Lectures on Algebraic Groups

Alexander Kleshchev

Contents

Part one

Algebraic Geometry

1
General Algebra

Definition 1.0.1 A functor $F : \mathcal{A} \to \mathcal{B}$ is called *faithful* if the map

$$\mathrm{Hom}_{\mathcal{A}}(A_1, A_2) \to \mathrm{Hom}_{\mathcal{B}}(F(A_1), F(A_2)),\ \theta \mapsto F(\theta) \tag{1.1}$$

is injective, and F is called *full* if the map (1.1) is surjective.

Theorem 1.0.2 *A functor $F : \mathcal{A} \to \mathcal{B}$ is an equivalence of categories if and only if the following two conditions hold:*

(i) *F is full and faithful;*
(ii) *every object of $\mathcal{B}$ is isomorphic to an object of the form $F(A)$ for some $A \in \mathrm{Ob}\,\mathcal{A}$.*

Proof ($\Rightarrow$) Let F be an equivalence of categories and $G : \mathcal{B} \to \mathcal{A}$ be the quasi-inverse functor. Let $\alpha : GF \to \mathrm{id}_{\mathcal{A}}$ and $\beta : FG \to \mathrm{id}_{\mathcal{B}}$ be isomorphisms of functors. First of all, for any object B of $\mathcal{B}$ $\beta_B : F(G(B)) \to B$ is an isomorphism, which gives (ii). Next, for each $\varphi \in \mathrm{Hom}_{\mathcal{A}}(A_1, A_2)$ we have the commutative diagram

$$\begin{tikzcd}
GF(A_1) \arrow[r, "\alpha_{A_1}"] \arrow[d, "GF(\varphi)"'] & A_1 \arrow[d, "\varphi"] \\
GF(A_2) \arrow[r, "\alpha_{A_2}"] & A_2
\end{tikzcd}$$

Hence φ can be recovered from $F(\varphi)$ by the formula

$$\varphi = \alpha_{A_2} \circ GF(\varphi) \circ (\alpha_{A_1})^{-1}. \tag{1.2}$$

This shows that F is faithful. Similarly, G is faithful. To prove that F

is full, consider an arbitrary morphism $\psi \in \mathrm{Hom}_{\mathcal{B}}(F(A_1), F(A_2))$, and set

$$\varphi := \alpha_{A_2} \circ G(\psi) \circ (\alpha_{A_1})^{-1} \in \mathrm{Hom}_{\mathcal{A}}(A_1, A_2).$$

Comparing this with (1.2) and taking into account that α_{A_1} and α_{A_2} are isomorphisms, we deduce that $G(\psi) = GF(\varphi)$. As G is faithful, this implies that $\psi = F(\varphi)$, which completes the proof that F is a full functor.

($\Leftarrow$) Assume that (i) and (ii) hold. In view of (i), we can (and will) identify the set $\mathrm{Hom}_{\mathcal{B}}(F(A_1), F(A_2))$ with the set $\mathrm{Hom}_{\mathcal{A}}(A_1, A_2)$ for any $A_1, A_2 \in \mathrm{Ob}\,\mathcal{A}$. Using (ii), for each object B in $\mathcal{B}$ we can pick an object A_B in $\mathcal{A}$ and an isomorphism $\beta_B : F(A_B) \to B$. We define a functor $G : \mathcal{B} \to \mathcal{A}$ which will turn out to be a quasi-inverse functor to F. on the objects we set $G(B) = A_B$ for any $B \in \mathrm{Ob}\,\mathcal{B}$. To define G on the morphisms, let $\psi \in \mathrm{Hom}_{\mathcal{B}}(B_1, B_2)$.

$$\begin{aligned} G(\psi) := \beta_{B_2}^{-1} \circ \psi \circ \beta_{B_1} \in &\mathrm{Hom}_{\mathcal{B}}(FG(B_1), FG(B_2)) \\ &= \mathrm{Hom}_{\mathcal{A}}(G(B_1), G(B_2)). \end{aligned}$$

It is easy to see that G is a functor, and $\beta = \{\beta_B\} : FG \to \mathrm{id}_{\mathcal{B}}$ is an isomorphism of functors. Further, $\beta_{F(A)} = F(\alpha_A)$ for the unique morphism $\alpha_A : GF(A) \to A$. Finally, it is not hard to see that $\alpha = \{\alpha_A\} : GF \to \mathrm{id}_{\mathcal{A}}$ is an isomorphism of functors. $\square$

2
Commutative Algebra

Here we collect some theorems from commutative algebra which are not always covered in 600 algebra. All rings and algebras are assumed to be commutative.

2.1 Some random facts

Lemma 2.1.1 *Let k be a field, $f, g \in k[x, y]$, and assume that f is irreducible. If g is not divisible by f, then the system $f(x, y) = g(x, y) = 0$ has only finitely many solutions.*

Proof See [Sh, 1.1]. $\square$

Proposition 2.1.2 *Let A, B be k-algebras, $I \lhd A, J \lhd B$ be ideals. Then*

$$A/I \otimes_k B/J \to (A \otimes_k B)/(A \otimes J + I \otimes B), \quad \bar{a} \otimes \bar{b} \mapsto \overline{a \otimes b}$$

is an isomorphism of algebras.

Definition 2.1.3 A subset S of a commutative ring R is called *multiplicative* if $1 \in S$ and $s_1 s_2 \in S$ whenever $s_1, s_2 \in S$. A multiplicative subset is called *proper* if $0 \notin S$.

Lemma 2.1.4 *Let $S \subset R$ be a proper multiplicative set. Let I be an ideal of R satisfying $I \cap S = \varnothing$. The set T of ideals $J \supseteq I$ such that $J \cap S = \varnothing$ has maximal elements, and each maximal element in T is a prime ideal.*

Proof That the set T has maximal elements follows from Zorn Lemma. Let M be such an element. Assume that $x, y \in R \setminus M$. By the choice of M, $M + Rx$ contains some $s_1 \in S$ and $M + Ry$ contains some $s_2 \in S$, i.e. $s_1 = m_1 + r_1 x$ and $s_2 = m_2 + r_2 y$. Hence

$$s_1 s_2 = (m_1 + r_1 x)(m_2 + r_2 y) \in M + Rxy.$$

It follws that $M + Rxy \neq M$, i.e. $xy \notin M$. $\square$

Theorem 2.1.5 (Prime Avoidance Theorem) *Let $P_1, \ldots, P_n$ be prime ideals of the ring R. If some ideal I is contained in the union $P_1 \cup \cdots \cup P_N$, then I is already contained in some P_i.*

