

$$\mathbf{V}\Big(\bigcup_{\lambda\in\Lambda} I_\lambda\Big) = \bigcap_{\lambda\in\Lambda} \mathbf{V}(I_\lambda).$$

Proof. We only prove (c), the rest are left as easy exercises. Consider the product ideal $IJ = \langle fg \mid f \in I \text{ and } g \in J\rangle \subseteq I \cap J$. By (b) we have

$$\mathbf{V}(I) \cup \mathbf{V}(J) \subseteq \mathbf{V}(I \cap J) \subseteq \mathbf{V}(IJ).$$

Now assume, if possible, that $x \in \mathbf{V}(IJ) \setminus (\mathbf{V}(I) \cup \mathbf{V}(J))$ then there exists $f \in I$ and $g \in J$ such $f(x) \neq 0$ and $g(x) \neq 0$ but then $f(x)g(x) \neq 0$, which is a contradiction. ■

Remark 1.2.3. The proof of (c) shows that $\mathbf{V}(IJ) = \mathbf{V}(I \cap J)$. As, in general, $IJ \neq I \cap J$ we have $\mathbf{V}$ is not injective on ideals.

Exercise 1.2.4. If the family $\{I_\lambda \mid \lambda \in \Lambda\}$ in (d) are ideals then show that $\bigcup_{\lambda\in\Lambda} I_\lambda$ may be replaced by $\sum_{\lambda\in\Lambda} I_\lambda$.

Notation. For any algebraic set $X \subseteq \mathbb{A}^n$ we will denote by $\mathcal{C}(X)$ the set of all algebraic sets $V \subseteq \mathbb{A}^n$ such that $V \subseteq X$.

1.2.5. Note that even if I and J are not ideals in (c) then the proof shows that

$$\mathbf{V}(I) \cup \mathbf{V}(J) = \mathbf{V}(\{fg \mid f \in I \text{ and } g \in J\}).$$

However, restricting to the case of ideals is beneficial and loses no information. Indeed it is immediately clear from the definition that, for any subset $S \subseteq A$, we have $\mathbf{V}(S) = \mathbf{V}(\langle S \rangle)$ where $\langle S \rangle \in \mathcal{I}(A)$ is the ideal generated by S. Therefore, we may and will consider $\mathbf{V}$ as a map $\mathcal{I}(A) \to \mathcal{C}(\mathbb{A}^n)$ without losing any information.

Example 1.2.6. Consider the case when $n = 1$ then if $V \in \mathcal{C}(\mathbb{A}^1)$ we either have V has finite cardinality or $V = \mathbb{A}^1$. As the polynomial ring $K[X]$ is a principal ideal domain we have every closed set in $\mathbb{A}^1$ is of the form $V = \mathbf{V}(\langle f \rangle) = \mathbf{V}(\{f\})$ for some polynomial $f \in K[X]$. Now either $f = 0$ in which case $V = \mathbb{A}^1$ or $f \neq 0$ in which case $|V| < \infty$ because f can have only finitely many roots. Hence every proper closed subset of $\mathbb{A}^1$ is finite.

1.2.7. Now (a), (c) and (d) of Lemma 1.2.2 show that the algebraic sets in $\mathbb{A}^n$ form the closed sets of a topology on $\mathbb{A}^n$ which we call the *Zariski topology*. If $V \subseteq \mathbb{A}^n$ is any subset then we also refer to the induced topology on V as the Zariski topology. Note that if V is an algebraic set then $\mathcal{C}(V)$ is the set of closed sets in the Zariski topology on V, i.e., the closed sets in V are the closed sets in $\mathbb{A}^n$ which are contained in V.

For any subset $V \subseteq \mathbb{A}^n$ one can also consider the so-called *vanishing ideal* of V given by

$$\mathbf{I}(V) = \{f \in A \mid f(x) = 0 \text{ for all } x \in V\} \subseteq A$$

(it is trivial to check that this is indeed an ideal). The following shows that the resulting map $\mathbf{I} : \mathrm{Pow}(\mathbb{A}^n) \to \mathcal{I}(A)$ gives a right inverse to $\mathbf{V}$.

Lemma 1.2.8. *The map* $\mathbf{I}$ *satisfies the following properties:*

(a) $\mathbf{I}(V) \subseteq \mathbf{I}(W)$ *for any subsets* $W \subseteq V \subseteq \mathbb{A}^n$*,*

(b) $V \subseteq \mathbf{V}(\mathbf{I}(V))$ *for any subset* $V \subseteq \mathbb{A}^n$ *and* $I \subseteq \mathbf{I}(\mathbf{V}(I))$ *for any subset* $I \subseteq A$*,*

(c) If $V \subseteq \mathbb{A}^n$ *is any subset then* $\mathbf{V}(\mathbf{I}(V)) = \overline{V}$ *is the closure of* V *in the Zariski topology,*

(d) given any (possibly infinite) family $\{V_\lambda \mid \lambda \in \Lambda\} \subseteq \mathrm{Pow}(\mathbb{A}^n)$ *we have*

$$\mathbf{I}\Big(\bigcup_{\lambda\in\Lambda} V_\lambda\Big) = \bigcap_{\lambda\in\Lambda} \mathbf{I}(V_\lambda).$$

Proof. Again we will only prove (c), the remaining points are easy exercises. By (b) we have $V \subseteq \mathbf{V}(\mathbf{I}(V))$ so $\overline{V} \subseteq \mathbf{V}(\mathbf{I}(V))$ because the right hand side is a closed set. Now assume $W \subseteq \mathbf{V}(\mathbf{I}(V))$ is a closed set containing V then $W = \mathbf{V}(J)$ for some ideal $J \in \mathcal{I}(A)$. By (a) and (b) we have

$$J \subseteq \mathbf{I}(\mathbf{V}(J)) = \mathbf{I}(W) \subseteq \mathbf{I}(V) \Rightarrow \mathbf{V}(\mathbf{I}(V)) \subseteq \mathbf{V}(J) = W.$$

As $\overline{V}$ is the intersection of all such closed sets W this gives (c). ■

1.2.9. As was remarked in Remark 1.2.3 the map $\mathbf{V}$ is not injective on $\mathcal{I}(A)$. We will see that this is related to the fact that $\mathbf{I}$ is not surjective. Indeed for any ideal $I \in \mathcal{I}(A)$ we define the *radical* of I to be

$$\sqrt{I} = \{f \in A \mid f^k \in I \text{ for some } k \in \mathbb{N}\}$$

We claim that this is again an ideal of I. Assume $a, b \in \sqrt{I}$ then there exists integers $r, s \in \mathbb{N}$ such that $a^r, b^s \in I$. Applying the binomial theorem we have

$$(a+b)^{r+s} = \sum_{i=0}^{r+s} \binom{r+s}{i} a^i b^{r-i+s}.$$

Now for each $0 \leqslant i \leqslant r+s$ we either have $i \geqslant r$ or $r-i+s \geqslant s$ so either $a^i \in I$ or $b^{r-i+s} \in I$. This implies each term in the sum is contained in I so $a+b \in \sqrt{I}$.

Definition 1.2.10. If S is a ring then we say an ideal $I \in \mathcal{I}(S)$ is a *radical ideal* if $I = \sqrt{I}$. We denote by $\mathcal{R}(S) \subseteq \mathcal{I}(S)$ the set of all radical ideals.

1.2.11. For any subset $V \subseteq \mathbb{A}^n$ it is clear that the vanishing ideal $\mathbf{I}(V)$ is a radical ideal. Indeed, let $f \in \sqrt{\mathbf{I}(V)}$ then there exists $k \in \mathbb{N}$ such that $f^k(x) = 0$ for all $x \in V$ but this implies $f(x) = 0$ for all $x \in V$ so $f \in \mathbf{I}(V)$. The following important theorem of Hilbert gives the analogue of Lemma 1.2.8(c) for ideals.

Theorem 1.2.12 (Hilbert's Nullstellensatz). *Given any ideal $I \in \mathcal{I}(A)$ we have $\mathbf{I}(\mathbf{V}(I))$ is the radical $\sqrt{I}$ of I.*

Proof. See [Hum75, §1.1]. ■

Corollary 1.2.13. *The maps $\mathbf{V}$ and $\mathbf{I}$ define order reversing inverse bijections $\mathcal{R}(A) \to \mathcal{C}(\mathbb{A}^n)$.*

Proof. The fact that the maps are order reversing is proved in Lemma 1.2.2(b) and Lemma 1.2.8(a). Now, we've already proved in Lemma 1.2.8(c) that $\mathbf{V} \circ \mathbf{I}$ is the identity on closed sets and Hilbert's Nullstellensatz shows that $\mathbf{I} \circ \mathbf{V}$ is the identity on radical ideals, so we're done. ■

1.2.14. This correspondence between algebraic sets and radical ideals is one of the fundamental relationship in algebraic geometry. Through this bijection one can try and relate geometric properties of algebraic sets to algebraic properties of ideals. We will see our first example of this in Proposition 1.3.7.

Exercise 1.2.15. For any two radical ideals $I, J \in \mathcal{R}(A)$ show that $I \cap J = \sqrt{IJ}$.

Definition 1.2.16. A ring S is called *Noetherian* if it satisfies the ascending chain condition on ideals. In other words, every ascending chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$ in S stabilises so that $I_k = I_{k+1} = \cdots$ for some index k.

Exercise 1.2.17. A ring S is Noetherian if and only if every ideal of S is finitely generated.

Theorem 1.2.18 (Hilbert's Basis Theorem). *The ring $K[X_1, \dots, X_n]$ is Noetherian.*

Proof. See [Gec03, Theorem 1.1.1]. ■

Definition 1.2.19. A topological space X is called *Noetherian* if it satisfies the descending chain condition on closed sets. In other words, every descending chain of closed sets $V_1 \supseteq V_1 \supseteq \cdots$ in X stabilises so that $V_k = V_{k+1} = \cdots$ for some index k.

Proposition 1.2.20. *Assume $V \in \mathcal{C}(\mathbb{A}^n)$ is an algebraic set then the following hold:*

(a) the Zariski topology on V is Noetherian.

(b) any finite subset of V is closed.

(c) any open cover of V has a finite subcover.

Proof. (a). Let $V_1 \supseteq V_2 \supseteq \cdots$ be a descending sequence of closed subsets of V then $\mathbf{I}(V_1) \subseteq \mathbf{I}(V_2) \subseteq \cdots$ is an ascending sequence of ideals in A. As A is Noetherian we have $\mathbf{I}(V_k) = \mathbf{I}(V_{k+1}) = \cdots$ for some index k but by Corollary 1.2.13 this implies $V_k = V_{k+1} = \cdots$ so V is Noetherian.

(b). For any $x = (x_1, \dots, x_n) \in V$ we have $\{x\} = \mathbf{V}(\{X_1 - x_1, \dots, X_n - x_n\})$, so all singletons are closed. This implies that all finite subsets are closed as they are a finite union of closed sets.

(c). By definition $V = \mathbf{V}(I)$ for some ideal $I \in \mathcal{I}(A)$. Assume $\{O_\lambda \mid \lambda \in \Lambda\} \subseteq V$ is an open cover of V then clearly

$$V = \bigcup_{\lambda \in \Lambda} O_\lambda \Leftrightarrow \varnothing = \bigcap_{\lambda \in \Lambda} V_\lambda$$

where $V_\lambda = V \setminus O_\lambda$ is a corresponding closed set. Therefore it suffices to show that the intersection may be refined to include only finitely many of the closed subsets $V_\lambda \subseteq V$. By Corollary 1.2.13, Lemma 1.2.2(d) and Exercise 1.2.4 there exists a corresponding family of ideals $\{I_\lambda \mid \lambda \in \Lambda\} \subseteq \mathcal{I}(A)$ such that $V_\lambda = \mathbf{V}(I_\lambda)$ and $\sum_{\lambda \in \Lambda} I_\lambda = A$. As A is finitely generated there must exist a finite subset $\Lambda' \subseteq \Lambda$ such that $\sum_{\lambda \in \Lambda'} I_\lambda = A$ so $\varnothing = \bigcap_{\lambda \in \Lambda'} V_\lambda$ as desired. ■

1.3 Irreducibility of Topological Spaces

Definition 1.3.1. Assume Z is a non-empty topological space. We say Z is *reducible* if $Z = Z_1 \cup Z_2$ with $Z_1, Z_2 \subsetneq Z$ proper non-empty closed subsets. We say Z is *irreducible* if it is not reducible. Any subset of Z is called reducible/irreducible if it is so in the induced topology on Z.

1.3.2. Note that we do not consider the emptyset to be an irreducible topological space. Also, simply rephrasing the definition we see that for any topological space Z we have the subset $W \subseteq Z$ is irreducible if and only if for any two non-empty open subsets of $O_1, O_2 \subseteq Z$ satisfying $O_i \cap W \neq \varnothing$ we have $O_1 \cap O_2 \cap W \neq \varnothing$.

Lemma 1.3.3. *Let Z be a topological space then:*

(a) $W \subseteq Z$ is irreducible if and only if $\overline{W}$ is irreducible.

(b) If $\phi : Z \to W$ is a continuous map and Z is irreducible then so is the image $\phi(Z)$.

Proof. (a). Assume W is irreducible and $\overline{W} = W_1 \cup W_2$ for some closed subsets $W_i \subseteq \overline{W}$ then $W = (W \cap W_1) \cup (W \cap W_2)$ with each subset $W \cap W_i$ being closed by definition. By the irreducibility of W we have $W \cap W_i = W$ for some $i \in \{1,2\}$, so $W \subseteq W_i \Rightarrow \overline{W} \subseteq W_i \Rightarrow \overline{W} = W_i$. In particular, $\overline{W}$ must be irreducible.

Conversely assume $\overline{W}$ is irreducible. If $W = W_1 \cup W_2$ for some closed subsets $W_i \subseteq W$ then by definition $W_i = W \cap Z_i$ for some closed sets $Z_i \subseteq Z$. Now clearly

$$\overline{W} = \overline{W_1 \cup W_2} = \overline{W_1} \cup \overline{W_2} \subseteq Z_1 \cup Z_2 \Rightarrow \overline{W} = (\overline{W} \cap Z_1) \cup (\overline{W} \cap Z_2).$$

As $\overline{W}$ is irreducible this implies that $\overline{W} = \overline{W} \cap Z_i$ for some index $i \in \{1,2\}$ but then clearly $W = W \cap \overline{W} \cap Z_i = W \cap Z_i$ so W is irreducible.

(b). Assume $O_1, O_2 \subseteq W$ are open subsets such that $O_i \cap \phi(Z) \neq \varnothing$ then we need to show that $O_1 \cap O_2 \cap \phi(Z) \neq \varnothing$ by 1.3.2. The pre-images $\phi^{-1}(O_i)$ are non-empty open subsets of Z because ϕ is continuous and we must have $\phi^{-1}(O_1) \cap \phi^{-1}(O_2) \neq \varnothing$ because Z is irreducible. Clearly the image of $\phi^{-1}(O_1) \cap \phi^{-1}(O_2)$ under ϕ is contained in $O_1 \cap O_2 \cap \phi(Z)$ so this is non-empty. ■

Corollary 1.3.4. *If X is an irreducible topological space then any non-empty open set in X is dense and irreducible.*

Proof. Assume $O \subseteq X$ is an open set of X then clearly we have $X = (X \setminus O) \cup \overline{O}$. As X is irreducible we either have $O = \varnothing$ or $\overline{O} = X$ so any non-empty open set is dense. As X is irreducible we have any non-empty open set is irreducible by Lemma 1.3.3. ■

Proposition 1.3.5. *If Z is a Noetherian topological space then Z has finitely many maximal irreducible subsets $Z_1, \dots, Z_r \subseteq Z$. These are closed subsets of Z such that $Z = Z_1 \cup \cdots \cup Z_r$.*

Proof. We start by showing that Z is a union of finitely many closed irreducible subsets. Assume for a contradiction that this is not the case then Z must be reducible, i.e., $Z = Z_1 \cup W_1$ for two proper closed subsets $Z_1, W_1 \subsetneq Z$. At least one of these subsets must be reducible, say W_1, so $W_1 = Z_2 \cup W_2$ for two proper closed subsets $Z_2, W_2 \subsetneq W$. Continuing in this way we may construct a descending chain of closed subsets $Z_1 \supsetneq Z_2 \supsetneq \cdots$ which never terminates. However this contradicts the fact that Z is Noetherian.