Proof We can assume that none of the prime ideals is contained in another, because then we could omit it. Fix an $i_0 \in \{1, \ldots, N\}$ and for each $i \neq i_0$ choose an $f_i \in P_i$, $f_i \notin P_{i_0}$, and choose an $f_{i_0} \in I$, $f_{i_0} \notin P_{i_0}$. Then $h_{i_0} := \prod f_i$ lies in each P_i with $i \neq i_0$ and I but not in P_{i_0}. Now, $\sum h_i$ lies in I but not in any P_i. $\square$

Lemma 2.1.6 (Nakayama's Lemma) *Let M be a finitely generated module over the ring A. Let I be an ideal in A such that for any $a \in 1+I$, $aM = 0$ implies $M = 0$. Then $IM = M$ implies $M = 0$.*

Proof Let $m_1, \ldots, m_l$ be generators of M. The condition $IM = M$ means that

$$m_i = \sum_{j=1}^{l} x_{ij} m_j \quad (1 \leq i \leq l).$$

for some $x_{ij} \in I$. Hence

$$\sum_{j=1}^{l} (x_{ij} - \delta_{ij}) m_j = 0 \quad (1 \leq i \leq l).$$

So by Cramer's rule, $dm_j = 0$, where $d = \det(x_{ij} - \delta_{ij})$. Hence $dM = 0$. But $d \in 1 + I$, so $M = 0$. $\square$

Corollary 2.1.7 *If $B \supset A$ is a ring extension, and B is finitely generated as an A-module, then $IB \neq B$ for any proper ideal I of A.*

Proof Since B contains 1, we have $aB = 0$ only if $a = 0$. Now all elements of $1 + I$ are non-zero for a proper ideal I, so we can apply Nakayama's Lemma. $\square$

Corollary 2.1.8 (Nakayama's Lemma) *Let M be a finitely generated module over the ring A, $M' \subseteq M$ be a submodule, and let I be an ideal in A such that all elements of $1+I$ are invertible. Then $IM + M' = M$ implies $M' = M$.*

Proof Apply Lemma 2.1.6 to M/M'. □

Another version:

Corollary 2.1.9 (Nakayama's Lemma) *Let M be a finitely generated module over a ring A, and I be a maximal ideal of A. If $IM = M$, then there exists $x \notin M$ such that $xM = 0$.*

Proof Localize at I and apply Corollary 2.1.8. □

Corollary 2.1.10 *Let M be a finitely generated module over the ring A and let I be an ideal in A such that all elements of $1+I$ are invertible. Then elements $m_1, \dots, m_n \in M$ generate M if and only if their images generate M/IM.*

Proof Apply Corollary 2.1.8 to $M' = (m_1, \dots, m_n)$. □

Lemma 2.1.11 *Let M be a maximal ideal of R, then the map $R \to R_M$ induces the isomorphism of the fields R/M and R_M/MR_M. If we identify the fields via this isomorphism, then the the map $R \to R_M$ also induces the isomorphism of vector spaces $M/M^2 \tilde{\to} MR_M/(MR_M)^2$.*

A field extension K/k is called *separable*, if either $\operatorname{char} k = 0$ or $\operatorname{char} k = p > 0$ and for any k-linearly independent elements $x_1, \dots, x_n \in K$, we have $x_1^p, \dots, x_n^p$ are linearly independent. A filed $K = k(x_1, \dots, x_n)$ is called *separably generated* over k if K is a finite separable extension of a purely transcendental extension of k.

Theorem 2.1.12

(i) *The extension $K = k(x_1, \dots, x_n)/k$ is separably generated if and only if K/k is separable.*
(ii) *If k is perfect (in particular algebraically closed), then any field extension K/k is separable.*
(iii) *Let $F/K/k$ be field extensions. If F/k is separable, then K/k is separable. If F/K and K/k are separable, then F/k is separable.*

Theorem 2.1.13 (Primitive Element Theorem) *If K/k is a finite separable extension, then there is an element $x \in K$ such that $K = k(x)$.*

Let L/E be a field extension. A *derivation* is a map $\delta : E \to L$ such that

$$\delta(x+y) = \delta(x) + \delta(y) \quad \text{and} \quad \delta(xy) = x\delta(y) + \delta(x)y \qquad (x, y \in E).$$

If F is a subfield of E, then the derivation δ is *F-derivation* if it is F-linear. The space $\mathrm{Der}_F(E, L)$ of all F-derivations is a vector space over L. With this notation, we have:

Theorem 2.1.14

(i) *If E/F is separably generated then*

$$\dim \mathrm{Der}_F(E, L) = \mathrm{tr.deg}_F\, E.$$

(ii) *E/F is separable if and only all derivations $F \to L$ extend to derivations $E \to L$.*

(iii) *If $\mathrm{char}\, E = p > 0$, then all derivations are zero on the subfield E^p. In particular, if E is perfect, all derivations of E are zero.*

Theorem 2.1.15 [Ma, Theorem 20.3] *A regular local ring is a UFD. In particular it is an integrally closed domain.*

2.2 Ring extensions

Definition 2.2.1 A *ring extension* of a ring R is a ring A of which R is a subring.

If A is a ring extension of R, A is a fathful R-module in a natural way. Let A be a ring extension of R and S be a subset of A. The subring of A generated by R and S is denoted $R[S]$. It is quite clear that $R[S]$ consists of all R-linear combinations of products of elements of S.

Definition 2.2.2 A ring extension A of R is called *finitely generated* if $A = R[s_1, \dots, s_n]$ for some finitely many elements $s_1, \dots, s_n \in A$.

The following notion resembles that of an algebraic element for field extensions.

Definition 2.2.3 Let A be a ring extension of R. An element $\alpha \in A$ is called *integral* over R if $f(\alpha) = 0$ for some monic polynomial $f(x) \in R[x]$. A ring extension $R \subseteq A$ is called *integral* if every element of A is integral over R.

In Proposition 2.2.5 we give two equivalent reformulations of the integrality condition. For the proof we will need the following technical

Lemma 2.2.4 *Let V be an R-module. Assume that $v_1, \ldots, v_n \in V$ and $a_{ij} \in R$, $1 \leq i, j \leq n$ satisfy $\sum_{j=1}^n a_{kj} v_j = 0$ for all $1 \leq k \leq n$. Then $D := \det(a_{ij})$ satisfies $Dv_i = 0$ for all $1 \leq i \leq n$.*

Proof We expand D by the ith column to get $D = \sum_{k=1}^n a_{ki} C_{ki}$, where C_{ki} is the (k, i) cofactor. We then also have $\sum_{k=1}^n a_{kj} C_{ki} = 0$ for $i \neq j$. So

$$\begin{aligned} Dv_i = \sum_{k=1}^n a_{ki} C_{ki} v_i &= \sum_{k=1}^n a_{ki} C_{ki} v_i + \sum_{j \neq i} (\sum_{k=1}^n a_{kj} C_{ki}) v_j \\ &= \sum_{j=1}^n \sum_{k=1}^n a_{kj} C_{ki} v_j = \sum_{k=1}^n C_{ki} \sum_{j=1}^n a_{kj} v_j = 0. \end{aligned}$$

□

Proposition 2.2.5 *Let A be a ring extension of R and $\alpha \in A$. The following conditions are equivalent:*

(i) *α is integral over R.*
(ii) *$R[\alpha]$ is a finitely generated R-module.*
(iii) *There exists a faithful $R[\alpha]$-module which is finitely generated as an R-module.*

Proof (i) $\Rightarrow$ (ii) Assume $f(\alpha) = 0$, where $f(x) \in R[x]$ is monic of degree n. Let $\beta \in R[\alpha]$. Then $\beta = g(\alpha)$ for some $g \in R[x]$. As f is monic, we can write $g = fq + r$, where $\deg r < n$. Then $\beta = g(\alpha) = r(\alpha)$. Thus $R[\alpha]$ is generated by $1, \alpha, \ldots, \alpha^{n-1}$ as an R-module.

(ii) $\Rightarrow$ (iii) is clear.

(iii) $\Rightarrow$ (i) Let V be a faithful $R[\alpha]$-module which is generated as an R-module by finitely many elements $v_1, \ldots, v_n$. Write

$$\alpha v_i = a_{i1} v_1 + \cdots + a_{in} v_n \quad (1 \leq i \leq n).$$

Then

$$-a_{i1}v_1 - \cdots - a_{i,i-1}v_{i-1} + (\alpha - a_{ii})v_i - a_{i,i+1}v_{i+1} - \cdots - a_{in}v_n = 0$$

for all $1 \leq i \leq n$. By Lemma 2.2.4, we have $Dv_i = 0$ for all i, where

$$D = \begin{vmatrix} \alpha - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & \alpha - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ -a_{n1} & a_{n2} & \cdots & \alpha - a_{nn} \end{vmatrix}.$$

As $v_1, \ldots, v_n$ generate V, this implies that D annihilates V. As V is faithful, $D = 0$. Expanding D shows that $D = f(\alpha)$ for some monic polynomial $f(x) \in R[x]$. □

Lemma 2.2.6 *Let $R \subseteq A \subseteq B$ be ring extensions. If A is finitely generated as an R-module and B is finitely generated as an A-module, then B is finitely generated as an R-module.*

Proof If $a_1, \ldots, a_m$ are generators of the R-module A and $b_1, \ldots, b_n$ are generators of the A-module B, then it is easy to see that $\{a_ib_j\}$ are generators of the R-module B. □

Proposition 2.2.7 *Let A be a ring extension of R.*

(i) *If A is finitely generated as an R-module, then A is integral over R.*
(ii) *If $A = R[\alpha_1, \ldots, \alpha_n]$ and $\alpha_1, \ldots, \alpha_n$ are integral over R, then A is finitely generated as an R-module and hence integral over R.*
(iii) *If $A = R[S]$ and every $s \in S$ is integral over R, then A is integral over R.*

Proof (i) Let $\alpha \in A$. Then A is a faithful $R[\alpha]$-module, and we can apply Proposition 2.2.5.

(ii) Note that $R[\alpha_1, \ldots, \alpha_i] = R[\alpha_1, \ldots, \alpha_{i-1}][\alpha_i]$. Now apply induction, Proposition 2.2.5 and Lemma 2.2.6.

(iii) Follows from (ii). □

Corollary 2.2.8 *Let A be a ring extension of R. The elements of A which are integral over R form a subring of A.*

Proof If $\alpha_1, \alpha_2 \in A$ are integral, then $\alpha_1 - \alpha_2$ and $\alpha_1\alpha_2$ belong to $R[\alpha_1, \alpha_2]$. So we can apply Proposition 2.2.7(ii). □

This result allows us to give the following definition

Definition 2.2.9 The *integral closure* of R in $A \supseteq R$ is the ring $\bar{R}$ of all elements of A that are integral over R. The ring R is *integrally closed* in $A \supseteq R$ in case $\bar{R} = R$. A domain R is called *integrally closed* if it is integrally closed in its field of fractions.

Example 2.2.10 The elements of the integral closure of $\mathbb{Z}$ in $\mathbb{C}$ are called *algebraic integers*. They form a subring of $\mathbb{C}$. In fact the field of algebraic numbers $\mathbb{A}$ is the quotient field of this ring.

We record some further nice properties of integral extensions.

Proposition 2.2.11 *Let R, A, B be rings.*

(i) *If $R \subseteq A \subseteq B$ then B is integral over R if and only if B is integral over A and A is integral over R.*
(ii) *If B is integral over A and $R[B]$ makes sense then $R[B]$ is integral over $R[A]$.*
(iii) *If A is integral over R and $\varphi : A \to B$ is a ring homomorphism then $\varphi(A)$ is integral over $\varphi(R)$.*
(iv) *If A is integral over R, then $S^{-1}A$ is integral over $S^{-1}R$ for every proper multiplicative subset S of R.*

Proof (i)-(iii) is an exercise.

(iv) First of all, it follows from definitions that $S^{-1}R$ is indeed a subring of $S^{-1}A$. Now, let $[\frac{a}{s}] \in S^{-1}A$. As $[\frac{a}{s}] = [\frac{a}{1}][\frac{1}{s}]$, it suffices to show that both $[\frac{a}{1}]$ and $[\frac{1}{s}]$ are integral over $S^{-1}R$. But $\frac{1}{s} \in S^{-1}R$ and for $[\frac{a}{1}]$ we can use the monic polynomial which annihilates a. $\square$

It follows from Proposition 2.2.11(i) that the closure of $\bar{R}$ in $A \supseteq R$ is again $\bar{R}$. In particular, if D is any domain and F is its field of fractions, then the closure $\bar{D}$ in F is an integrally closed domain (since the quotient field of $\bar{D}$ is also F).

We recall that a domain R is called a *unique factorization domain* or *UFD* if every non-zero non-unit element of R can be written as a product of irreducible elements, which is unique up to a permutation and units.