Let us therefore write $Z = Z_1 \cup \cdots \cup Z_r$ with each Z_i irreducible and closed. We may clearly assume that Z_i is not contained in Z_j for each $i \neq j$. Assume $W \subseteq Z$ is a closed irreducible subset then

$$W = W \cap Z = W \cap (Z_1 \cup \cdots \cup Z_r) = (W \cap Z_1) \cup \cdots (W \cap Z_r).$$

Each intersection $W \cap Z_i$ is closed in W so we must have $W = W \cap Z_i$ for some index i because W is irreducible. Hence we have $W \subseteq Z_i$ so the Z_i are the maximal closed irreducible subsets of Z. ■

Definition 1.3.6. The maximal closed irreducible subsets of a Noetherian topological space Z are called the *components* of Z.

As promised in 1.2.14 we come to our first example relating geometric and algebraic properties.

Proposition 1.3.7. *A closed subset $V \subseteq \mathbb{A}^n$ is irreducible if and only if $\mathbf{I}(V) \in \mathcal{I}(A)$ is a prime ideal.*

Proof. Assume V is irreducible and let $f, g \in A$ be such that $fg \in \mathbf{I}(V)$ then $V \subseteq \mathbf{V}(fg)$ so

$$V = V \cap \mathbf{V}(fg) = V \cap (\mathbf{V}(f) \cup \mathbf{V}(g)) = (V \cap \mathbf{V}(f)) \cup (V \cap \mathbf{V}(g)).$$

By the irreducibility of V we either have $V = V \cap \mathbf{V}(f)$ or $V = V \cap \mathbf{V}(g)$ so either $f \in \mathbf{I}(V)$ or $g \in \mathbf{I}(V)$. Hence $\mathbf{I}(V)$ is a prime ideal.

Conversely assume $\mathbf{I}(V)$ is a prime ideal. Let $I, J \in \mathcal{I}(A)$ be ideals such that $V = \mathbf{V}(I) \cup \mathbf{V}(J) = \mathbf{V}(I \cap J)$ (c.f., Lemma 1.2.2(c)). If $V \neq \mathbf{V}(I)$ then there exists $f \in I$ with $f \notin \mathbf{I}(V)$. Now, for any $g \in J$ we have $fg \in \mathbf{I}(V)$ which implies $g \in \mathbf{I}(V)$ because $\mathbf{I}(V)$ is a prime ideal. In particular $J \subseteq \mathbf{I}(V) \Rightarrow V = \mathbf{V}(\mathbf{I}(V)) \subseteq \mathbf{V}(J)$ so $V = \mathbf{V}(J)$ and V is irreducible. ■

Definition 1.3.8. A topological space Z is called *connected* if Z cannot be written as the disjoint union of two proper closed subsets.

Exercise 1.3.9. Assume Z is a Noetherian topological space. Show that Z is a disjoint union of finitely many closed connected subsets, called the connected components of Z. Furthermore, show that any connected component of Z is a union of irreducible components.

1.4 Affine Algebras

1.4.1. At this point we could continue by only studying closed subsets of affine n-space, however this is somewhat undesirable. An analogy would be to approach finite group theory by only studying subgroups of the symmetric group. Therefore we will now axiomatise our current setup so as to break free of the embedding into affine space. To do this we need to analyse the algebraic sets.

1.4.2. Assume $X \subseteq \mathbb{A}^n$ is an algebraic set then we may consider the quotient algebra $K[X] = K[X_1, \dots, X_n]/\mathbf{I}(X)$ which we call the *affine algebra* of X. The following two properties turn out to be enough to characterise the affine algebra of an algebraic set:

- $K[X]$ is *finitely generated*, i.e., there exists a finite subset $\{f_1, \dots, f_r\} \subseteq K[X]$ such that $K[X] = K[f_1, \dots, f_r]$.
- $K[X]$ is *reduced*, i.e., $K[X]$ contains no non-zero nilpotent elements (c.f., Theorem 1.2.12).

Indeed, assume S is a finitely generated reduced K-algebra and let $\{f_1, \dots, f_r\} \subseteq S$ be a generating set. Clearly we have a surjective map $\pi : K[X_1, \dots, X_r] \to S$ given by $X_i \mapsto f_i$ and as S is reduced we must have the kernel $I = \mathrm{Ker}(\pi)$ is a radical ideal. Setting $Y = \mathbf{V}(I) \subseteq \mathbb{A}^r$ we then have $S \cong K[Y]$.

Note that, as in the case of affine n-space, we view $K[X]$ as a subalgebra of $\mathrm{Maps}(X, K)$. Indeed, assume $f \in K[X]$ then we have $f = g + \mathbf{I}(X)$ for some $g \in A$. For any $x \in X$ we then set $f(x) := g(x)$ for all $x \in X$. Note this is well defined because if $h \in A$ is also such that $f = h + \mathbf{I}(X)$ then we have $g - h \in \mathbf{I}(X)$ so $g(x) = h(x)$ for all $x \in X$.

Definition 1.4.3. We say a K-algebra is an *affine K-algebra* if it is finitely generated and reduced.

1.4.4. The algebraic set X and the Zariski topology on X are easily recovered from the affine algebra. Indeed, for any subset $S \subseteq K[X]$ and any subset $Y \subseteq X$ we define

$$\mathbf{V}_X(S) = \{x \in X \mid f(x) = 0 \text{ for all } f \in S\},$$
$$\mathbf{I}_X(Y) = \{f \in K[X] \mid f(x) = 0 \text{ for all } x \in X\}.$$

By the definition of the Zariski topology we have $V \subseteq X$ is a closed set if and only if $V = \mathbf{V}(I) \subseteq \mathbb{A}^n$ is an algebraic set for some ideal $I \in \mathcal{I}(A)$ necessarily satisfying $\mathbf{I}(X) \subseteq I$. Note that we have a bijection

$$\{I \in \mathcal{I}(A) \mid \mathbf{I}(X) \subseteq I\} \longleftrightarrow \mathcal{I}(K[X]) \tag{1.4.5}$$

given by $I \mapsto I + \mathbf{I}(X)$. From the definition it is clear that $\mathbf{V}(I) = \mathbf{V}_X(I + \mathbf{I}(X))$ which immediately shows that $\{\mathbf{V}_X(I) \mid I \in \mathcal{I}(K[X])\}$ is precisely the set of closed sets in X. Thus we have recovered the Zariski topology on X. Now let us assume that $V \subseteq X \subseteq \mathbb{A}^n$ is a closed subset of X then we have $\mathbf{I}(X) \subseteq \mathbf{I}(V) \subseteq A$. It is immediate from the definitions that we have $\mathbf{I}_X(V) = \mathbf{I}(V) + \mathbf{I}(X)$.

Definition 1.4.6. For any ring S we denote by $\mathrm{Spec}(S) \subseteq \mathcal{I}(S)$ the set of all prime ideals of S, which we call the *spectrum* of S. Furthermore, we denote by $\mathrm{MSpec}(S) \subseteq \mathrm{Spec}(S)$ the set of all maximal ideals of S, which we call the *maximal spectrum* of S.

Exercise 1.4.7. The map in (1.4.5) restricts to a bijection between radical, prime and maximal ideals.

Exercise 1.4.8. Any maximal ideal of a ring is a radical ideal.

1.4.9. We have already seen in Proposition 1.3.7 that $\mathrm{Spec}(K[X])$ corresponds to the closed irreducible subsets of X. Clearly amongst those closed irreducible subsets are the singletons of X, i.e., the points of X. The following shows that on the side of $\mathrm{Spec}(K[X])$ these correspond to the maximal ideals.

Lemma 1.4.10. *The map $x \mapsto \mathfrak{m}_x := \mathbf{I}_X(\{x\})$ defines a bijection $X \to \mathrm{MSpec}(K[X])$.*

Proof. Clearly $\mathfrak{m}_x$ is maximal because we have

$$K[X]/\mathfrak{m}_x \cong A/\mathbf{I}(\{x\}) \cong \mathrm{Maps}(\{x\}, K) \cong K.$$

The injectivity of the map is obvious, so we need only show that it is surjective. Now assume $\mathfrak{m} \in \mathrm{MSpec}(A)$ is a maximal ideal then $\mathbf{I}(\mathbf{V}(\mathfrak{m})) = \mathfrak{m}$ by Exercise 1.4.8 and as $\mathbf{I}(X) \subseteq \mathfrak{m} \subsetneq A$ we have $\varnothing \neq \mathbf{V}(\mathfrak{m}) \subseteq X$. Assume $V \subseteq \mathbf{V}(\mathfrak{m})$ is a proper closed subset then we have $\mathfrak{m} \subsetneq \mathbf{I}(V) \subseteq A$. As $\mathfrak{m}$ is maximal this forces $\mathbf{I}(V) = A$ so $V = \varnothing$ which implies $\mathbf{V}(\mathfrak{m}) = \{x\}$ for some $x \in X$. In particular, we have $\mathfrak{m} + \mathbf{I}(X) = \mathbf{I}_X(\{x\}) = \mathfrak{m}_x$ so the map is surjective. ■

We state here without proof the following generalisations of results concerning affine n-space. Their proof is an easy exercise using 1.4.4.

Proposition 1.4.11. *Assume $X \in \mathcal{C}(\mathbb{A}^n)$ is an algebraic set then the following hold:*

(a) $\mathbf{V}_X(\mathbf{I}_X(V)) = \overline{V}$ for any subset $V \subseteq X$,

(b) $\mathbf{I}_X(\mathbf{V}_X(I)) = \sqrt{I}$ for any ideal $I \in \mathcal{I}(K[X])$,

(c) the maps $\mathbf{V}_X$ and $\mathbf{I}_X$ define order reversing inverse bijections $\mathcal{C}(X) \to \mathcal{R}(K[X])$.

1.4.12. Although we have shown that the Zariski topology admits certain nice topological features (c.f., Proposition 1.2.20) it is not true that the Zariski topology on X is Hausdorff. Indeed, in the case of $\mathbb{A}^1$ every proper closed subset is finite (c.f., Example 1.2.6) so any two open subsets of $\mathbb{A}^1$ must intersect non-trivially. To get a better idea of the open subsets we introduce the most basic of such sets.

Definition 1.4.13. For any non-zero $f \in K[X]$ we set

$$X_f := \{x \in X \mid f(x) \neq 0\},$$

which we call a *principal open set* of X.

1.4.14. Clearly $X_f \subseteq X$ is an open subset of X as it is the complement of $\mathbf{V}_X(\{f\})$. It is clear that we have $X_{fg} = X_f \cap X_g$ for any $f, g \in K[X]$ and $X_{f^n} = X_f$ for any $n \geqslant 1$. The following now shows that the set of principal open subsets of X form a basis for the Zariski topology on X.

Lemma 1.4.15. *For any algebraic set $X \in \mathcal{C}(\mathbb{A}^n)$ the following hold:*

(a) if $f, g \in K[X]$ satisfy $X_f \subseteq X_g$ then $f \in \sqrt{\langle g \rangle}$,

(b) any open subset of X is a finite union of principal open sets.

Proof. (a). Now clearly we have

$$X_f \subseteq X_g \Rightarrow \mathbf{V}(\{g\}) \subseteq \mathbf{V}(\{f\}) \Rightarrow \mathbf{I}(\mathbf{V}(\{f\})) \subseteq \mathbf{I}(\mathbf{V}(\{g\})) \Rightarrow \sqrt{\langle f \rangle} \subseteq \sqrt{\langle g \rangle}$$

hence $f \in \sqrt{\langle g \rangle}$.

(b). Assume $O \subseteq X$ is open then $X \backslash O$ is closed so it is equal to some algebraic set $\mathbf{V}(I) \in \mathcal{C}(X)$. By Exercise 1.2.17 and Theorem 1.2.18 we have $I = \langle f_1, \dots, f_r \rangle$ is finitely generated so

$$\mathbf{V}(I) = \mathbf{V}\left(\sum_{i=1}^{r} \langle f_i \rangle\right) = \bigcap_{i=1}^{r} \mathbf{V}(\langle f_i \rangle).$$

Taking complements we have $O = \bigcup_{i=1}^{r} X_{f_i}$ as desired. ■

1.5 Regular Functions and Ringed Spaces

1.5.1. So far we have tried to study an algebraic set $X \in \mathcal{C}(\mathbb{A}^n)$ together with its affine algebra $K[X]$, which we viewed as functions on X given by polynomials. We could progress further without introducing any more machinery. However, to study X locally (for example around a point) it will be convenient to introduce a sheaf of functions on X. This not only associates to X a set of functions (which will turn out to be $K[X]$) but also associates to every open set of X a set of suitably defined functions. Such machinery also allows us the flexibility to study more complicated geometric objects such as projective varieties, which we will introduce later. Roughly speaking, projective varieties are certain topological spaces which locally look like $\mathbb{A}^n$ (in complete analogy to a manifold which locally looks like $\mathbb{R}^n$). The following makes precise the meaning of suitably defined.

Definition 1.5.2. If O is an open subset of X then a function $f \in \mathrm{Maps}(O, K)$ is called *regular in* $x \in X$ if there are functions $g, h \in K[X]$ and an open neighbourhood $U \subseteq O \cap X_h$ of x such that $f = g/h$ on U. We say f is *regular* if it is regular in all points of O.

Remark 1.5.3. In particular, this means that f is regular in x if it is a rational function on an open neighbourhood containing x. Note that our definition here makes sense because the assumption $U \subseteq O \cap X_h$ ensures that $h(y) \neq 0$ for all $y \in U$.

1.5.4. For any open set U of X we will denote by $\mathcal{O}_X(U) \subseteq \mathrm{Maps}(U, K)$ the K-algebra consisting of all the regular functions in U. The map $\mathcal{O}_X$ satisfies the following properties (whose verification we leave to the reader):

(S1) For any two open sets $U, V \subseteq X$ satisfying $U \subseteq V$ we have a restriction map $\mathrm{res}_{U,V} : \mathcal{O}_X(V) \to \mathcal{O}_X(U)$. In our setting this is given by $\mathrm{res}_{V,U}(f) = f \circ \iota_{U,V}$ where $\iota_{U,V} : U \hookrightarrow V$ is the natural inclusion map.

(S2) $\mathrm{res}_{U,U}$ is the identity for any open set $U \subseteq X$.

(S3) $\mathrm{res}_{W,V} \circ \mathrm{res}_{V,U} = \mathrm{res}_{W,U}$ for any sequence of nested open sets $U \subseteq V \subseteq W \subseteq X$.