Proposition 2.2.12 *Every UFD is integrally closed.*

Proof Let R be a UFD and F be its field of fractions. Let $\frac{a}{b} \in F$ be integral over R. We may assume that no irreducible element of R divides both a and b. There is a monic polynomial $f(x) = x^n + r_{n-1}x^{n-1} + \cdots + r_0 \in R[x]$ with $f(\frac{a}{b}) = 0$, which implies $a^n + r_{n-1}a^{n-1}b + \cdots + r_0 b^n = 0$. So, if $p \in R$ is an irreducible element dividing b then p divides a^n, and hence p divides a, a contradiction. Therefore b is a unit and $\frac{a}{b} \in R$. $\square$

Proposition 2.2.13 *If a domain R is integrally closed, then so is $S^{-1}R$ for any proper multiplicative subset S of R.*

Proof Exercise. $\square$

Example 2.2.14 The ring $\mathbb{Z}[i]$ of Gaussian integers is Euclidean (the degree function is $\partial(a + bi) = a^2 + b^2$, hence it is a UFD, and so it is integrally closed by Proposition 2.2.13. On the other hand consider the ring $\mathbb{Z}[2i]$. The quotient field of both $\mathbb{Z}[i]$ and $\mathbb{Z}[2i]$ is $\mathbb{Q}(i)$, and we have $\mathbb{Z}[2i] \subset \mathbb{Z}[i] \subset \mathbb{Q}[i]$. Clearly $\mathbb{Z}[2i]$ is not integrally closed, as $i \notin \mathbb{Z}[2i]$ is integral over it. It is easy to see that $\overline{\mathbb{Z}[2i]} = \mathbb{Z}[i]$.

Theorem 2.2.15 *If R is integrally closed, then so is $R[x_1, \dots, x_r]$.*

Next we are going to address the question of how prime ideals of R and A are related if $A \supseteq R$ is an integral extension.

Definition 2.2.16 Let $R \subseteq A$ be a ring extension. We say that a prime ideal P of A *lies over* a prime ideal $\mathfrak{p}$ of R if $P \cap R = \mathfrak{p}$.

The following lemma is a key technical trick.

Lemma 2.2.17 *Let $A \supseteq R$ be an integral ring extension, $\mathfrak{p}$ be a prime ideal of R, and $S := R \setminus \mathfrak{p}$.*

(i) *Let I be an ideal of A avoiding S, and P be an ideal of A maximal among the ideals of A which contain I and avoid S. Then P is a prime ideal of A lying over $\mathfrak{p}$.*
(ii) *If P is a prime ideal of A which lies over $\mathfrak{p}$, then P is maximal in the set T of all ideals in A which avoid S.*

Proof (i) Clearly, S is a proper multiplicative subset of A. So P is prime in view of Lemma 2.1.4. We claim that $P \cap R = \mathfrak{p}$. That $P \cap R \subseteq \mathfrak{p}$ is clear as $P \cap S = \varnothing$.

Assume that $P \cap R \subsetneq \mathfrak{p}$. Let $c \in \mathfrak{p} \setminus P$. By the maximality of P, $p + \alpha c = s \in S$ for some $p \in P$ and $\alpha \in A$. As A is integral over R, we have

$$0 = \alpha^n + r_{n-1}\alpha^{n-1} + \cdots + r_0$$

for some $r_0, \dots, r_{n-1} \in R$. Multiplying by c^n yields

$$\begin{aligned} 0 &= c^n\alpha^n + cr_{n-1}c^{n-1}\alpha^{n-1} + \cdots + c^n r_0 \\ &= (s-p)^n + cr_{n-1}(s-p)^{n-1} + \cdots + c^n r_0. \end{aligned}$$

If we decompose the last expression as the sum of monomials, then the part which does not involve any positive powers of p looks like

$$x := s^n + cr_{n-1}s^{n-1} + \cdots + c^n r_0.$$

It follows that $x \in P$. On the other hand, $x \in R$, so $x \in R \cap P \subseteq \mathfrak{p}$. Now $c \in \mathfrak{p}$ implies $s^n \in \mathfrak{p}$. As $\mathfrak{p}$ is prime, $s \in \mathfrak{p}$, a contradiction.

(ii) If P is not maximal in T, then there exists an ideal I in T which properly contains P. As I still avoids S, it also lies over $\mathfrak{p}$. Take $u \in I \backslash P$. Then $u \notin R$ and u is integral over R. So the set of all polynomials $f \in R[x]$ such that $\deg f \geq 1$ and $f(u) \in P$ is non-empty. Take such $f(x) = \sum_{i=0}^n r_i x^i$ of minimal possible degree. We have

$$u^n + r_{n-1}u^{n-1} + \cdots + r_0 \in P \subseteq I,$$

whence $r_0 \in R \cap I = \mathfrak{p} = R \cap P \subseteq P$. Therefore

$$u^n + r_{n-1}u^{n-1} + \cdots + r_1 u = u(u^{n-1} + r_{n-1}u^{n-2} + \cdots + r_1) \in P.$$

By the choice of u and minimality of $\deg f$, $u \notin P$ and $u^{n-1} + r_{n-1}u^{n-2} + \cdots + r_1 \notin P$. We have contradiction because P is prime. □

Corollary 2.2.18 (Lying Over Theorem) *If A is integral over P then for every prime ideal $\mathfrak{p}$ of R there exists a prime ideal P of A which lies over $\mathfrak{p}$. More generally, for every ideal I of A such that $I \cap R \subseteq \mathfrak{p}$ there exists a prime ideal P of A which contains I and lies over $\mathfrak{p}$.*

Corollary 2.2.19 (Going Up Theorem) *Let $A \supseteq R$ be an integral ring extension, and $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ be prime ideals in R. If P_1 is a prime ideal of A lying over $\mathfrak{p}_1$, then there exists a prime ideal P_2 of A such that $P_1 \subseteq P_2$ and P_2 lies over $\mathfrak{p}_2$.*

Proof Take $\mathfrak{p} = \mathfrak{p}_2$ and $I = P_1$ in Lemma 2.2.17(i). □

Corollary 2.2.20 (Incomparability) *Let $A \supseteq R$ be an integral ring extension, and P_1, P_2 be prime ideals of A lying over a prime ideal $\mathfrak{p}$ of R. Then $P_1 \subseteq P_2$ implies $P_1 = P_2$.*

Proof Use Lemma 2.2.17(ii). □

The relation between prime ideals established above has further nice properties.

Theorem 2.2.21 (Maximality) *Let $A \supseteq R$ be an integral ring extension, and P be a prime ideal of A lying over a prime ideal $\mathfrak{p}$ of R. Then P is maximal if and only if $\mathfrak{p}$ is maximal.*

Proof If $\mathfrak{p}$ is not maximal, we can find a maximal ideal $\mathfrak{m} \supsetneq \mathfrak{p}$. By the Going Up Theorem, there is an ideal M of A lying over $\mathfrak{m}$ and containing P. It is clear that M actually containg P properly, and so P is not maximal.

Conversely, let $\mathfrak{p}$ be maximal in R. Let M be a maximal ideal containing P. Then $M \cap R \supseteq P \cap R = \mathfrak{p}$ and we cannot have $M \cap R = R$, as $1_R = 1_S \notin M$. It follows that $M \cap R = \mathfrak{p}$. Now $M = P$ by Incomparability Theorem. □

The previous results can be used to prove some useful properties concerning extensions of homomorphisms.

Lemma 2.2.22 *Let $A \supseteq R$ be an integral ring extension. If R is a field then $A \supseteq R$ is an algebraic field extension.*

Proof Let $\alpha \in A$ be a non-zero element. Then α is algebraic over R, hence $R[\alpha] \subseteq A$ is a field, and α is invertible. Hence A is a field. □

Proposition 2.2.23 *Let A be integral over R. Every homomorphism φ of R to an algebraically closed field F can be extended to A.*

Proof If R is a field, then A is an algebraic field extension of R by Lemma 2.2.22. Now the result follows from Proposition **??**.

If R is local, then $\ker \varphi$ is the maximal ideal $\mathfrak{m}$ of R. By Lying Over and Maximality Theorems, there is an ideal M of A lying over $\mathfrak{m}$. The inclusion $R \to A$ then induces an embedding of fields $R/\mathfrak{m} \to A/M$, which we use to identify $R/\mathfrak{m}$ with a subfield of A/M. Note that the field extension $A/M \supseteq R/\mathfrak{m}$ is algebraic. Since $\ker \varphi = \mathfrak{m}$, φ factors through the projection $R \to R/\mathfrak{m}$. The resulting homomorphism $\varphi : R/\mathfrak{m} \to F$ can be extended to $\psi : A/M \to F$ by Proposition **??**. Now if $\pi : A \to A/M$ is the natural projection, then $\psi \circ \pi$ is the desired extension of φ.

Now we consider the general case. Let $\mathfrak{p} := \ker \varphi$, a prime ideal in R, and $S = R \setminus \mathfrak{p}$. Then $S^{-1}A$ is integral over $S^{-1}R$ by Proposition 2.2.11(iv). Now $S^{-1}R = R_{\mathfrak{p}}$ is local. By the universal property of localizations, φ extends to a ring homomorphism $\hat{\varphi} : S^{-1}R \to F$. By the local case, $\hat{\varphi}$ extends to $\hat{\psi} : S^{-1}A \to F$, and the desired extension $\psi : A \to F$ is obtained by composing ψ with the natural homomorphism $A \to S^{-1}A$. □

Proposition 2.2.24 *Every homomorphism of a field k into an algebraically closed field can be extended to every finitely generated ring extension of k.*

Proof Let $\varphi : k \to F$ be a homomorphism to an algebraically closed field F and R be a finitely generated ring extension of k, so that $R = k[\alpha_1, \dots, \alpha_n]$ for some $\alpha_1, \dots, \alpha_n \in R$.

First assume that R is a field. By Proposition 2.2.23, we may assume that R is not algebraic over k. Let $\{\beta_1, \dots, \beta_t\}$ be a (necessarily finite) transcendence base of R over k. Each $\alpha \in R$ is algebraic over $k(\beta_1, \dots, \beta_t)$, i.e. satisfies a polynomial $a_k\alpha^k + \dots + a_1\alpha + a_0 = 0$ with coefficients $a_k, \dots, a_0 \in k(\beta_1, \dots, \beta_t)$, $a_k \neq 0$. Multiplying by a common denominator yields a polynomial equation

$$b_k\alpha^k + \dots + b_1\alpha + b_0 = 0$$

with coefficients $b_k, \dots, b_0 \in k[\beta_1, \dots, \beta_t]$, $b_k \neq 0$. Hence α is integral over $k[\beta_1, \dots, \beta_t, \frac{1}{b_k}]$. Applying this to $\alpha_1, \dots, \alpha_n$ yields nonzero $c_1, \dots, c_n \in k[\beta_1, \dots, \beta_t]$ such that $\alpha_1, \dots, \alpha_n$ are integral over $k[\beta_1, \dots, \beta_t, \frac{1}{c_1}, \dots, \frac{1}{c_n}]$. Set $c = c_1 \dots c_n$. Then $\alpha_1, \dots, \alpha_n$ are integral over $k[\beta_1, \dots, \beta_t, \frac{1}{c}]$, and hence R is integral over $k[\beta_1, \dots, \beta_t, \frac{1}{c}]$, see Proposition 2.2.7(ii). Let c^φ be the image of c under the homomorphism

$$k[\beta_1, \dots, \beta_t] \cong k[x_1, \dots, x_t] \to F[x_1, \dots, x_t]$$

induced by φ. As F is infinite there exist $\gamma_1, \dots, \gamma_t \in F$ such that $c^\varphi(\gamma_1, \dots, \gamma_t) \neq 0$. By the universal property of polynomial rings, there exists a homomorphism $\psi : k[\beta_1, \dots, \beta_t] \to F$ which extends φ and sends

$\beta_1, \ldots, \beta_t$ to $\gamma_1, \ldots, \gamma_t$, respectively. The universal property of localizations yields an extension of ψ to ring $k[\beta_1, \ldots, \beta_t, \frac{1}{c}] = k[\beta_1, \ldots, \beta_t]_c$. Now Proposition 2.2.23 extends φ to R, which completes the case where R is a field.

Now, let $R = k[\alpha_1, \ldots, \alpha_n]$ be any finitely generated ring extension of k. Let $\mathfrak{m}$ be a maximal ideal of R and $\pi : R \to R/\mathfrak{m}$ be the natural projection. Then $R/\mathfrak{m}$ is a field extension of $\pi(k) \cong k$ generated by $\pi(\alpha_1), \ldots, \pi(\alpha_n)$. By the first part of the proof, every homomorphism of $\pi(k)$ into F extends to $R/\mathfrak{m}$. Therefore every homomorphism of $k \cong \pi(k)$ extends to R. $\square$

Let K/k be a finite field extension. Consider K as a k-vector space. Then the map $x \mapsto ax$ is a k-linear map of this vector space. Define the *norm* $N_{K/k}(a)$ to be the determinant of this map. Note that $N_{K/k}|K^\times : K^\times \to k^\times$ is a group homomorphism.

Lemma 2.2.25 *If $a = a_1, \ldots, a_s$ be the roots with multiplicity of the minimal polynomial* $\mathrm{irr}\,(a, k)$ *(in some extension of the field K), then* $N_{K/k}(a) = (\prod_{i=1}^s a_i)^{[K:k(a)]}$.

Proof If $1 = v_1, v_2, \ldots, v_r$ is a basis of K over $k(u)$, then $\{a^i v_j \mid 0 \leq i < s, 1 \leq j \leq r\}$ is a basis of K over k in which the matrix of the map $x \mapsto ax$ is block diagonal with blocks all equal to the companion matrix of $\mathrm{irr}\,(a, k)$. $\square$

Lemma 2.2.26 *Let $S \subseteq R$ be integral domains with fields of fractions $k \subseteq K$, S be integrally closed, and $r \in R$ be integral over S. Then* $\mathrm{irr}\,(r, k) \in S[x]$.