(S4) Assume $U \subseteq X$ is an open subset and $U = \bigcup_{\lambda \in \Lambda} U_\lambda$ is an open cover of U. Let us further assume that we have a family of functions $\{f_\lambda \mid f_\lambda \in \mathcal{O}_X(U_\lambda)\}$ such that whenever $U_\lambda \cap U_\mu \neq \varnothing$ we have $\mathrm{res}_{U_\lambda, U_\lambda \cap U_\mu}(f_\lambda) = \mathrm{res}_{U_\mu, U_\lambda \cap U_\mu}(f_\mu)$. Then there exists a unique function $f \in \mathcal{O}_X(U)$ such that $f_\lambda = \mathrm{res}_{U,U_\lambda}(f)$ for all $\lambda \in \Lambda$.

The last property may seem obtuse but it is quite natural. Indeed, it merely states that a locally determined function can be patched together to form a unique regular function on the whole space. In particular, if $\{U_\lambda \mid \lambda \in \Lambda\}$ is an open cover of X (which we may assume to be finite by Proposition 1.2.20) and $f \in \mathcal{O}_X(X)$ is a regular function then the functions $\{f_\lambda \mid \lambda \in \Lambda\}$ with $f_\lambda = \mathrm{res}_{X,U_\lambda}(f)$ uniquely determine f.

Definition 1.5.5. Assume Z is a topological space and $\mathcal{O}_Z$ is a map assigning to every open set U of Z a K-subalgebra $\mathcal{O}_Z(U) \subseteq \mathrm{Maps}(U, K)$. If properties (S1) to (S4) hold then we say $\mathcal{O}_Z$ is a *sheaf of functions* on Z and the pair $(Z, \mathcal{O}_Z)$ is a *ringed space*.

Remark 1.5.6. Property (S4) is normally referred to as the sheaf axiom. If only (S1) to (S3) hold then $\mathcal{O}_Z$ is called a presheaf. Any presheaf can be made into a sheaf via the process of sheafification. An alternative definition for a presheaf can be given as follows. Note that one can turn the open sets of Z into a category $\mathcal{U}_Z$ with the hom sets $\mathrm{Hom}_{\mathcal{U}_Z}(U, V)$ being either 0 if $U \not\subseteq V$ or simply $\{\iota_{U,V}\}$ if $U \subseteq V$. In this language a presheaf is simply a contravariant functor $\mathcal{O}_Z : \mathcal{U}_Z \to \mathcal{A}$ where $\mathcal{A}$ is any desired target category. The restriction maps are then simply the images of the inclusion maps under this functor.

Definition 1.5.7. For an algebraic set $X \in \mathcal{C}(\mathbb{A}^n)$ the sheaf of rings $\mathcal{O}_X$ defined above is called the *structure sheaf* of X.

1.5.8. We continue to assume that $X \in \mathcal{C}(\mathbb{A}^n)$ is an algebraic set. Above we have introduced two sets of global functions on X, namely $K[X]$ and $\mathcal{O}_X(X)$. It is clear from the definition that we have an inclusion $K[X] \subseteq \mathcal{O}_X(X)$, in other words any function in the affine algebra is regular. Indeed, we have for any $f \in K[X]$ that $f(x) = f(x)/1(x)$ for all $x \in X$ where $1 \in K[X]$ is the constant function satisfying $1(x) = 1$. In fact, equality holds.

Theorem 1.5.9. *For any algebraic set X we have $K[X] = \mathcal{O}_X(X)$.*

Proof. We need only show that $\mathcal{O}_X(X) \subseteq K[X]$. Assume $f \in \mathcal{O}_X(X)$ is regular then for every $x \in X$ there exist functions $f_x, g_x \in K[X]$ and an open neighbourhood $O_x \subseteq X_{g_x}$ of x such that $\mathrm{res}_{X,O_x}(f) = f_x/g_x$. We claim that we may assume that $O_x = X_{g_x}$. By Lemma 1.4.15(ii) O_x is a union of finitely many principal open sets so we certainaly may assume that $O_x = X_{h_x}$ for some $h_x \in K[X]$. As $X_{h_x} \subseteq X_{g_x}$ we have by Lemma 1.4.15(i) that there exists an integer $n \geqslant 1$ and a function $t_x \in K[X]$ such that

$$h_x^n = g_x t_x \Rightarrow \mathrm{res}_{X,O_x}(f) = f_x t_x / h_x^n.$$

As $X_{h_x^n} = X_{h_x}$ this proves the claim.

Clearly we have $X = \bigcup_{x \in X} O_x$ and by Proposition 1.2.20 there exists a finite subset $\{x_1, \dots, x_r\} \subseteq X$ such that $X = \bigcup_{i=1}^r O_{x_i} = \bigcup_{i=1}^r X_{g_i}$ where $g_i := g_{x_i}$ for all $1 \leqslant i \leqslant r$. Now let $f_i \in K[X]$ be such that $\mathrm{res}_{X,X_{g_i}}(f) = f_i/g_i$. Being defined as the restriction of a common function f we have f_i/g_i and f_j/g_j agree on $X_{g_i} \cap X_{g_j}$ so $f_i g_j - f_j g_i = 0$ on $X_{g_i} \cap X_{g_j}$. However, by definition $g_i g_j$ is identically 0 on the complement $X \setminus (X_{g_i} \cap X_{g_j})$ so we have

$$g_i g_j (f_i g_j - f_j g_i) = 0 \Rightarrow g_j^2 f_i g_i = g_i^2 f_j g_j$$

on X. By the properties of principal open sets mentioned in 1.4.14 we have

$$X = \bigcup_{i=1}^{r} X_{g_i^2} \Rightarrow \varnothing = \bigcap_{i=1}^{r} \mathbf{V}(\langle g_i^2 \rangle) \Rightarrow \varnothing = \mathbf{V}\left(\sum_{i=1}^{r} \langle g_i^2 \rangle \right) \Rightarrow A = \sum_{i=1}^{r} \langle g_i^2 \rangle .$$

In particular, if $b_i \in K[X]$ are such that $\sum_{i=1}^{r} b_i g_i^2 = 1$ then for any $1 \leqslant j \leqslant r$ we have

$$\sum_{i=1}^{r} b_i g_j^2 f_i g_i = \sum_{i=1}^{r} b_i g_i^2 f_j g_j = f_j g_j \sum_{i=1}^{r} b_i g_i^2 = f_j g_j \Rightarrow g_j \left(f_j - \sum_{i=1}^{r} b_i f_i g_i g_j \right) = 0.$$

For any $x \in X_{g_j}$ we thus have

$$f(x) = \frac{f_j(x)}{g_j(x)} = \sum_{i=1}^{r} b_i(x) f_i(x) g_i(x).$$

As the X_{g_j} cover X this proves that $f = \sum_{i=1}^{r} b_i f_i g_i \in K[X]$ as desired. ■

1.5.10. To progress further we need to develop some terminology concerning ringed spaces; for this we will assume that $(Z, \mathcal{O}_Z)$ is a ringed space. If $Y \subseteq Z$ is a subset of Z then we may view Y as a topological space with the induced topology. We now consider how to naturally complete this topological space to a ringed space $(Y, \mathcal{O}_Y)$. For any open set U of Y we define $\mathcal{O}_Y(U)$ to be the set of all functions $f \in \mathrm{Maps}(U, K)$ satisfying the following property:

- there exists a family of open sets $\{U_\lambda \mid \lambda \in \Lambda\} \subseteq X$ such that $U \subseteq \bigcup_{\lambda\in\Lambda} U_\lambda$ and a function $f_\lambda \in \mathcal{O}_X(U_\lambda)$ such that $\mathrm{res}_{U_\lambda, U\cap U_\lambda}(f_\lambda) = \mathrm{res}_{U_\lambda, U\cap U_\lambda}(f)$.

One readily checks that with this definition $\mathcal{O}_Y$ is a sheaf of rings on Y and we call the corresponding ringed space $(Y, \mathcal{O}_Y)$ the induced ring space on Y.

Exercise 1.5.11. If $Y \subseteq X$ is an open set in X then for any open set $U \subseteq Y$ we have $\mathcal{O}_Y(U) = \mathcal{O}_X(U)$.

1.5.12. Now let us assume that $(W, \mathcal{O}_W)$ is also a ringed space. Note that any map $\varphi : W \to Z$ induces a restriction map $\varphi_U^* : \mathrm{Maps}(U, K) \to \mathrm{Maps}(\varphi^{-1}(U), K)$ for any subset $U \subseteq Z$ given by $\varphi_U^*(f) = f \circ \varphi$.

Definition 1.5.13. We say a continuous map $\varphi : W \to Z$ of topological spaces is a *morphism of ringed spaces* if $\varphi_U^*(\mathcal{O}_Z(U)) \subseteq \mathcal{O}_W(\varphi^{-1}(U))$ for all open sets $U \subseteq Z$. We say φ is an isomorphism if it is a homeomorphism of topological spaces and φ_U^* is an isomorphism of K-algebras for each open set $U \subseteq Z$.

Exercise 1.5.14. Assume $\varphi : W \to Z$ is a continuous map. For any open set $U \subseteq Z$ define $(\varphi_* \mathcal{O}_W)(U) = \mathcal{O}_W(\varphi^{-1}(U))$. Show that $\varphi_* \mathcal{O}_W$ defines a sheaf of rings on Z called the *direct image sheaf*.

Exercise 1.5.15. Assume $\varphi : W \to Z$ is a morphism of ringed spaces. Show that the map $\varphi^* : \mathcal{O}_Z \to \varphi_*\mathcal{O}_Z$, which assigns to each open set $U \subseteq Z$ the map $\varphi^*_U : \mathcal{O}_Z(U) \to \mathcal{O}_W(\varphi^{-1}(U))$, is a morphism of sheaves. In other words, show that the diagram

$$\begin{tikzcd}
\mathcal{O}_Z(U) \arrow[r, "\varphi^*_U"] \arrow[d, "\mathrm{res}_{U,V}"'] & \mathcal{O}_W(\varphi^{-1}(U)) \arrow[d, "\mathrm{res}_{\varphi^{-1}(U),\varphi^{-1}(V)}"] \\
\mathcal{O}_Z(V) & \mathcal{O}_W(\varphi^{-1}(V)) \arrow[l, "\varphi^*_V"]
\end{tikzcd}$$

is commutative for any open set V of Z contained in U. Deduce that a continuous map $\varphi : W \to Z$ is a morphism of rings if and only if $\varphi^* : \mathcal{O}_Z \to \varphi_*\mathcal{O}_Z$ is a morphism of sheaves.

Definition 1.5.16. An *affine variety* is a ringed space which is isomorphic to $(X, \mathcal{O}_X)$ for some algebraic set $X \in \mathcal{C}(\mathbb{A}^n)$, where $\mathcal{O}_X$ is the structure sheaf on X.

1.5.17. We consider a morphism of affine varieties $\varphi : X \to Y$ simply to be a morphism of ringed spaces. Now, as φ is a morphism of ringed spaces we have φ induces a K-algebra homomorphism $\mathcal{O}_Y(Y) \to \mathcal{O}_X(X)$ and hence a K-algebra homomorphism $\varphi^* : K[Y] \to K[X]$ which we call the *comorphism* of φ. Note that taking comorphisms is contravariant in the sense that $(\varphi \circ \psi)^* = \psi^* \circ \varphi^*$ for any two morphisms of affine varieties $\psi : X \to Y$ and $\varphi : Y \to Z$.

Lemma 1.5.18. *We have a bijection $X \to \mathrm{Hom}_{K-\mathrm{alg}}(K[X], K)$ given by $x \mapsto \varepsilon_x$ where ε_x is the evaluation homomorphism given by $\varepsilon_x(f) = f(x)$ for all $f \in K[X]$.*

Proof. Assume $\varepsilon_x = \varepsilon_y$ for some $x, y \in X$ then clearly we have $\mathbf{I}_X(\{x\}) = \mathbf{I}_X(\{y\})$ and so by Proposition 1.4.11 this gives

$$\{x\} = \mathbf{V}_X(\mathbf{I}_X(\{x\})) = \mathbf{V}_X(\mathbf{I}_X(\{y\})) = \{y\}.$$

In particular, $x = y$ so the map is injective. Now assume $\gamma : K[X] \to K$ is a K-algebra homomorphism then $\mathrm{Ker}(\gamma)$ is a maximal ideal; by Lemma 1.4.10 we therefore have $\mathrm{Ker}(\gamma) = \mathfrak{m}_x$ for some $x \in X$. Note that there is only one non-zero K-algebra homomorphism $f : K[X] \to K$, which is necessarily an isomorphism. As both γ and ε_x factor uniquely through $K[X]/\mathfrak{m}_x$ we must have $\gamma = f \circ p = \varepsilon_x$ where $p : K[X] \to K[X]/\mathfrak{m}_x$ is the natural projection map. This shows the map is bijective. ■

Proposition 1.5.19. *Given a K-algebra homomorphism $\psi : K[Y] \to K[X]$ we have a unique morphism of affine varieties $\psi^* : X \to Y$ such that $\varepsilon_x \circ \psi = \varepsilon_{\psi^*(x)}$ for all $x \in X$. In particular, we have $(\psi^*)^* = \psi$.*

Proof. For any $x \in X$ we have $\varepsilon_x \circ \psi$ is a K-algebra homomorphism $K[Y] \to K$ so we have $\varepsilon_x \circ \psi = \varepsilon_{\psi^*(x)}$ for a unique $\psi^*(x) \in Y$ by Lemma 1.5.18. Equivalently we have $\psi^*(x)$ is the unique element such that $\mathfrak{m}_{\psi^*(x)} = \psi^{-1}(\mathfrak{m}_x)$. Consequently we have that

$$\psi(g)(x) = 0 \Leftrightarrow g(\psi^*(x)) = 0 \tag{1.5.20}$$

for all $g \in K[Y]$. We now need to show that the map $\psi^* : X \to Y$ is continuous. However, (1.5.20) shows that for any subset $V \subseteq Y$ we have

$$\psi(\mathbf{I}_Y(V)) \subseteq \mathbf{I}_X(\psi^{*-1}(V)) \Rightarrow \mathbf{V}_X(\mathbf{I}_X(\psi^{*-1}(V))) \subseteq \mathbf{V}_X(\psi(\mathbf{I}_Y(V))).$$

Inspecting the right hand side we see that

$$\begin{aligned}\mathbf{V}_X(\psi(\mathbf{I}_Y(V))) &= \{x \in X \mid \psi(g)(x) = 0 \text{ for all } g \in \mathbf{I}_Y(V)\}\\ &= \{x \in X \mid g(\psi^*(x)) = 0 \text{ for all } g \in \mathbf{I}_Y(V)\}\\ &\subseteq \psi^{*-1}(\mathbf{V}_Y(\mathbf{I}_Y(V))).\end{aligned}$$

By Proposition 1.4.11(i) this gives

$$\psi^{*-1}(V) \subseteq \overline{\psi^{*-1}(V)} \subseteq \psi^{*-1}(\overline{V}),$$

so if V is closed then so is $\psi^{*-1}(V)$, which means ψ^* is continuous. The fact that ψ^* defines a morphism of ringed spaces is left as an exercise.

By the equality $\varepsilon_x \circ \psi = \varepsilon_{\psi*(x)}$ we have $\psi(f)(x) = f(\psi^*(x))$ for any $f \in K[X]$ and for all $x \in X$ hence $\psi(f) = f \circ \psi^*$ for any $f \in K[X]$. This shows that $(\psi^*)^* = \psi$. ■

This result has the following nice consequences, which are examples of the central idea that geometric notions can be phrased in terms of algebra.