Proof Let F be an extension of K which contains all roots $r = r_1, \ldots, r_s$ of $\mathrm{irr}\,(r, k)$. Then each r_i is integral over S. So the coefficients of $\mathrm{irr}\,(r, k)$, being polynomials in the r_i are also integral over S. As S is integrally closed, the coefficients belong to S. $\square$

Corollary 2.2.27 *Let $S \subseteq R$ be domains with fields of fractions $k \subseteq K$ such that the field extension K/k is finite. Assume that the ring extension $S \subseteq R$ is integral and that S is integrally closed. Then $N_{K/k}(r) \in S$ for any $r \in R$.*

Proof Apply Lemmas 2.2.25 and 2.2.26. $\square$

Lemma 2.2.28 (Noether's Normalization Lemma) *Let k be a field, and $R = k[x_1, \dots, x_n]$ be a domain, finitely generated over k with the field of fractions F. If $\operatorname{tr.deg}_k F = d$, then there exist algebraically independent over k elements $S_1, \dots, S_d \in R$ such that R is integral over $k[S_1, \dots, S_d]$.*

Theorem 2.2.29 (Going Down Theorem) *Let $S \subseteq R$ be an integral ring extension and S be integrally closed. Let $P_1 \supseteq P_2$ be prime ideals of S, and Q_1 be a prime ideal of R lying over P_1. Then there exists a prime ideal $Q_2 \subseteq Q_1$ lying over P_2.*

3
Affine and Projective Algebraic Sets

3.1 Zariski topology

Algebraic geometry is the subject which studies (algebraic) varieties. Naively, varieties are just algebraic sets.

Throughout we fix an algebraically closed ground field k. (It is much harder to develop algebraic geometry over non-algebraically closed fields and we will not try to do this). Denote by $\mathbb{A}^n$ the *affine space* k^n—this is just the set of all n-tuples of elements of k.

Definition 3.1.1 Let $S \subset k[T_1, \dots, T_n]$. A *zero* of the set S is an element $(x_1, \dots, x_n)$ of $\mathbb{A}^n$ such that $f(x_1, \dots, x_n) = 0$ for all $f \in S$. The *zero set* of S is the set $Z(S)$ of all zeros of S. An *algebraic set* in $\mathbb{A}^n$ (or *affine algebraic set*) is the zero set of some set $S \subset k[T_1, \dots, T_n]$, in which case S is called a set of *equations* of the algebraic set.

Example 3.1.2 The straight line $x+y-1=0$ and the 'circle' $x^2+y^2-1=0$ are examples of algebraic sets in $\mathbb{C}^2$. More generally, algebraic sets in $\mathbb{C}^2$ with a single equation are called complex algebraic curves. Note that the curve given by the equation $(x+y-1)(x^2+y^2-1)=0$ is the union of the line and the 'circle' above. On the other hand, the zero set of $\{x+y-4, x^2+y^2-1\}$ consists of two points $(1,0)$ and $(0,1)$. Finally, two more examples: $\varnothing = Z(1)$, and $\mathbb{C}^2 = Z(0)$.

Note that $Z(S) = Z((S))$, where (S) is the ideal of $k[T_1, \dots, T_n]$ generated by S. Therefore every algebraic set is the zero set of some ideal. Since $k[T_1, \dots, T_n]$ is noetherian by Hilbert's Basis Theorem, every algebraic set is the sero set of a finite set of polynomials.

Example 3.1.3 Let us try to 'classify' algebraic sets in $\mathbb{A}^1$ and $\mathbb{A}^2$.

(i) Algebraic sets in $\mathbb{A}^1$ are $\mathbb{A}^1$ itself and all finite subsets (including $\varnothing$).

(ii) Let X be an algebraic set in $\mathbb{A}^2$. It is given by a system of polynomial equations: $f_1(T_1, T_2) = \cdots = f_m(T_1, T_2) = 0$. If all polynomials are zero, we get $X = \mathbb{A}^2$. If $f_1, \ldots, f_m$ do not have a common divisor, then our system has only finitely many solutions, see Lemma 2.1.1. Finally, let all f_i have greatest common divisor $d(T_1, T_2)$. Then $f_i = dg_i$, where the polynomials $g_i(T_1, T_2)$ do not have a common divisor. Now, $X = X_1 \cup X_2$, where X_1 is given by the system $g_1 = \cdots = g_m = 0$, and X_2 is given by $d = 0$. As above X_1 is a finite (possibly empty) set of points, while X_2 is given by one non-trivial equation $d = 0$ (and can be thought of as a 'curve' in $\mathbb{A}^2$).

Proposition 3.1.4

(i) *Every intersection of algebraic sets is an algebraic set; the union of finitely many algebraic sets is an algebraic set.*

(ii) $\mathbb{A}^n$ *and* $\varnothing$ *are algebraic sets in* $\mathbb{A}^n$.

Proof (i) Let $(X_j = Z(I_j))_{j \in J}$ be a family of algebraic sets, given as zero sets of certain ideals I_j. To see that their intersection is again an algebraic set, it is enough to note that $\cap_{j \in J} Z(I_j) = Z(\sum_{j \in J} I_j)$. For the union, let $Z(I)$ and $Z(J)$ be algebraic sets corresponding to ideals I and J, and note that $Z(I) \cup Z(J) = Z(I \cap J)$ (why?).

(ii) $\mathbb{A}^n = Z(0)$ and $\varnothing = Z(1)$. $\square$

The proposition above shows that algebraic sets in $\mathbb{A}^n$ are closed sets of some topology. This topology is called the *Zariski topology*. Zariski toplology on $\mathbb{A}^n$ also induces Zariski topology on any subset of $\mathbb{A}^n$, in particular algebraic set. This topology is very weird and it takes time to get used to it. The main unintuitive thing here is that the topology is 'highly non-Hausdorf'—its open sets are huge. For example, we saw above that proper closed sets in k are exactly the finite sets, and so any two non-empty open sets intersect non-trivially.

Let $f \in k[T_1, \ldots, T_n]$. The corresponding *principal open set* is $\mathbb{A}^n \setminus Z(f) = \{x \in \mathbb{A}^n \mid f(x) \neq 0\}$. It is easy to see that each open set in $\mathbb{A}^n$ is a finite union of principal open sets, so principal open sets form a base of Zariski topology.

3.2 Nullstellensatz

The most important theorem of algebraic geometry is called Hilbert's Nullstellensatz (or theorem on zeros). It has many equivalent reformulations and many corollaries. The idea of the theorem is to relate algebraic sets in $\mathbb{A}^n$ (geometry) and ideals in $k[T_1, \dots, T_n]$ (commutative algebra). We have two obvious maps

$$Z : \{\text{ideals in } k[T_1, \dots, T_n]\} \to \{\text{algebraic sets in } \mathbb{A}^n\}$$

and

$$I : \{\text{algebraic sets in } \mathbb{A}^n\} \to \{\text{ideals in } k[T_1, \dots, T_n]\}.$$

We have already defined $Z(J)$ for an ideal J in $k[T_1, \dots, T_n]$. As for I, let X be any subset of $\mathbb{A}^n$. Then the ideal $I(X)$ is defined to be

$$I(X) := \{f \in k[T_1, \dots, T_n] \mid f(x_1, \dots, x_n) = 0 \text{ for all } (x_1, \dots, x_n) \in X\}.$$

Lemma 3.2.1 *Let X be any subset of $\mathbb{A}^n$. Then $Z(I(X)) = \bar{X}$, the closure of X in Zariski topology. In particular, if X is an algebraic set, then $Z(I(X)) = X$.*

Proof We have to show that for any algebraic set $Z(J)$ containing X we actually have $Z(I(X)) \subseteq Z(J)$. Well, as $X \subseteq Z(J)$, we have $I(X) \supseteq J$, which in turn implies $Z(I(X)) \subseteq Z(J)$. $\square$

Note, however, that Z and I do not give us a one-to one correspondence. For example, in $\mathbb{A}^1$ we have $Z((T)) = Z((T^2)) = \{0\}$, that is the different ideals (T) and (T^2) give the same algebraic set. Also, note that $I(\{0\}) = (T) \neq (T^2)$. Nullstellensatz sorts out problems like this in a very satisfactory way.

The first formulation of the Nulltellensatz is as follows (don't forget that k is algebraically closed, otherwise the theorem is wrong):

Theorem 3.2.2 (Hilbert's Nullstellensatz) *Let J be an ideal of $k[T_1, \dots, T_n]$. Then $I(Z(J)) = \sqrt{J}$.*

Proof First of all, it is easy to see that $\sqrt{J} \subseteq I(Z(J))$. Indeed, let $f \in \sqrt{J}$. Then $f^n \in J$. Then f^n is zero at every point of $Z(J)$. But this implies that f is zero at every point of $Z(J)$, i.e. $f \in I(Z(J))$.

The converse is much deeper. Let $f \in I(Z(J))$ and assume that no power of f belongs to J. Applying Lemma 2.1.4 to the multiplicative set $\{1, f, f^2, \dots\}$ yields a prime ideal P containing J but not f. Let

$R = k[T_1, \dots, T_n]/P$ and $\pi : k[T_1, \dots, T_n] \to R$ be the natural projection. Then R is a domain which is generated over $\pi(k) \cong k$ by $\alpha_1 := \pi(T_1), \dots, \alpha_n := \pi(T_n)$. We identify k and $\pi(k)$, and so π can be considered as a homomorphism of k-algebras. Under this agreement, $y := f(\alpha_1, \dots, \alpha_n) = \pi(f) \neq 0$, non-zero element of R, as $f \notin P$.

By Proposition 2.2.24, the identity isomorphism $k \to k$ can be extended to a homomorphism ψ from the subring $k[\alpha_1, \dots, \alpha_n, \frac{1}{y}]$ of the fraction field of R to k. Then $\psi(y) \neq 0$. So

$$f(\psi(\alpha_1), \dots, \psi(\alpha_n)) = \psi(f(\alpha_1, \dots, \alpha_n)) = \psi(y) \neq 0.$$

On the other hand, for any $g \in J \subseteq P$ we have

$$\begin{aligned} g(\psi(\alpha_1), \dots, \psi(\alpha_n)) &= \psi(g(\alpha_1, \dots, \alpha_n)) = \psi(g(\pi(T_1), \dots, \pi(T_n))) \\ &= \psi(\pi(g(T_1, \dots, T_n))) = \psi(\pi(g)) = \psi(0) = 0. \end{aligned}$$

Thus $(\psi(\alpha_1), \dots, \psi(\alpha_n))$ is a zero of J but not of f, i.e. $f \notin I(Z(J))$, a contradiction. □

Definition 3.2.3 We say that an ideal I of a commutative ring R is *radical* if $\sqrt{I} = I$.

The following corollary is also often called Nullstellensatz.

Corollary 3.2.4 *The maps I and Z induce an order-reversing bijection between algebraic sets in $\mathbb{A}^n$ and radical ideals in $k[T_1, \dots, T_n]$.*

Proof Note that $I(X)$ is always a radical ideal for any subset $X \subseteq \mathbb{A}^n$. Now the result follows from Theorem 3.2.2 and Lemma 3.2.1. □

Corollary 3.2.5 *Let J_1 and J_2 be two ideals of $k[T_1, \dots, T_n]$. Then $Z(J_1) = Z(J_2)$ if and only if $\sqrt{J_1} = \sqrt{J_2}$.*

Proof It is clear that $Z(J) = Z(\sqrt{J})$ for any ideal J, which gives the 'if'-part. The converse follows from Theorem 3.2.2. □

Corollary 3.2.6 *Every proper ideal of $k[T_1, \dots, T_n]$ has at least one zero in $\mathbb{A}^n$.*

Proof If $\sqrt{I} = k[T_1, \dots, T_n]$, then $I = k[T_1, \dots, T_n]$. Now the result follows from above. □

Let $x = (x_1, \dots, x_n) \in \mathbb{A}^n$. Denote $I(\{x\})$ by M_x, i.e.

$$M_x = \{f \in k[T_1, \dots, T_n] \mid f(x_1, \dots, x_n) = 0\}.$$

Corollary 3.2.7 *The mapping $x \mapsto M_x$ is a one-to-one correspondence between $\mathbb{A}^n$ and the maximal ideals of $k[T_1, \dots, T_n]$.*

Proof Note that the maximal ideals are radical and apply Nullstellensatz. □

3.3 Regular functions

Let $X \subseteq \mathbb{A}^n$ be an algebraic set. Every polynomial $f \in k[T_1, \dots, T_n]$ defines a k-valued function on $\mathbb{A}^n$ and hence on X via restriction. Such functions are called *regular* functions on X. The regular functions form a k-algebra with respect to the obvious 'point-wise operations'. The algebra is called the *coordinate algebra* (or *coordinate ring*) of X (or simply the *algebra/ring of regular functions* on X) and denoted $k[X]$. Clearly,

$$k[X] \cong k[T_1, \dots, T_n]/I(X).$$

If I is an ideal of $k[X]$ then we write $Z(I)$ for the set of all points $x \in X$ such that $f(x) = 0$ for every $f \in I$, and if Z is a subset of X we denote by $I(Z)$ the ideal of $k[X]$ which consists of all functions $f \in k[X]$ such that $f(z) = 0$ for every $z \in Z$. Note that closed subsets of X all look like $Z(I)$.