Corollary 1.5.21. *Let X and Y be affine varieties then a map of sets $\varphi : X \to Y$ is a morphism of varieties if and only if $\varphi = \psi^*$ for some algebra homomorphism $\psi : K[Y] \to K[X]$.*

Corollary 1.5.22. *A morphism of affine varieties $\varphi : X \to Y$ is an isomorphism if and only if the comorphism $\varphi^* : K[Y] \to K[X]$ is an isomorphism.*

Proof. The if direction is clear so assume $\varphi^* : K[Y] \to K[X]$ is an isomorphism then $(\varphi^*)^{-1} : K[X] \to K[Y]$ is a K-algebra homomorphism. In particular, by Proposition 1.5.19 there is a morphism of varieties $\psi : Y \to X$ such that $\psi^* = (\varphi^*)^{-1}$. As $\varphi^* \circ \psi^* = (\psi \circ \varphi)^*$ is the identity we must have $\psi \circ \varphi$ is the identity by Proposition 1.5.19 so φ is an isomorphism. ■

Exercise 1.5.23. If X is an affine variety and $V \subseteq X$ is a closed set then show that the natural inclusion map $\iota : V \to X$ is a morphism of varieties.

Exercise 1.5.24. Assume $X \in \mathcal{C}(\mathbb{A}^n)$ and $Y \in \mathcal{C}(\mathbb{A}^m)$ are algebraic sets and $\varphi : X \to Y$ is a morphism of varieties. Show that there exist polynomial functions $\varphi_1, \dots, \varphi_m \in K[X_1, \dots, X_n]$ such that $\varphi(x) = (\varphi_1(x), \dots, \varphi_m(x))$ for all $x \in X$.

1.5.25. At the beginning of this section we mentioned that introducing the structure of a sheaf on X would allow us to study X locally at a point. We now make this statement more precise. For each $x \in X$ we denote by $\mathcal{O}_{X,x}$ the stalk of the structure sheaf $\mathcal{O}_X$ at x. Formally this is defined to be the direct limit

$$\mathcal{O}_{X,x} = \varinjlim_{U} \mathcal{O}_X(U)$$

where the limit is taken over all open subsets $U \subseteq X$ containing x. A more concrete way to see this limit is as follows. Consider the union $\mathcal{F}_x = \bigcup_{U \subseteq X} \mathcal{O}_X(U)$ of all open subsets of X containing x. We define an equivalence relation $\sim$ on $\mathcal{F}_x$ by setting $f \sim g$ whenever $f \in \mathcal{O}_X(U)$ and $g \in \mathcal{O}_X(V)$ are such that $V \subseteq U$ and $\mathrm{res}_{V,U}(g) = f$. The stalk $\mathcal{O}_{X,x}$ is then the set of equivalence classes $\mathcal{F}_x/\sim$. It is clear that $\mathcal{O}_{X,x}$ is naturally the set of functions $f : X \to K$ that are regular in $x \in X$, i.e., regular in an open neighbourhood of x.

Definition 1.5.26. Assume R is a ring then we say R is a *local ring* if it has a unique maximal ideal $\mathfrak{m}$.

Lemma 1.5.27. *$\mathcal{O}_{X,x}$ is a local ring with unique maximal ideal $\mathfrak{m}_x$.*

Proof. Assume $f \in \mathcal{O}_X(U)$ for some open neighbourhood U of x then we may write $f = g/h$ for some $g, h \in K[X]$ and $U \subseteq X_h$. If $f(x) \neq 0$ then we have $g(x) \neq 0$ so the open set $V = U \cap X_g$ is non-empty and we have $f^{-1} = h/g \in \mathcal{O}_X(V)$. This shows that every non-invertible element of $\mathcal{O}_{X,x}$ lies in $\mathfrak{m}_x$, hence $\mathcal{O}_{X,x}$ is a local ring. ■

1.5.28. Assume R is a ring and $S \subseteq R$ is a multiplicatively closed subset, i.e., $1 \in S$ and S is closed under multiplication. We define a relation $\sim$ on $R \times S$ by setting

$$(a, s) \sim (b, t) \Leftrightarrow (at - bs)u = 0 \text{ for some } u \in S,$$

which is easily checked to be an equivalence relation. We denote by a/s the equivalence class of (a, s) and denote by $S^{-1}R$ the set of all such equivalence classes. The set $S^{-1}R$ is given a ring structure by setting

$$a/s + b/t = (at + bs)/st \qquad \text{and} \qquad (a/s)(b/t) = ab/st$$

for all $a/s, b/t \in S^{-1}R$ and we call $S^{-1}R$ the ring of fractions of R with respect to S. If $\mathfrak{p} \in \operatorname{Spec}(R)$ is a prime ideal of R then we denote by $R_{\mathfrak{p}}$ the ring of fractions $S^{-1}R$ where $S = R \setminus \mathfrak{p}$. We call $R_{\mathfrak{p}}$ the *localisation* of R at $\mathfrak{p}$.

Definition 1.5.29. If R is an integral domain then we call the localisation $R_{\langle 0 \rangle}$ of R at $\langle 0 \rangle$ the *field of fractions* of R.

Exercise 1.5.30. Show that for any ring R and any prime ideal $\mathfrak{p} \in \operatorname{Spec}(R)$ we have $R_{\mathfrak{p}}$ is a local ring.

Exercise 1.5.31. Assume $(X, \mathcal{O}_X)$ is an affine variety then show that $\mathcal{O}_{X,x}$ is isomorphic to the localisation $K[X]_{\mathfrak{m}_x}$ of $K[X]$ at $\mathfrak{m}_x$.

Exercise 1.5.32. Let $\mathcal{A}_K$ be the category whose objects are affine K-algebras and whose homomorphisms consist of all K-algebra homomorphisms. Furthermore, let $\mathcal{V}_K$ be the category consisting of all affine varieties over K whose homomorphisms consist of all morphisms of varieties. Show that we have a contravariant equivalence of categories $\mathcal{A}_K \to \mathcal{V}_K$.

1.6 Products

From now on $\mathbb{A}^n$ will denote the affine variety determined by the algebraic set K^n.

1.6.1. Given two affine varieties X and Y we wish to show that a product structure $X \times Y$ exists. The notion of a product is a categorical construction and is defined in the following way. We say an affine variety $X \times Y$ is the product of X and Y if there exist morphisms $p_X : X \times Y \to X$ and $p_Y : X \times Y \to Y$ such that for every affine variety W and every pair of morphisms $f_X : W \to X$ and $f_Y : W \to Y$ there exists a unique morphism $f : W \to X \times Y$ making the following diagram commute

$$\begin{tikzcd}
 & W \arrow[dl, "f_X"'] \arrow[d, "f"] \arrow[dr, "f_Y"] & \\
X & X \times Y \arrow[l, "p_X"] \arrow[r, "p_Y"'] & Y
\end{tikzcd}$$

This is clearly a universal property so when the product $X \times Y$ exists it is unique.

1.6.2. Assume for a moment that the product $X \times Y$ exists then we may consider its affine algebra $K[X \times Y]$. Using Proposition 1.5.19 we see the above property can be translated as follows. There exist K-algebra homomorphisms $p_X^* : K[X] \to K[X \times Y]$ and $p_Y^* : K[Y] \to K[X \times Y]$ such that for every affine algebra A and every pair of homomorphisms $g_X : K[X] \to A$ and $g_Y : K[Y] \to A$ there exists a unique homomorphism $g : K[X \times Y] \to A$ making the following diagram commute

$$\begin{tikzcd} & A & \\ K[X] \arrow[ur, "g_X"] \arrow[r, "p_X^*"] & K[X \times Y] \arrow[u, "g"] & K[Y] \arrow[ul, "g_Y"'] \arrow[l, "p_Y^*"'] \end{tikzcd}$$

If we drop our assumption that A is an affine algebra and instead just take A to be any K-algebra then we would expect $K[X \times Y]$ to be the tensor product $K[X] \otimes_K K[Y]$ (see the proof of Theorem 1.6.4). However, apriori it's not clear that the tensor product of affine algebras is again an affine algebra. The following shows this is the case.

Lemma 1.6.3. *The tensor product $K[X] \otimes_K K[Y]$ is an affine algebra. Furthermore, if $K[X]$ and $K[Y]$ are integral domains then so is $K[X] \otimes_K K[Y]$.*

Proof. We have to show that $K[X] \otimes_K K[Y]$ is finitely generated and reduced. An easy exercise shows that if $\{a_1, \dots, a_r\} \subseteq K[X]$ and $\{b_1, \dots, b_s\} \subseteq K[Y]$ are bases then $\{a_i \otimes b_j \mid 1 \leqslant i \leqslant r \text{ and } 1 \leqslant j \leqslant s\} \subseteq K[X] \otimes_K K[Y]$ is also a basis. So we need only show that $K[X] \otimes_K K[Y]$ is reduced.

Now assume $d = \sum_{j=1}^s d_j \otimes b_j$ is a nilpotent element for some $d_j \in K[X]$ (it is clear that any such element may be written this way). For any $x \in X$ we have the map $\pi_x : K[X] \times K[Y] \to K[Y]$ given by $\pi_x(f, g) = \varepsilon_x(f)g = f(x)g$ is a K-bilinear map so it factors uniquely through a K-linear map $\pi_x : K[X] \otimes_K K[Y] \to K$. This is in fact a K-algebra homomorphism so

$$\pi_x(d) = \sum_{j=1}^s d_j(x) b_j$$

is a nilpotent element in $K[Y]$. As $K[Y]$ is reduced we must have $\pi_x(d) = 0$ and as the b_j are linearly independent this implies $d_j(x) = 0$ for all j. In particular, $d_j \in \mathbf{I}_X(X)$ so $d_j = 0$ by Proposition 1.4.11 which implies $d = 0$ so the tensor product is reduced.

Now assume $K[X]$ and $K[Y]$ are integral domains. Let $d = \sum_{j=1}^s d_j \otimes b_j$ and $e = \sum_{j=1}^s e_j \otimes b_j$ be such that

$$de = \sum_{j=1}^s \sum_{k=1}^s (d_j \otimes b_j)(e_k \otimes b_k) = \sum_{j=1}^s \sum_{k=1}^s d_j e_k \otimes b_j b_k = 0.$$

Again, applying π_x we have

$$\pi_x(de) = \sum_{j=1}^s \sum_{k=1}^s d_j(x) e_k(x) b_j b_k = \left(\sum_{j=1}^s d_j(x) b_j \right) \left(\sum_{k=1}^s e_k(x) b_k \right) = 0.$$

However $K[Y]$ is an integral domain so we either have $\sum_{j=1}^s d_j(x) b_j = 0$ or $\sum_{k=1}^s e_k(x) b_k = 0$. By the linear independence of the basis we must therefore have $d_j(x) = 0$ for all $1 \leqslant j \leqslant s$ or

$e_k(x) = 0$ for all $1 \leqslant k \leqslant s$. The same trick as before now implies that either $d = 0$ or $e = 0$ so $K[X] \otimes_K K[Y]$ is an integral domain. ■

Theorem 1.6.4. *If X and Y are affine varieties then the following hold:*

(a) a product structure $X \times Y$ exists and is unique up to isomorphism,

(b) $K[X \times Y] \cong K[X] \otimes_K K[Y]$,

(c) if X and Y are irreducible then so is $X \times Y$.

Proof. Firstly, if (a) and (b) hold then (c) follows immediately from Lemma 1.6.3 and Proposition 1.3.7. So let us prove (a) and (b).

By Lemma 1.6.3 the tensor product $K[X] \otimes_K K[Y]$ is an affine algebra so to prove (a) and (b) it suffices to show that $K[X] \otimes_K K[Y]$ satisfies the universal property in 1.6.2. In this case we define the maps p_X^* and p_Y^* by $p_X^*(a) = a \otimes 1_{K[Y]}$ and $p_Y^*(b) = 1_{K[X]} \otimes b$. Now assume (A, g_X, g_Y) are as in 1.6.2. We define $t : K[X] \times K[Y] \to A$ (where this is the Cartesian product of sets) by $t(a, b) = g_X(a)g_Y(b)$. The map t is clearly K-bilinear so it factors uniquely through a K-linear map $g : K[X] \otimes_K K[Y] \to A$ which satisfies

$$g\left(\sum_{i=1}^{n} a_i \otimes b_i\right) = \sum_{i=1}^{n} g_X(a_i)g_Y(b_i)$$

(see [AM69, 2.12]). We leave it as an exercise to show that g defines a unique K-algebra homomorphism making the diagram in 1.6.2 commute. ■

1.6.5. Let us choose generating sets $\{f_1, \dots, f_n\} \subseteq K[X]$ and $\{g_1, \dots, g_m\} \subseteq K[Y]$ then we have a natural isomorphism of K-algebras

$$\gamma : K[f_1, \dots, f_n, g_1, \dots, g_m] \to K[X] \otimes K[Y]$$

defined by $\gamma(f_i) = f_i \otimes 1$ and $\gamma(g_j) = 1 \otimes g_j$. According to Lemma 1.4.10 every maximal ideal of $K[f_1, \dots, f_n, g_1, \dots, g_m]$ is of the form

$$\langle f_1 - a_1, \dots, f_n - a_n, g_1 - b_1, \dots, g_m - b_m \rangle$$

for some $a_i, b_j \in K$. Applying γ to this ideal we obtain the maximal ideal

$$\langle f_1 - a_1, \dots, f_n - a_n \rangle \otimes K[Y] + K[X] \otimes \langle g_1 - b_1, \dots, g_m - b_m \rangle$$

where for any ideals $I \in \mathcal{I}(K[X])$ and $J \in \mathcal{I}(K[Y])$ we denote by $I \otimes J \in \mathcal{I}(K[X] \otimes K[Y])$ the ideal generated by the simple tensors $x \otimes y$ with $x \in I$ and $y \in J$. Applying Lemma 1.4.10 we have the following.

Lemma 1.6.6. *The map $\Phi : \{(x, y) \mid x \in X \text{ and } y \in Y\} \to \mathrm{MSpec}(K[X] \otimes K[Y])$ defined by*

$$\Phi(x, y) = \mathfrak{m}_x \otimes K[Y] + K[X] \otimes \mathfrak{m}_y$$

is a bijection. In particular, we may identify the product $X \times Y$ of X and Y as a set with the Cartesian product.

Exercise 1.6.7. Identify $X \times Y$ with the Cartesian product of sets. Show that the comorphisms of the natural inclusion maps $p_X^* : K[X] \to K[X] \otimes K[Y]$ and $p_Y^* : K[Y] \to K[X] \otimes K[Y]$ are the natural projection maps $p_X : X \times Y \to X$ and $p_Y : X \times Y \to Y$.

Exercise 1.6.8. Identify, as sets, the affine space $\mathbb{A}^2$ with the Cartesian product $\mathbb{A}^1 \times \mathbb{A}^1$. Show that the Zariski topology on $\mathbb{A}^2$ is finer than the product topology on $\mathbb{A}^1 \times \mathbb{A}^1$ (in the sense that it has more closed sets).

1.7 Varieties and Prevarieties

1.7.1. So far we have focused our attention on affine varieties but during our study of algebraic groups we will encounter other kinds of geometric structures that are not affine varieties, for instance projective and quasi-projective varieties. The notion of a ringed spaced provides the framework in which we can study all of these geometric structures. Although we develop here the general notions and tools of varieties we will leave the study of projective varieties until later.

Definition 1.7.2. Let $(X, \mathcal{O}_X)$ be a ringed space. We say an open set $U \subseteq X$ is an *affine open subset* of X if $(U, \mathcal{O}_X|_U)$ is an affine variety. We say $(X, \mathcal{O}_X)$ is a *prevariety* if it is quasi-compact (in the sense that it satisfies Proposition 1.2.20(c)) and any point of X has an open neighbourhood which is an affine open subset. Or equivalently that X is covered by affine open subsets.

1.7.3. A morphism of prevarieties is simply a morphism of ringed spaces. If $Y \subseteq X$ is a subset of X then we say the induced ringed space $(Y, \mathcal{O}_Y)$ is a *subprevariety* of X if it is a variety. We start by showing that affine varieties are varieties in the sense just defined. By Lemma 1.4.15(b) it suffices to show that every principal open set is affine. Hence the following shows that affine varieties are varieties.

Definition 1.7.4. Assume R is a ring, $f \in R$ is a non-zero element and $S = \{f^m \mid m \geqslant 0\}$. We denote by R_f the ring of fractions $S^{-1}R$ (c.f., 1.5.28) which we call the *localisation of R at f*.

Lemma 1.7.5. *Assume $(X, \mathcal{O}_X)$ is an affine variety and let $X_f \subseteq X$ be a principal open subset of X then $(X_f, \mathcal{O}_X|_{X_f})$ is an affine variety. Furthermore, we have an isomorphism of K-algebras $K[X_f] \cong K[X]_f$.*

Proof. We clearly have an injective K-linear map $K[X]_f \to \mathcal{O}_X(X_f)$ so it suffices to show that this map is surjective. Assume $\Phi \in \mathcal{O}_X(X_f)$ then for any $x \in X_f$ there exist functions $g, h \in K[X]$ and an open neighbourhood $U \subseteq X_f \cap X_h$ of x such that $\Phi = g/h$ on U. Let $U = \bigcup_{i=1}^n X_{f_i}$ be a covering by principal open sets then as $X_{f_i} \subseteq U \subseteq X_f \cap X_h \subseteq X_f$ we have $f_i \in \sqrt{\langle f\rangle}$ by Lemma 1.4.15(a) so $f_i^k \in \langle f\rangle$ for some $k \in \mathbb{N}$. As $X_{f_i} = X_{f_i^k} = X_f$ we have $U = X_f$ so $\Phi = g/h$ on X_f. Furthermore, we have $X_f \subseteq X_f \cap X_h \subseteq X_h$ so we must have $h = f^m$ for some $m \geqslant 1$ by Lemma 1.4.15(a), hence $\mathcal{O}_X(X_f) \cong K[X]_f$.

To show that $(X_f, \mathcal{O}_X|_{X_f})$ is affine we need only show that $\mathcal{O}_X(X_f)$ is an affine algebra. If $\{f_1, \dots, f_n\} \subseteq K[X]$ is a generating set of $K[X]$ then $\mathcal{O}_X(X_f)$ is clearly generated by $\{f_1, \dots, f_n, 1/f\}$. Now assume $g/f^m \in \mathcal{O}_X(X_f)$ is such that $g^k/f^{mk} = 0$ for some $k \geqslant 1$ then $g^k(x) = 0$ for all $x \in X_f$ hence $g(x) = 0$ for all $x \in X_f$. In other words $g/f^m = 0$ on X_f so $\mathcal{O}_X(X_f)$ is reduced, hence affine. ■

1.7.6. Now assume $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ are prevarieties then there exist finite coverings $X = \bigcup_{i=1}^n U_i$ and $Y = \bigcup_{j=1}^m V_j$ by affine open sets. Consider the Cartesian product $X \times Y$ then we have $X \times Y = \bigcup_{i=1}^n \bigcup_{j=1}^m U_i \times V_j$ and each $U_i \times V_j$ is an affine variety by Lemma 1.6.6. We define a topology on $X \times Y$ by specifying that $U \subseteq X \times Y$ is open if $U \cap U_i \times V_j$ is open in $U_i \times V_j$ for all i, j. Furthermore we define $\mathcal{O}_{X\times Y}(U) \subseteq \text{Maps}(U, K)$ to be all $f \in \text{Maps}(U, K)$ such that $f|_{U\cap U_i\times V_j} \in \mathcal{O}_{U_i\times V_j}(U \cap U_i \times V_j)$ for all i, j. With this we have the following (we omit the proof).

Proposition 1.7.7. *$(X \times Y, \mathcal{O}_{X\times Y})$ is a prevariety and is the product of $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ in the categorical sense of 1.6.1.*

1.7.8. The category of all prevarieties is often too big to desirable conclusions about its objects. So we must somehow limit how the open affine subsets can be glued together. With this regard, if X is a prevariety then we denote by Δ_X the image of the map $i_X : X \to X \times X$ given by $i_X(x) = (x, x)$. Note that Δ_X is naturally a topological space with the induced topology.

Lemma 1.7.9. *Let $(X, \mathcal{O}_X)$ be a prevariety then the map i_X is a homeomorphism onto its image. Furthermore, if $(X, \mathcal{O}_X)$ is an affine variety then the image Δ_X of i_X is closed in $X \times X$.*

Proof. Let $X = \bigcup_{i=1}^n U_i$ be a covering by finitely many affine open sets then $\Delta_X = \bigcup_{i=1}^n U_i \times U_i$. Assume $O \subseteq X$ is an open set. If $i_X(O\cap U_i) = i_X(O)\cap i_X(U_i)$ is an open set for each i then $i_X(O)$ is open in Δ_X by the definition of the topology on Δ_X. In particular, it is sufficient to show that $i_X|_{U_i}$ is a homeomorphism for each i so we may assume that X is affine.

We have a K-bilinear map $\gamma : K[X] \times K[X] \to K[X]$ given by $\gamma(f, g) = fg$ which factors uniquely through the tensor product $\gamma : K[X]\otimes K[X] \to K[X]$. This is a K-algebra homomorphism such that

$$\gamma\left(\sum_{i=1}^n f_i \otimes g_i\right) = \sum_{i=1}^n f_i g_i.$$

It is clear that $\text{Ker}(\gamma) = \mathbf{I}_{X\times X}(\Delta_X)$ and $i_X = \gamma^*$ so i_X is a morphism by Corollary 1.5.21. A similar argument to the one used in 1.6.5 shows that $\text{Ker}(\gamma)$ is generated by the set $\{f \otimes 1 - 1 \otimes f \mid f \in K[X]\}$. In particular, we must have $\Delta_X = \mathbf{V}_{X\times X}(\mathbf{I}_{X\times X}(\Delta_X))$ so Δ_X is closed in $X \times X$. As γ is surjective it induces an isomorphism $K[\Delta_X] \to K[X]$ so i_X is a homeomorphism. ■

Definition 1.7.10. A prevariety $(X, \mathcal{O}_X)$ is called a *variety* if Δ_X is closed in $X\times X$. This condition is referred to as the *separation axiom*.

Exercise 1.7.11. Show that a topological space X is Hausdorff if and only if the diagonal $\Delta_X \subseteq X \times X$ is closed in the product topology.

Lemma 1.7.12. *Assume X is a variety and Y is a prevariety.*

(a) If $\phi : Y \to X$ is a morphism then the graph $\Gamma_\phi = \{(y, \phi(y)) \mid y \in Y\}$ of ϕ is closed in $Y \times X$.

(b) If $\phi, \psi : Y \to X$ are two morphisms which coincide on a dense set of Y then $\phi = \psi$.

Proof. (a). Consider the map $\varphi : Y \times X \to X \times X$ given by $(y, x) \mapsto (\phi(y), x)$ then we have

$$\Gamma_\phi = \varphi^{-1}(\Delta_X) = \{(y, x) \in Y \times X \mid \phi(y) = x\}.$$

As ϕ is a morphism we have φ is continuous so Γ_ϕ is closed.

(b). As ϕ and ψ are morphisms we have a continuous map $\varphi : Y \to X \times X$ given by $\varphi(y) = (\phi(y), \psi(y))$. As before we have

$$\varphi^{-1}(\Delta_X) = \{y \in Y \mid \phi(y) = \psi(y)\} \subseteq Y$$

is a closed set because X is a variety. By assumption $\varphi^{-1}(\Delta_X)$ is dense so must be the whole of Y. ■

We note for later the following useful characterisation of varieties, which we give without proof.

Proposition 1.7.13. *Let X be a prevariety and $X = \bigcup_{i=1}^n U_i$ be a covering by affine open sets then X is a variety if and only if the following hold: for all i, j the intersection $U_i \cap U_j$ is an affine open set and the images of the restriction maps $\mathrm{res}_{U_i, U_i \cap U_j}$ and $\mathrm{res}_{U_j, U_i \cap U_j}$ generate $\mathcal{O}_X(U_i \cap U_j)$.*

1.8 Dimension

1.8.1. Assume X is an *irreducible* variety and recall from Corollary 1.3.4 that any non-empty open set is also irreducible. Now assume X is affine then by Proposition 1.3.7 the affine algebra $K[X]$ is an integral domain. In particular, we may form its field of fractions (c.f., Definition 1.5.29) which we denote by $\mathbb{A}(X)$. With this the following makes sense.

Lemma 1.8.2. *If X is an irreducible variety then $\mathbb{A}(U) \cong \mathbb{A}(V)$ for any two non-empty affine open subsets $U, V \subseteq X$.*

Proof. First, let us assume that X is affine and $X_f \subseteq X$ is a principal open set of X. By Lemma 1.7.5 and Theorem 1.5.9 we have X_f is affine and $K[X_f] \cong K[X]_f$. From this one sees easily that $\mathbb{A}(X_f) \cong \mathbb{A}(X)$. As the principal open sets form a basis for the topology on X this implies $\mathbb{A}(U) \cong \mathbb{A}(X)$ for any open set U.

Now assume X is any irreducible variety and let $X = \bigcup_{i=1}^n U_i$ be a covering by affine open sets. The irreducibility of X forces the intersection $U_i \cap U_j$ to be non-empty so the function fields $\mathbb{A}(U_i)$ and $\mathbb{A}(U_j)$ are isomorphic. From this the statement follows. ■

1.8.3. Assume $E \subseteq F$ is a field extension and $S \subseteq F$ is any subset. We say S is an *algebraically independent set* over E if for any subset $\{s_1, \dots, s_n\} \subseteq S$ there exists no non-zero polynomial $P \in E[X_1, \dots, X_n]$ such that $P(s_1, \dots, s_n) = 0$. We then define the transcendence degree of the extension $E \subseteq F$ to be the maximal cardinality of any subset of F which is algebraically independent over E. With this in hand we have the following notion of dimension.

Definition 1.8.4. If X is an irreducible variety then we define the dimension of X to be the transcendence degree of the extension $K \subseteq \mathbb{A}(X)$, which we denote by $\dim(X)$. For any variety X we define $\dim(X) = \max\{\dim(X_1), \dots, \dim(X_n)\}$ where $X_1, \dots, X_n$ are the irreducible components of X.

Exercise 1.8.5. Show that $\dim(\mathbb{A}^n) = n$.

Proposition 1.8.6. *If X is an irreducible variety then for any proper closed non-empty subvariety Y of X we have $\dim Y < \dim X$.*

Proof. We can clearly reduce to the case where X is affine so that $K[X] = K[f_1, \dots, f_n]$. Furthermore, we may assume that Y is irreducible so that $K[Y] = K[X]/\mathfrak{p}$ for some prime ideal $\mathfrak{p} \in \mathrm{Spec}(K[X])$. Let $g_i \in K[Y]$ be the image of f_i under the natural projection map $K[X] \to K[Y]$. Let $d = \dim(X)$ and $e = \dim(Y)$ then, after possibly rearranging the terms, we may assume that $\{g_1, \dots, g_e\}$ is algebraically independent over K. This clearly implies that $\{f_1, \dots, f_e\}$ is algebraically independent over K so $e \leqslant d$.

Now assume for a contradiction that $d = e$ and let $f \in K[X]$ be a non-zero element such that $f \notin \mathfrak{p}$, which exists because $\mathfrak{p} \neq K[X]$. By the definition of dimension there exists a polynomial $P \in K[X_0, \dots, X_e]$ such that $P(f, f_1, \dots, f_e) = 0$. Assume $P = X_0 Q$ for some polynomial $Q \in K[X_1, \dots, X_e]$ then $fQ(f_1, \dots, f_e) = 0$ and we may view this as a relation in $K[X]$ because

$Q(f_1, \ldots, f_e) \in K$. As $K[X]$ is an integral domain this implies that $Q(f_1, \ldots, f_e) = 0$ because $f \neq 0$ but this is a contradiction because $Q \neq 0$ and the f_i are algebraically independent. Hence, we may assume that X_0 does not divide P so the polynomial $H(X_1, \ldots, X_e) := P(0, X_1, \ldots, X_e) \in K[X_1, \ldots, X_e]$ is non-zero. With this we have $H(f_1, \ldots, f_e) = 0$ but again this is a contradiction so $d \neq e$. ■

Corollary 1.8.7. *A variety X is finite if and only if* $\dim(X) = 0$.

Proof. Firstly, we may assume X is irreducible. Secondly, as X is covered by finitely many affine open subsets we may assume X is affine. Now as X is irreducible and $\dim(X) = 0$ we must have X has no proper closed non-empty subvarieties by Proposition 1.8.6. This implies X is a singleton, so we're done. ■

1.9 Some results on morphisms

1.9.1. Recall that we say a morphism of varieties $\phi : X \to Y$ is a *closed embedding* if $\phi(X)$ is closed in Y and the restriction map defines an isomorphism of X onto $\phi(X)$. Furthermore we say ϕ is *dominant* if $\overline{\phi(X)} = Y$. With this in hand we have the following.

Lemma 1.9.2. *Assume $\phi : X \to Y$ is a morphism of affine varieties then the following hold:*

(a) ϕ is a closed embedding if and only if ϕ^* is surjective,

(b) ϕ is dominant if and only if ϕ^* is injective.

Proof. (a). If ϕ is a closed embedding then $\phi = \iota \circ \psi$ where $\psi : X \to \phi(X)$ is an isomorphism and $\iota : \phi(X) \to Y$ is the natural inclusion, which is a morphism by Exercise 1.5.23. Clearly $\iota^* : K[Y] \to K[\phi(X)] = K[Y]/\mathbf{I}_Y(\phi(X))$ is surjective hence so is $\phi^* = (\iota \circ \psi)^* = \psi^* \circ \iota^*$ by Corollary 1.5.22.

If ϕ^* is surjective then we claim that $\phi(X) = \mathbf{V}_Y(\mathrm{Ker}(\phi^*))$. Assume $g \in \mathrm{Ker}(\phi^*)$ then $g(\phi(x)) = \phi^*(g)(x) = 0$ for all $x \in X$ so $\phi(X) \subseteq \mathbf{V}_Y(\mathrm{Ker}(\phi^*))$. Conversely assume $y \in \mathbf{V}_Y(\mathrm{Ker}(\phi^*))$ and consider the evaluation map $\varepsilon_y : K[Y] \to K$ (c.f., Lemma 1.5.18). As ϕ^* is surjective we have ε_y factors as $\varepsilon_x \circ \phi^*$ for a unique K-algebra homomorphism $\varepsilon_x : K[X] \to K$. By Proposition 1.5.19 this implies that $y = \phi(x) \in \phi(X)$ so $\phi(X)$ is closed in Y.

Now clearly we have

$$g \in \mathbf{I}_Y(\phi(X)) \Leftrightarrow g(\phi(x)) = \phi^*(g)(x) = 0 \text{ for all } x \in X \Leftrightarrow \phi^*(g) = 0$$

so $\mathrm{Ker}(\phi^*) = \mathbf{I}_Y(\phi(X))$ is a radical ideal. Hence ϕ^* induces an isomorphism $K[\phi(X)] \cong K[Y]/\mathbf{I}_Y(\phi(X)) \to K[X]$ so ϕ induces an isomorphism onto its image by Corollary 1.5.22.

(b). Using the fact that $\mathrm{Ker}(\phi^*) = \mathbf{I}_Y(\phi(X))$ together with Proposition 1.4.11 we see that $\overline{\phi(X)} = \mathbf{V}_Y(\mathbf{I}_Y(\phi(X))) = \mathbf{V}_Y(\mathrm{Ker}(\phi^*))$. Furthermore, as $\mathrm{Ker}(\phi^*)$ is a radical ideal $\mathbf{V}_Y(\mathrm{Ker}(\phi^*)) = Y$ if and only if $\mathrm{Ker}(\phi^*) = \{0\}$ so we're done. ■

Exercise 1.9.3. Assume X is an affine variety and let $X_f \subseteq X$ be a principal open set. Describe a closed embedding $X_f \subseteq \mathbb{A}^m$ for some $m \geqslant 1$. [Hint: $f(x)$ is invertible for all $x \in X_f$.]

Theorem 1.9.4. *Assume $\phi : X \to Y$ is a morphism of varieties then $\phi(X)$ contains a non-empty open subset of $\overline{\phi(X)}$.*

2. Algebraic Groups

2.3 G-spaces

2.3.6. Recall that if G is an affine algebraic group then we denote by $\lambda, \rho : G \to \mathrm{GL}(K[G])$ the homomorphisms given by

$$(\lambda(g)f)(x) = f(g^{-1}x) \qquad (\rho(g)f)(x) = f(xg)$$

for all $x, g \in G$ and $f \in K[G]$. These are faithful representations of the abstract group G such that $\rho = \iota \circ \lambda \circ \iota^{-1}$ where $\iota : G \to G$ is the inversion map.

Lemma 2.3.7. *Let H be a closed subgroup of G and $\mathbf{I}_G(H) \subseteq K[G]$ be the corresponding vanishing ideal then*

$$H = \{g \in G \mid \lambda(g)\mathbf{I}_G(H) = \mathbf{I}_G(H)\} = \{g \in G \mid \rho(g)\mathbf{I}_G(H) = \mathbf{I}_G(H)\}.$$

Proof. If $f \in I$ then we have

$$(\lambda(g)f)(x) = f(g^{-1}x) = 0$$

for all $g, x \in H$ so $\lambda(g)f \in \mathbf{I}_G(H)$. Conversely, if $g \in G$ is such that $\lambda(g)\mathbf{I}_G(H) = \mathbf{I}_G(H)$ then we have

$$f(g^{-1}) = (\lambda(g)f)(1) = 0$$

for any $f \in \mathbf{I}_G(H)$ because $\lambda(g)f \in \mathbf{I}_G(H)$. Hence $g^{-1} \in \mathbf{V}_G(\mathbf{I}_G(H)) = H$ so $g \in H$. The statement for ρ follows from the fact that $\rho = \iota \circ \lambda \circ \iota^{-1}$. ■

Exercise 2.3.8. With the setting of Proposition 2.3.5, there is an increasing sequence of finite dimensional subspaces $\{V_i\}_{i\in\mathbb{N}}$ such that

(a) each V_i is stable under $s(G)$ and $s : G \to \mathrm{GL}(K[G])$ defines a rational representation of G in V_i,

(b) $K[X] = \bigcup_{i\in\mathbb{N}} V_i$.

2.4 The Jordan Decomposition

2.4.1. If G is a finite group and $p > 0$ is a prime dividing the order of the group then it is well known that every element $g \in G$ may be written uniquely as a product $g = g_p g_{p'} = g_{p'} g_p$ where $g_p \in G$ is an element of order a power of p and $g_{p'}$ is an element whose order is coprime to p. What we would like is a similar decomposition for elements in an algebraic group but now it does not make sense to speak of element orders. However, we can talk instead about semisimple and unipotent elements.

2.4.2. An endomorphism $x \in \mathrm{End}(V)$ of a finite dimensional K-vector space is called *semisimple* if there exists a basis of V which consists of eigenvectors of x. Furthermore, we say x is *nilpotent* if

$x^n = 0$ for some positive integer $n \geqslant 1$ and x is *unipotent* if $x - 1$ is nilpotent. We now recall some results from linear algebra. Note that fixing a basis of V we may identify $\mathrm{End}(V)$ with $\mathrm{Mat}_n(K)$ and $\mathrm{GL}(V)$ with $\mathrm{GL}_n(K)$.

Lemma 2.4.3. *Assume $S \subseteq \mathrm{GL}_n(K)$ is a set of pairwise commuting matrices then there exists $g \in \mathrm{GL}_n(K)$ such that $gSg^{-1} \subseteq \mathrm{T}_n(K)$. If all the matrices in S are semisimple then we may assume that $gSg^{-1} \subseteq \mathrm{D}_n(K)$.*

Lemma 2.4.4.

(a) If $x, y \in \mathrm{End}(V)$ are semisimple (resp., nilpotent, unipotent) endomorphisms such that $xy = yx$ then so is xy.

(b) If $x \in \mathrm{End}(V)$ and $y \in \mathrm{End}(W)$ are semisimple (resp., nilpotent, unipotent) endomorphisms then so are $x \oplus y \in \mathrm{End}(V \oplus W)$ and $x \otimes y \in \mathrm{End}(V \otimes W)$.

Proposition 2.4.5. *Assume $x \in \mathrm{End}(V)$ is an endomorphism then the following hold:*

(a) there exist unique $x_s, x_n \in \mathrm{End}(V)$ with x_s semisimple and x_n nilpotent such that $x = x_s + x_n = x_n + x_s$ and $x_s x_n = x_n x_s$,

(b) there exist polynomials $p(X), q(X) \in K[X]$ without constant term such that $p(x) = x_s$ and $q(x) = x_n$.

(c) if $W \subseteq V$ is an x-stable subspace then W is also stable under x_s and x_n and $x|_W = x_s|_W + x_n|_W$ is the additive Jordan decomposition of the restriction to W. Similarly, we have $x|_{V/W} = x_s|_{V/W} + x_n|_{V/W}$ is the additive Jordan decomposition of the restriction to the quotient V/W.

(d) if $y \in \mathrm{End}(V)$ is an endomorphism such that $xy = yx$ then $(x+y)_s = x_s + y_s$ and $(x+y)_n = x_n + y_n$.

(e) Let $\phi : V \to W$ and $y \in \mathrm{End}(W)$ be linear maps. If $\phi \circ x = y \circ \phi$ then $\phi \circ x_s = x_s \circ \phi$ and $\phi \circ x_n = y_n \circ \phi$.

Remark 2.4.6. We call x_s (resp., x_n) the semisimple (resp., nilpotent) part of x.

Corollary 2.4.7. *For $x \in \mathrm{GL}(V)$ we have $x_s \in \mathrm{GL}(V)$ and there exists a unique unipotent element $x_u \in \mathrm{GL}(V)$ such that $x = x_s x_u = x_u x_s$.*

Proof. Since x is invertible so is x_s so we can therefore set $x_u := 1 + x_s^{-1}x_n$. Let $a \geqslant 1$ be such that $x_n^a = 0$ then we have

$$(x_u - 1)^a = (x_s^{-1}x_n)^a = x_s^{-a}x_n^a = 0$$

because $x_s x_n = x_n x_s$ so x_u is unipotent. If $x = su = us$ is another such decomposition then $x = s + s(u-1)$ is the additive Jordan decomposition of x so we must have $s = x_s$ and $u - 1 = x_n$.■

Corollary 2.4.8. *For any $x \in \mathrm{GL}(V)$ and $y \in \mathrm{GL}(W)$ we have $x \oplus y = (x_s \oplus y_s)(x_u \oplus y_u)$ and $x \otimes y = (x_s \otimes y_s)(x_u \otimes y_u)$ are the Jordan decompositions of $x \oplus y \in \mathrm{GL}(V \oplus W)$ and $x \otimes y \in \mathrm{GL}(V \otimes W)$ respectively.*

2.4.9. Unfortunately for us the vector space V we have considered so far has been finite dimensional. However, in what follows we will need to consider the case where V is infinite dimensional (in particular the case where V is the group algebra of an affine algebraic group). To deal with this case we will need to introduce the concept of local finiteness.

2.4.10. In particular, assume now that V is an arbitrary, possibly infinite dimensional, vector space. We say $x \in \mathrm{End}(V)$ is *locally finite* if V is a union of finite dimensional x-stable subspaces. We say that x is *locally semisimple* (resp., *locally nilpotent*) if its restriction to any finite-dimensional x-stable subspace is semisimple (resp., nilpotent). Note that if $x \in \mathrm{End}(V)$ is locally finite then there exist unique $x_s, x_n \in \mathrm{End}(V)$ with x_s locally semisimple and x_n locally nilpotent such that $x = x_s + x_n = x_n + x_s$. These are defined as follows. Given $v \in V$ choose a finite dimensional x-stable subspace W containing x then we put

$$x_s v := (x|_W)_s v \qquad x_n v := (x|_W)_n x.$$

This definition is independent of W by Proposition 2.4.5(c).

Similarly if $x \in \mathrm{GL}(V)$ is locally finite then $x_s \in \mathrm{GL}(V)$ is locally semisimple and there exists a unique $x_u \in \mathrm{GL}(V)$ such that $x = x_s x_u = x_u x_s$ and x_u is *locally unipotent* in the sense that $x_u - 1$ is locally nilpotent. With this we are now ready to prove the existence of the Jordan decomposition.

Theorem 2.4.11 (Jordan Decomposition). *Let G be an affine algebraic group and let $A = K[G]$ be the affine algebra. We denote by $\rho : G \to \mathrm{GL}(A)$ the right translation homomorphism then the following hold:*

(a) For any $g \in G$ there exist unique elements $g_s, g_u \in G$ such that $\rho(g)_s = \rho(g_s)$ and $\rho(g)_u = \rho(g_u)$ and $g = g_s g_u = g_u g_s$.

(b) If $\phi : G \to G'$ is a homomorphism of algebraic groups then $\phi(g)_s = \phi(g_s)$ and $\phi(g)_u = \phi(g_u)$.

(c) If $G = \mathrm{GL}_n(K)$ then g_s and g_u are the semisimple and unipotent parts of Corollary 2.4.7 with $V = K^n$.

Remark 2.4.12. We call g_s (resp., g_u) the semisimple (resp., unipotent) part of g.

Proof. (a). Let $A = K[G]$ and $m : A \otimes A \to A$ be the homomorphism defined by multiplication, i.e., m is the K-linear extension of $m(a \otimes b) = ab$. Now, for any $g \in G$, we have $\rho(g)$ is an algebra automorphism of A which is equivalent to the fact that

$$m \circ (\rho(g) \otimes \rho(g)) = \rho(g) \circ m.$$

As $\rho(g)$ is locally finite by Exercise 2.3.8 we have a Jordan decomposition $\rho(g) = \rho(g)_s \rho(g)_u$ as in 2.4.10. Applying Proposition 2.4.5(e) to m we have

$$m \circ (\rho(g)_s \otimes \rho(g)_s) = \rho(g)_s \circ m \Rightarrow \rho(g)_s(a)\rho(g)_s(b) = \rho(g)_s(ab)$$

for all $a, b \in A$. In particular, this implies $\rho(g)_s$ is an algebra automorphism of A.

With this we see that the map $f \mapsto (\rho(g)_s f)(1)$ defines a homomorphism $A \to K$. By Lemma 1.5.18 there exists a unique point $g_s \in G$ such that $(\rho(g)_s f)(1) = f(g_s)$ for all $f \in A$. As $\rho(g)$ commutes with all left translations $\lambda(x)$, with $x \in G$, (which are again locally finite) we have by Proposition 2.4.5(e) that

$$(\rho(g)_s f)(x) = (\lambda(x^{-1})\rho(g)_s f)(1) = (\rho(g)_s \lambda(x^{-1})f)(1) = (\lambda(x^{-1})f)(g_s) = f(xg_s).$$

Hence $\rho(g)_s = \rho(g_s)$ is the right translation by g_s. In the same way we obtain an element $g_u \in G$ with $\rho(g)_u = \rho(g_u)$. The uniqueness now follows from the fact that ρ is a faithful representation of G.

(b). Note that a homomorphism of algebraic groups $\phi : G \to G'$ can be factored as

$$G \to \phi(G) \to G'.$$

Using Proposition 2.2.9(b) we have $\phi(G)$ is a closed subgroup of G' so we can prove (b) in two steps.

First assume that G is a closed subgroup of G' and ϕ is the inclusion map. If $I = \mathrm{Ker}(\phi^*) = \mathbf{I}_{G'}(\phi(G))$ then we have

$$G = \{g \in G' \mid \rho(g)I = I\}$$

by Lemma 2.3.7. In particular, for any $g \in G$ we have the algebra automorphism $\rho(g) : K[G'] \to K[G']$ induces a locally finite automorphism of $K[G] = K[G']/I$. The result now follows from Proposition 2.4.5(c).

Now assume that the map ϕ is surjective then we identify $K[G']$ with a subspace of $K[G]$ (by Lemma 1.9.2) which is stable under all $\rho(g)$ $(g \in G)$. The result then follows again from Proposition 2.4.5(c).

(c). Let $G = \mathrm{GL}(V)$ with $V = K^n$. Let $f \in \mathrm{Hom}(V, K)$ be a non-zero element of the dual space. For $v \in V$ define $\tilde{f}(v) \in K[G]$ by

$$\tilde{f}(v)(g) = f(gv).$$

This gives an injective linear map $V \to K[G]$. For all $g, x \in G$ and $v \in V$ we have

$$\begin{aligned} \tilde{f}(gv)(x) = f(xgv) = \tilde{f}(v)(xg) = (\rho(g)\tilde{f}(v))(x) &\Rightarrow \tilde{f}(gv) = \rho(g)\tilde{f}(v), \\ &\Rightarrow \tilde{f} \circ g = \rho(g) \circ \tilde{f}. \end{aligned}$$

From Proposition 2.4.5(e) we see that

$$\tilde{f} \circ s = \rho(g)_s \circ \tilde{f} \qquad \text{and} \qquad \tilde{f} \circ u = \rho(g)_u \circ \tilde{f},$$

where $g = su = us$ is the decomposition in Corollary 2.4.7. Putting this back into the previous calculation we have

$$(\rho(g)_s\tilde{f}(v))(x) = \tilde{f}(v)(xs) \qquad \text{and} \qquad (\rho(g)_u\tilde{f}(v))(x) = \tilde{f}(v)(xu)$$

for all $v \in V$ and $x \in G$. However, this implies that $s = g_s$ and $u = g_u$ because g_s and g_u are the unique elements with this property by the proof of (a). ■

3. Diagonalisable Groups

3.1 Characters

For any natural number $n \geqslant 1$ we denote by $\mathbb{D}_n$ the direct product $\mathbb{G}_m \times \cdots \times \mathbb{G}_m$ with n factors (we take $\mathbb{D}_0$ to be the trivial group).

Definition 3.1.1. An algebraic group G is called *diagonalisable* if there exists a closed embedding $\varphi : G \to \mathbb{D}_n$ for some $n \geqslant 0$. We say G is a *torus* if it is isomorphic to $\mathbb{D}_n$ for some $n \geqslant 0$.

Example 3.1.2. Let $D_n(K) \leqslant \mathrm{GL}_n(K)$ be the closed subgroup consisting of all diagonal matrices. This is clearly isomorphic to $\mathbb{D}_n$, hence is a torus. Now consider the subgroup

$$Z = \{\mathrm{diag}(\zeta, \dots, \zeta) \in T_n \mid \zeta^n = 1\} \leqslant T_n,$$

which is simply the centre of $\mathrm{SL}_n(K)$. If $Z \neq \{1\}$ then Z is an example of a diagonalisable group which is not a torus. Note, that if $p = \mathrm{char}(K) > 0$ then $|Z| = n/\gcd(n, p)$.

3.1.3. If G is an algebraic group we will denote by $X(G)$ the set of all *characters* of G, which are homomorphisms of algebraic groups $G \to \mathbb{G}_m$. For any two characters $\chi_1, \chi_2 \in X(G)$ we have a character $\chi_1\chi_2 \in X(G)$ given by

$$(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g)$$

for all $g \in G$. This gives $X(G)$ the structure of an abelian group. Every character of G is also a regular function on G so we have natural embeddings $X(G) \hookrightarrow K \otimes_{\mathbb{Z}} X(G) \hookrightarrow K[G]$. Now, viewing $X(G)$ as a subset of the K-vector space $K \otimes_{\mathbb{Z}} X(G)$ we have the following result of Dedekind.

Lemma 3.1.4 (Dedekind). *Assume $\{\chi_1, \dots, \chi_m\} \subseteq X(G)$ are pairwise distinct characters of G then $\{\chi_1, \dots, \chi_m\}$ is a linearly independent set over K. In particular, $X(G)$ is linearly independent over K.*

Proof. Assume for a contradiction that $\{\chi_1, \dots, \chi_m\}$ is a linearly dependent set of pairwise distinct characters with minimal cardinality $m > 1$ then we have

$$\sum_{i=1}^{m-1} a_i\chi_i + \chi_m = 0 \tag{3.1.5}$$

for some $a_i \in K$. After relabelling we may assume that $a_1 \neq 0$. As $\chi_1 \neq \chi_m$ there exists $g \in G$ such that $\chi_1(g) \neq \chi_m(g)$. Now, for any $x \in G$ we have

$$\sum_{i=1}^{m-1} a_i\chi_i(x)\chi_i(g) + \chi_m(x)\chi_m(g) = \sum_{i=1}^{m-1} a_i\chi_i(x)\chi_m(g) + \chi_m(x)\chi_m(g),$$

where the left hand side is obtained by evaluating (3.1.5) at xg and the right hand side is obtained by first evaluating (3.1.5) at x then multiplying through by $\chi_m(g)$. Rearranging this gives

$$\sum_{i=1}^{m-1} a_i(\chi_i(g) - \chi_m(g))\chi_i = 0$$

but as $a_1(\chi_1(g) - \chi_m(g)) \neq 0$ this implies that $\{\chi_1, \ldots, \chi_{m-1}\}$ is linearly dependent over K, a contradiction. ■

Remark 3.1.6. It is often typical to consider the group structure on $X(G)$ as an additive structure not a multiplicative structure. However, viewing it as a multiplicative structure makes it compatible with the K-algebra structure of $K[G]$.

Example 3.1.7. Consider the case of $G = \mathbb{D}_n$ then for each $1 \leqslant i \leqslant n$ we have a canonical character $\chi_i \in X(G)$ given by projection onto the ith factor, i.e.

$$\chi_i(g_1, \ldots, g_n) = g_i.$$

It is clear that we can identify $K[G]$ with $K[\chi_1^{\pm 1}, \ldots, \chi_n^{\pm 1}]$ using the natural inclusion $X(G) \hookrightarrow K[G]$. Now assume $f \in X(G)$ is a character then we have $f = \sum_{a \in \mathbb{Z}^n} c_a \chi_1^{a_1} \cdots \chi_n^{a_n}$ where $c_a \in K$ and $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$. Dedekind's lemma implies that $f = \chi_1^{a_1} \cdots \chi_n^{a_n}$ for a unique $a \in \mathbb{Z}^n$ so we have

$$X(G) = \{\chi_1^{a_1} \cdots \chi_n^{a_n} \mid (a_1, \ldots, a_n) \in \mathbb{Z}^n\} \cong \mathbb{Z}^n.$$

Furthermore, $X(G)$ is also clearly a basis of $K[G]$.

3.1.8. As we have seen in the previous example the diagaonalisable group $\mathbb{D}_n$ has a lot of characters; in fact enough to give a basis of the affine algebra. In this situation one often says that the group has enough characters to *separate points* because each maximal ideal of the affine algebra is generated by characters. This is in stark contrast to a group such as $\mathrm{SL}_n(K)$ which has no non-trivial characters as it is perfect. We now wish to characterise diagonalisable groups as those groups which have enough characters. However, we first consider the role of characters amongst rational representations.

3.1.9. Let G be an algebraic group and $\rho : G \to \mathrm{GL}(V)$ a rational representation of G. If $\chi \in X(G)$ is a character then we define a subspace

$$V_\chi = \{v \in V \mid \rho(g)v = \chi(g)v \text{ for all } g \in G\} \subseteq V.$$

We say $\chi \in X(G)$ is a *weight* of ρ if $V_\chi \neq \{0\}$; we then call V_χ the corresponding *weight space* of ρ. We will denote by $X_\rho(G)$ the set of all weights of ρ.

Remark 3.1.10. If $W \subseteq V$ is a 1-dimensional G-invariant subspace of V, i.e., $\rho(g)W \subseteq W$ for all $g \in G$, then it is clear that $W \subseteq V_\chi$ for some $\chi \in X_\rho(G)$. Conversely V_χ is a direct sum of 1-dimensional G-invariant subspaces because any subspace of V is G-invariant. In particular, the weight spaces encapsulate all G-invariant 1-dimensional subspaces of V.

Lemma 3.1.11. *Let G be an algebraic group. If $\rho : G \to \mathrm{GL}(V)$ is a rational representation of G then the set of weights $X_\rho(G)$ is finite and the sum of the corresponding weight spaces is direct.*

Proof. We claim that for any finite set $\{\chi_1, \ldots, \chi_r\} \subseteq X_\rho(G)$ of pairwise distinct weights the sum of the corresponding weight spaces $V_{\chi_1} + \cdots + V_{\chi_r}$ is direct. As the result is clearly true for $r = 1$ we may assume that $r > 1$ and proceed by induction. Let $v = v_1 + \cdots + v_{r-1} \in (V_{\chi_1} + \cdots + V_{\chi_{r-1}}) \cap V_{\chi_r}$ with $v_i \in V_{\chi_i}$ then for any $g \in G$ we have

$$\chi_r(g)v_1 + \cdots + \chi_r(g)v_{r-1} = \rho(g)v = \chi_1(g)v_1 + \cdots + \chi_{r-1}(g)v_{r-1}$$

for all $g \in G$. By the induction hypothesis the sum $V_{\chi_1} + \cdots + V_{\chi_{r-1}}$ is direct and it clearly contains $\rho(g)v$ as the weight spaces are G-invariant. In particular, we may compare the coefficients of the elements v_i to deduce that $\chi_i = \chi_r$ if $v_i \neq 0$. However, we assumed $\chi_i \neq \chi_r$ for all $i \neq r$ so we must have $v = 0$ as desired. As V is finite dimensional this clearly implies that $X_\rho(G)$ is finite. ∎

Corollary 3.1.12. *A rational representation $\rho : G \to \mathrm{GL}(V)$ is a direct sum of 1-dimensional representations if and only if V is the direct sum of its weight spaces.*

Theorem 3.1.13. *The following are equivalent:*

(a) G is diagonalisable,

(b) $X(G)$ is a basis of $K[G]$,

(c) any rational representation of G is a direct sum of 1-dimensional representations.

Proof. (a) ⇒ (b). Assume G is diagonalisable and let $\varphi : G \to \mathbb{D}_n$ be a closed embedding, then $\varphi^* : K[\mathbb{D}_n] \to K[G]$ is surjective by Lemma 1.9.2. It is clear that this restricts to a homomorphism of abelian groups $\varphi^* : X(\mathbb{D}_n) \to X(G)$. By Example 3.1.7 we know that $X(\mathbb{D}_n)$ is a basis of $K[\mathbb{D}_n]$ so $\varphi^*(X(\mathbb{D}_n)) \subseteq X(G)$ spans $K[G]$. Dedekind's lemma now shows that $X(G)$ is a basis of $K[G]$.

(b) ⇒ (c). Assume $\phi : G \to \mathrm{GL}(V)$ is a rational representation of G. We denote by $\widetilde{\phi} : G \times V \to V$ the morphism given by $\widetilde{\phi}(g, v) = \rho(g)v$, where we view V as an affine variety. We thus obtain an induced algebra homomorphism $\widetilde{\phi}^* : K[V] \to K[G] \otimes K[V] = K[G \times V]$. Let us identify V with K^n then $K[V]$ is identified with the polynomial ring $K[X_1, \ldots, X_n]$. By assumption we have for any polynomial X_i that

$$\widetilde{\phi}^*(X_i) = \sum_{\chi \in X(G)} \chi \otimes A_{\chi,i}$$

with $A_{\chi,i} \in K[V]$. Now assume $v = (v_1, \ldots, v_n) \in V$ then this implies that

$$\rho(g)v = \widetilde{\phi}(g, v) = \sum_{\chi \in X(G)} (\chi(g)A_{\chi,1}(v_1), \ldots, \chi(g)A_{\chi,n}(v_n)) = \sum_{\chi \in X(G)} \chi(g)A_\chi(v),$$

where $A_\chi(v) = (A_{\chi,1}(v_1), \ldots, A_{\chi,n}(v_n))$ for all $v \in V$.

Using the fact that $\rho(gh) = \rho(g)\rho(h)$ for any $g, h \in G$ we have

$$\sum_{\chi \in X(G)} A_\chi(v)(\chi \boxtimes \chi)(g, h) = \sum_{\chi \in X(G)} \sum_{\psi \in X(G)} (A_\chi A_\psi)(v)(\chi \boxtimes \psi)(g, h),$$

where $\chi \boxtimes \chi$ and $\chi \boxtimes \psi$ are characters of $G \times G$. Applying Dedekind's lemma to $X(G \times G)$ we see that

$$A_\chi A_\psi = \begin{cases} A_\chi & \text{if } \chi = \psi \\ 0 & \text{otherwise} \end{cases}$$

because the equality holds for all $(g, h) \in G \times G$ and $v \in V$. In particular, if $v \in \mathrm{Im}(A_\chi)$ then we have

$$\rho(g)v = \sum_{\psi \in X(G)} \psi(g)A_\psi(v) = \chi(g)A_\chi(v) = \chi(g)v$$

so $\mathrm{Im}(A_\chi) \subseteq V_\chi$. This clearly shows that $V = \rho(g)V \subseteq \oplus_{\chi \in X_\phi(G)} V_\chi$ so we're done by Corollary 3.1.12.

(c) $\Rightarrow$ (a). Let $\phi : G \to \mathrm{GL}(V)$ be a closed embedding of G. By assumption V is a direct sum of 1-dimensional G-invariant subspaces $V_1 \oplus \cdots \oplus V_n$. In particular the image of G is contained in the subgroup $\mathrm{GL}(V_1) \times \cdots \times \mathrm{GL}(V_n) \leqslant \mathrm{GL}(V)$ which is isomorphic to $\mathbb{D}_n$ so G is diagonalisable. ∎

Corollary 3.1.14. *If $\varphi : G \hookrightarrow \mathbb{D}_n$ is a closed embedding then $\varphi^* : X(\mathbb{D}_n) \to X(G)$ is surjective.*

Proof. The proof of Theorem 3.1.13 shows that $\varphi^*(X(\mathbb{D}_n)) \subseteq X(G)$ spans $K[G]$ so every character of G is a K-linear combination of the characters in $\varphi^*(X(\mathbb{D}_n))$. Dedekind's lemma then gives the equality. ∎

Corollary 3.1.15. *If G is diagonalisable then $X(G)$ is a finitely generated abelian group with no p-torsion.*

Proof. By Corollary 3.1.14 there exists a surjective homomorphism $X(\mathbb{D}_n) \to X(G)$ for some $n \geqslant 0$. In particular, $X(G)$ is a quotient of $\mathbb{Z}^n$ so must be finitely generated. Finally $X(G)$ has no p-torsion otherwise K would contain a non-trivial p^dth root of unity for some integer $d \geqslant 1$. ∎

3.2 Structure of Diagonalisable Groups

We now wish to consider the structure of a diagonalisable group, which turns out to be quite simple. For this we will need the following lemma.

Lemma 3.2.1. *If G is a connected algebraic group then $X(G)$ is torsion-free.*

Proof. Assume $\chi \in X(G)$ satisfies $\chi^n = 0$ for some integer $n > 0$ then the image $\chi(G)$ is finite because it is contained in the set $\{\zeta \in \mathbb{G}_m \mid \zeta^n = 1\}$. As $\chi(G^\circ) = \chi(G)^\circ$ we must have $\chi(G) = \{1\}$ because G is connected, hence $X(G)$ is torsion-free. ∎

Remark 3.2.2. Note that the converse of Lemma 3.2.1 holds if $\mathrm{char}(K) = 0$. However, it can fail in positive characteristic. For instance, if G is a finite cyclic group of order $p = \mathrm{char}(K)$ then $X(G)$ is torsion free but G is not connected.

Theorem 3.2.3. *Assume G is a diagonlisable group then the connected component G° is a torus. Furthermore, there exists a finite subgroup $H \leqslant G$ whose order is coprime to p such that $G = G^\circ \times H$.*

Proof. As G is diagonalisable we may and will identify G as a closed subgroup of $\mathbb{D}_n$. Now the natural inclusion morphism $\varphi : G^\circ \hookrightarrow \mathbb{D}_n$ is a closed embedding which induces a surjective homomorphism $\varphi^* : X(\mathbb{D}_n) \to X(G^\circ)$ by Corollary 3.1.14. By Corollary 3.1.15 and Lemma 3.2.1 we have $X(G^\circ)$ is a finitely generated abelian group with no torsion, so it is isomorphic to $\mathbb{Z}^r$ for some $r \geqslant 0$. As free modules are projective we must have φ^* splits so that $X(\mathbb{D}_n) = M \oplus \mathrm{Ker}(\varphi^*)$ with $M \cong \mathbb{Z}^r$.

We may now choose a basis $\{\chi_1, \ldots, \chi_n\}$ of $X(\mathbb{D}_n)$ so that we have $\{\chi_1, \ldots, \chi_r\} \subseteq M$ and $\{\chi_{r+1}, \ldots, \chi_n\} \subseteq \mathrm{Ker}(\varphi^*)$. The map $\psi : \mathbb{D}_n \to \mathbb{D}_n$ given by $\psi(g) = (\chi_1(g), \ldots, \chi_n(g))$ clearly defines an automorphism of $\mathbb{D}_n$. If we identify G with its image $\psi(G)$ under this automorphism then we have

$$G^\circ = \{(g_1, \dots, g_n) \in \mathbb{D}_n \mid g_{r+1} = \cdots = g_n = 1\} \cong \mathbb{D}_r.$$

This shows that G° is a torus. Now clearly we have $\mathbb{D}_n = G^\circ \times A$ where

$$A = \{(g_1, \dots, g_n) \in \mathbb{D}_n \mid g_1 = \cdots = g_r = 1\}.$$

In particular, taking $H = A \cap G$ we have $G = H \times G^\circ$ and $H \cong G/G^\circ$. The group H is finite as the component group G/G° is finite and must have order coprime to p because K contains no non-trivial p^dth roots of unity. ■

Remark 3.2.4. As is to be expected in such situations, the complement H is by no means unique. Furthermore, this result is quite surprising as it is easy to come up with examples of abelian groups possesing a subgroup with no complement. For example consider the subgroup $2\mathbb{Z} \leqslant \mathbb{Z}$ consisting of all even integers. Any non-zero element in a complement of $2\mathbb{Z}$ must be an odd integer but this is clearly impossible as no such subset is closed under addition.

Corollary 3.2.5. *A diagonalisable group is a torus if and only if it is connected.*

Definition 3.2.6. For any algebraic group G we will denote by G_{fin} the set of all elements of finite order. Furthermore, for any integer $d > 0$ we denote by $G_d \subseteq G_{\text{fin}}$ the set $\{g \in G \mid g^d = 1\}$.

Corollary 3.2.7. *If G is diagonalisable then G_d is finite for any integer $d > 0$. Furthermore, G_{fin} has infinite cardinality and $G = \overline{G_{\text{fin}}}$.*

Proof. By Theorem 3.2.3 we need only show this when $G = \mathbb{G}_m$. However, it is easy to see that G_d has finite cardinality because there are only finitely many dth roots of unity in K. On the other hand, G_{fin} clearly has infinite cardinality because K has infinitely many roots of unity. By Corollary 1.8.7 this implies that $\dim \overline{G_{\text{fin}}} \geqslant \dim G = 1$ which in turn implies that $G = \overline{G_{\text{fin}}}$ by Proposition 1.8.6. ■

3.3 Rigidity of Diagonalisable Groups

3.3.1. Given an algebraic group G one often used tool in trying to study the structure of G is to consider its diagonalisable subgroups (or more specifically tori). Now, this may not always be successful as G may have no non-trivial diagonalisable subgroups (for instance a unipotent group). However, reductive groups such as $\mathrm{GL}_n(K)$ do have non-trivial diagonalisable subgroups; in this case the group $D_n(K)$ from Example 3.1.2 is an example. One of the main features of diagonalisable groups is that they are *rigid*. More precisely, we mean the following.

Proposition 3.3.2 (Rigidity of diagonalisable groups). *Assume G is an algebraic group and $T \leqslant G$ is a diagonalisable subgroup then $N_G(T)^\circ = C_G(T)^\circ$ and $N_G(T)/C_G(T)$ is finite.*

Proof. Clearly we have $C_G(T)^\circ \subseteq N_G(T)^\circ$ so we need only show that the reverse inclusion holds. In particular, we need to show that any $n \in N_G(T)^\circ$ centralises T. Given $t \in T$ let us denote by $\varphi_t : N_G(T)^\circ \to T$ the morphism given by $\varphi_t(n) = ntn^{-1}$. Assume $t \in T_d \subseteq T_{\text{fin}}$ is of finite order $d > 0$ then clearly $\varphi_t(N_G(T)^\circ) \subseteq T_d$. However, $\varphi_t(N_G(T)^\circ)$ is finite by Corollary 3.2.7 and connected because $N_G(T)^\circ$ is connected. As the image contains t we must have $\varphi_t(N_G(T)^\circ) = \{t\}$. This shows that, for any $n \in N_G(T)^\circ$, the conjugation morphism $\iota_n : T \to T$ given by $\iota_n(t) = ntn^{-1}$ restricts to the identity on T_{fin}. However, by Corollary 3.2.7 T_{fin} is dense in T so we must have $\iota_n = \mathrm{id}_T$ by Lemma 1.7.12(b). ■

3.4 Structure of Abelian Algebraic Groups

As an example of the power of the abstract Jordan decomposition we may entirely describe the structure of an abelian affine algebraic group.

Theorem 3.4.1. *Let G be an abelian affine algebraic group then the following hold:*

(a) The set G_s (resp., G_u) of semisimple (resp., unipotent) elements of G is a closed subgroup.

(b) The product map $\pi : G_s \times G_u \to G$ is an isomorphism of algebraic groups.

Proof. (a). Let us identify G with a closed subgroup of $\mathrm{GL}_n(K)$. As G is abelian we may assume that $G \subseteq T_n(K)$ by Lemma 2.4.3. In this is the case then we have $G_s = G \cap D_n(K)$ and $G_s = G \cap U_n(K)$, which implies G_s and G_u are closed as they are obtained as the intersection of two closed sets. We now need only show that G_s and G_u are closed under multiplication as they are clearly closed under inversion. However, for any $x, y \in G$ we have $x_s y_s$ is semisimple and $x_u y_u$ is unipotent by Lemma 2.4.4 so G_s and G_u are subgroups.

(b). The uniqueness of the Jordan decomposition shows that this map is a bijective morphism of algebraic groups. The inverse map is given by $x \mapsto (x_s, x_s^{-1}x)$. This is clearly a morphism of varieties as $x \mapsto x_s$ is a morphism of varieties by Proposition 2.4.5(b) so π is an isomorphism. ■

Corollary 3.4.2. *If G is a connected abelian affine algebraic group then G_s and G_u are closed connected subgroups of G.*

Proof. G_s, resp., G_u, is the image of G under the morphism $x \mapsto x_s$, resp., $x \mapsto x_u$. As G is connected this implies G_s and G_u are connected. ■

We close this section by stating the following innocuous looking result, which is surprisingly difficult to prove.

Theorem 3.4.3. *Assume G is a connected 1-dimensional affine algebraic group then G is isomorphic to $\mathbb{G}_m$ or $\mathbb{G}_a$.*

Remark 3.4.4. In the proof of this result the first thing to show is that G must be abelian. Let us assume that this is known then Theorem 3.4.1 and Corollary 3.4.2 show that G must either consist entirely of semisimple elements or unipotent elements. Assume $G = G_s$ then the argument used in the proof of Theorem 3.4.1 shows that there exists a closed embedding $G \to \mathrm{D}_n(K) \cong \mathbb{D}_n$ hence G is diagonalisable. By the structure of diagonalisable groups (c.f., Theorem 3.2.3) this implies $G \cong \mathbb{G}_m$. The case when $G = G_u$ is significantly more involved and requires a close study of so-called vector groups, which are the unipotent analogues of tori. We do not discuss this here.

4. Differentials and Lie Algebras

4.1 Heuristics

4.1.1. Consider the classical situation where M is a differentiable manifold. When trying to study M locally around a point $x \in M$ it is often helpful to look at the tangent space $T_x(M)$ of M at x. This is an $\mathbb{R}$-vector space which approximates M near x. For instance, if M is a sphere then $T_x(M)$ is the plane meeting M at the point x. We wish to generalise these notions to the setting of algebraic geometry. We will start with a heuristic approach and then progress towards more intrinsic but possibly less transparent definitions.

4.1.2. Let $V \subseteq \mathbb{A}^n$ be a non-empty affine variety with associated vanishing ideal $\mathbf{I}(V) \subseteq K[X_1, \dots, X_n]$ and let us fix a point $p = (p_1, \dots, p_n) \in V$. Then for any $f \in K[X_1, \dots, X_n]$ we define a linear polynomial

$$d_p(f) = \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(p) X_i \in K[X_1, \dots, X_n].$$

This clearly gives us a K-linear map $d_p : K[X_1, \dots, X_n] \to K[X_1, \dots, X_n]$ which satisfies the usual rules for differentiation, namely

$$d_p(f+g) = d_p(f) + d_p(g) \qquad d_p(fg) = d_p(f)g(p) + f(p)d_p(g)$$

for all $f, g \in K[X_1, \dots, X_n]$.

For any point $v = (v_1, \dots, v_n) \in \mathbb{A}^n$ we consider the 'line through p in the direction of v' given by $L_v = \{p + tv \mid t \in K\} \subseteq \mathbb{A}^n$. Restricting f to L_v we can think of f as a function in t. Now considering the Taylor expansion of f around the point $t = 0$ we have

$$f(p + tv) = f(p) + \underbrace{\left(\sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(p) v_i\right)}_{=d_p(f)(v)} t + O(t^2).$$

With this, we say L_v is a *tangent line* at $p \in V$ if $d_p(f)(v) = 0$ for all $f \in \mathbf{I}(V)$.

Definition 4.1.3. Let $V \subseteq \mathbb{A}^n$ be a non-empty algebraic set. For a fixed point $p \in V$ we define

$$\begin{aligned}\mathfrak{T}_p(V) &= \{v \in \mathbb{A}^n \mid d_p(f)(v) = 0 \text{ for all } f \in \mathbf{I}(V)\},\\ &= \{v \in \mathbb{A}^n \mid L_v \text{ is a tangent line at } p \in V\},\end{aligned}$$

to be the *tangent space* at $p \in V$.

Example 4.1.4. Consider the variety $V \subseteq \mathbb{A}^2$ which is the zero locus of the polynomial $f = X_1^2 + X_2^2 - 1 \in K[X_1, X_2]$. If $\mathrm{char}(K) \neq 2$ then the vanishing ideal $\mathbf{I}(V)$ is generated by f. Now consider the point $p = (0,1) \in V$ then we have

$$d_p(f) = \frac{\partial f}{\partial X_1}(0,1)X_1 + \frac{\partial f}{\partial X_2}(0,1)X_2 = 2X_2.$$

In particular, this shows that $\mathfrak{T}_p(V)$ is simply the straight line $\{(x,0) \mid x \in K\}$. Now let us assume that $\mathrm{char}(K) = 2$ then $f = f'^2$ with $f' = X_1 + X_2 + 1 \in K[X_1, X_2]$. In this case f' generates $\mathbf{I}(V)$ and we have

$$d_p(f') = \frac{\partial f'}{\partial X_1}(0,1)X_1 + \frac{\partial f'}{\partial X_2}(0,1)X_2 = X_1 + X_2.$$

Hence, in this case, we have $\mathfrak{T}_p(V)$ is the straight line $\{(v,v) \mid v \in K\}$. Note that taking $K = \mathbb{R}$ we get the familiar picture of a tangent line to a circle.

4.1.5. For calculations we note that it is sufficient to check the defining condition of the tangent space on a generating set of the vanishing ideal. Indeed, let $V \subseteq \mathbb{A}^n$ be a non-empty algebraic set such that $\mathbf{I}(V)$ is generated by $f_1, \dots, f_r \in K[X_1, \dots, X_n]$. Then we claim that for any point $p \in V$ we have

$$\mathfrak{T}_p(V) = \{v \in \mathbb{A}^n \mid d_p(f_i)(v) = 0 \text{ for all } 1 \leqslant i \leqslant r\}.$$

It suffices to show that the right hand side is contained in the left hand side. Assume $v \in \mathbb{A}^n$ satisfies $d_p(f_i)(v) = 0$ for all $1 \leqslant i \leqslant r$ and write $f \in \mathbf{I}(V)$ as $\sum_{i=1}^n h_i f_i$ for some $h_i \in K[X_1, \dots, X_n]$ then we have

$$d_p(f) = \sum_{i=1}^n d_p(h_i f_i) = \sum_{i=1}^n (f_i(p)d_p(h_i) + h_i(p)d_p(f_i)) = \sum_{i=1}^n h_i(p)d_p(f_i)$$

because $f_i \in \mathbf{I}(V)$ and $p \in V$. The claim follows immediately.

4.2 Derivations and the Tangent Space

4.2.1. The definition we have given of the tangent space in the previous section depends upon the embedding of the variety into affine space. Our goal now is to show that we may give an equivalent definition of the tangent space which is intrinsic to the variety.

Definition 4.2.2. Let A be a K-algebra and M an A-module, let the action of A on M be denoted by $a \cdot m$ for all $a \in A$, $m \in M$. We say a K-linear map $D : A \to M$ is a *derivation* if D satisfies the Leibniz rule

$$D(ab) = a \cdot D(b) + b \cdot D(a),$$

for all $a, b \in A$. We write $\mathrm{Der}_K(A, M)$ for the space of all derivations from A to M.

Remark 4.2.3. Note that $\mathrm{Der}_K(A, M)$ is naturally an A-module via the action $(a \cdot D)(f) = aD(f)$ for all $a, f \in A$.

Example 4.2.4. Consider the polynomial ring $R = K[X_1, \dots, X_n]$ and an R-module M. It is easily shown that for any derivation $D \in \mathrm{Der}_K(R, M)$ we have

$$D(f) = \sum_{i=1}^n D(X_i) \cdot \frac{\partial f}{\partial X_i}.$$

In fact, since the set of partial derivatives $\{\partial/\partial X_i\}_{1 \leqslant i \leqslant n}$ is linearly independent we conclude that $\mathrm{Der}_K(R, R)$ is a free R-module of rank n.

4.2.5. Let $V \subseteq \mathbb{A}^n$ be an affine variety and pick a point $p \in V$. We turn the field K into a module for the affine algebra $K[V]$ by defining the action to be $\overline{f} \cdot \alpha = f(p)\alpha$. We will write K_p when we consider K as a $\mathbb{K}[V]$ module in this way.

Lemma 4.2.6. *Let $V \subseteq \mathbb{A}^n$ be a non-empty affine variety and $p \in V$ be any point. Then for any $v \in \mathfrak{T}_p(V)$ we have a well defined derivation $D_v \in \mathrm{Der}_K(K[V], K_p)$ given by $D_v(\overline{f}) = d_p(f)(v)$ for any $f \in K[X_1, \ldots, X_n]$. Furthermore, the map $\Psi : \mathfrak{T}_p(V) \to \mathrm{Der}_K(K[V], K_p)$ given by $v \mapsto D_v$ is an isomorphism of $K[V]$-modules.*

Proof. Let R denote the polynomial ring $K[X_1, \ldots, X_n]$ and let $\pi : R \to K[V]$ be the canonical projection map. We start by confirming that Ψ is well defined. Assume $f, g \in K[V]$ satisfy $f - g \in \mathbf{I}(V)$ then for any $v \in \mathfrak{T}_p(V)$ we have

$$D_v(\overline{f}) - D_v(\overline{g}) = d_p(f)(v) - d_p(g)(v) = d_p(f - g)(v) = 0$$

by the definition of $\mathfrak{T}_p(V)$. Hence Ψ is well defined.

If $v = (v_1, \ldots, v_n) \in \mathfrak{T}_p(V)$ then it is clear that we have $D_v(\overline{X_j}) = v_j$ for each $1 \leqslant j \leqslant n$, which shows Ψ is injective. Let $D \in \mathrm{Der}_K(K[V], K_p)$ be a derivation then the composition $\tilde{D} = D \circ \pi \in \mathrm{Der}_K(R, K_p)$ is also a derivation. By Example 4.2.4 we see that for all $f \in R$ we have

$$D(\overline{f}) = \tilde{D}(f) = \sum_{i=1}^{n} \frac{\partial f}{\partial X_i} \cdot \tilde{D}(X_i) = \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(p) v_i = d_p(f)(v).$$

For any $f \in \mathbf{I}(V)$ we have $\overline{f} = 0$ and so $D(\overline{f}) = d_p(f)(v) = 0$, which means $v \in \mathfrak{T}_p(V)$. Since $D_v(\overline{X_j}) = v_j = D(\overline{X_j})$ we have $D_v = D$ so Ψ is surjective and we're done. ∎

Definition 4.2.7. Assume V is an affine variety then for any $p \in V$ we define the tangent space $T_p(V)$ of V at p to be the $K[V]$-module $\mathrm{Der}_K(K[V], K_p)$ of derivations.

References

[AM69] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969, ix+128.

[Bor91] A. Borel, *Linear algebraic groups*, Second, vol. 126, Graduate Texts in Mathematics, Springer-Verlag, New York, 1991, xii+288.

[Gec03] M. Geck, *An introduction to algebraic geometry and algebraic groups*, vol. 10, Oxford Graduate Texts in Mathematics, Oxford: Oxford University Press, 2003, xii+307.

[Hum75] J. E. Humphreys, *Linear algebraic groups*, Graduate Texts in Mathematics, No. 21, New York: Springer-Verlag, 1975, xiv+247.

[Spr09] T. A. Springer, *Linear algebraic groups*, Modern Birkhäuser Classics, Boston, MA: Birkhäuser Boston Inc., 2009, xvi+334.