Now the Nullstellensatz and the correspondence theorem for ideals imply:

Theorem 3.3.1 (Hilbert's Nullstellensatz) *Let X be an algebraic set.*

(i) *If J is an ideal of $k[X]$, then $I(Z(J)) = \sqrt{J}$.*
(ii) *The maps I and Z induce an order-reversing bijection between closed sets in X and radical ideals in $k[X]$.*
(iii) *Every proper ideal of $k[X]$ has at least one zero in X.*
(iv) *The mapping $x \mapsto M_x = \{f \in k[X] \mid f(x) = 0\}$ is a one-to-one correspondence between X and the maximal ideals of $k[X]$.*

Definition 3.3.2 A commutative finitely generated k-algebra without nilpotent elements is called an *affine k-algebra*.

Proposition 3.3.3

(i) *Let X be an algebraic set. Then $k[X]$ is an affine k-algebra.*
(ii) *Every affine k-algebra A is isomorphic to $k[X]$ for some affine algebraic set X.*

Proof (i) clear. For (ii), if $A = k[\alpha_1, \dots, \alpha_n]$ is an k-algebra generated by $\alpha_1, \dots, \alpha_n$, then by the universal property of polynomial rings, $A \cong k[T_1, \dots, T_n]/I$ for some radical ideal I. So $I = I(X)$ for some algebraic set X by the Nulltellensatz. $\square$

Let $f \in k[X]$. The corresponding *principal open set* is

$$X_f := X \setminus Z(f) = \{x \in X \mid f(x) \neq 0\}. \tag{3.1}$$

Each open set in X is a finite union of principal open sets, so principal open sets form a base of Zariski topology.

Example 3.3.4

(i) If X is a point, then $k[X] = k$.
(ii) If $X = \mathbb{A}^n$, then $k[X] = k[T_1, \dots, T_n]$.
(iii) Let $X \subset \mathbb{A}^2$ be given by the equation $T_1T_2 = 1$. Then $k[X]$ is isomorphic to the localization $k[t]_t \cong k[t, t^{-1}]$.

3.4 Irreducible components

Definition 3.4.1 A topological space is *noetherian* if its open sets satisfy the ascending chain condition.

A topological space is *irreducible* if it cannot be written as a union of its two proper closed subsets.

Note that a non-empty open subset of an irreducible topological space X is dense in X, and that any two non-empty open subsets of X intersect non-trivially. Problem 3.13.18 contains some further important properties of irreducible spaces.

Lemma 3.4.2 *$\mathbb{A}^n$ with Zariski topology is noetherian. Hence the same is true for any subspace of $\mathbb{A}^n$.*

Proof An ascending chain of open sets corresponds to a descending chain of closed sets, which, by the Nullstellensatz, corresponds to an ascending chain of radical ideals of $k[T_1, \ldots, T_n]$, which stabilizes since $k[T_1, \ldots, T_n]$ is noetherian. $\square$

Lemma 3.4.3 *Algebraic set $X \subseteq \mathbb{A}^n$ is irreducible if and only if the ideal $I(X)$ is prime.*

Proof If X is irreducible and $f_1, f_2 \in k[T_1, \ldots, T_n]$ with $f_1 f_2 \in I(X)$, then $X \subseteq Z((f_1)) \cup Z((f_2))$, and we deduce that $X \subseteq Z((f_1))$ or $X \subseteq Z((f_2))$, i.e. $f_1 \in I(X)$ or $f_2 \in I(X)$.

Conversely, if $I(X)$ is prime and $X = X_1 \cup X_2$ for proper closed subsets X_1, X_2, then there are polynomials $f_i \in I(X_i)$ with $f_i \notin I(X)$. But $f_1 f_2 \in I(X)$, contradiction. $\square$

Since prime ideals are radical, Lemma 3.4.3 allows us to further refine the one-to-one correspondence between radical ideals and algebraic sets: under this correspondence prime ideals correspond to irreducible algebraic sets. Also note that X is irreducible if and only if $k[X]$ is a domain. So for irreducible algebraic sets X we can form the quotient field of $k[X]$ is called the *field of rational functions* on X and denoted $k(X)$. In a natural way, $k(X)$ is a field extension of k.

We now establish a general fact on noetherian topological spaces, which in some sense reduces the study of algebraic sets to that of irreducible algebraic sets.

Proposition 3.4.4 *Let X be a noetherian topological space. Then X is a finite union $X = X_1 \cup \cdots \cup X_r$ of irreducible closed subsets. If one assumes that $X_i \not\subseteq X_j$ for all $i \neq j$ then the X_i are unique up to permutation. They are called the irreducible components of X and can be characterized as the maximal irreducible closed subsets of X.*

Proof Let X be a topological noetherian space for which the first statement is false. Then X is reducible, hence $X = X_1 \cup X_1'$ for proper closed subsets X_1, X_1'. Moreover, the first statement is false for at least one of X_1, X_1'. Continuing this way, we get an infinite chain $X \supsetneq X_1 \supsetneq \cdots \supsetneq X_2 \supsetneq \ldots$ of closed subsets, which is a contradiction, as X is noetherian.

To show uniqueness, assume that we have two irredundant decompositions $X = X_1 \cup \cdots \cup X_r$ and $X = X_1' \cup \cdots \cup X_s'$. For each i, $X_i \subseteq (X_1' \cap X_i) \cup \cdots \cup (X_s' \cap X_i)$, so by irreducibility of X_i we may assume that $X_i \subseteq X_{\sigma(i)}'$ for some $\sigma(i)$. For the same reason, $X_j' \subseteq X_{\tau(j)}$ for some $\tau(j)$. Now the irredundancy of the decompositions implies that σ and τ are mutually inverse bijections between $\{1, \dots, r\}$ and $\{1, \dots, s\}$, and $X_i = X'_{\sigma(i)}$ for all i. $\square$

3.5 Category of algebraic sets

We now define morphisms between algebraic sets. Let $X \subseteq \mathbb{A}^n$, $Y \subseteq \mathbb{A}^m$ be two algebraic sets and consider a map $\varphi : X \to Y$. Let $T_1, \dots, T_n$ and $S_1, \dots, S_m$ be the coordinate functions on $\mathbb{A}^n$ and $\mathbb{A}^m$, respectively. Denote $S_i \circ \varphi$ by φ_i for all $1 \leq i \leq m$. So that we can think of φ as the m-tuple of functions $\varphi = (\varphi_1, \dots, \varphi_m)$, where $\varphi_i : X \to k$, and $\varphi(x) = (\varphi_1(x), \dots, \varphi_m(x)) \in \mathbb{A}^m$. The map $\varphi : X \to Y$ is called a *morphism of algebraic sets* or a *regular map* from X to Y if each function $\varphi_i : X \to k$, $1 \leq i \leq n$ is a regular function on X. It is easy to see that algebraic sets and regular maps form a category, in particular a composition of regular maps is a regular map again.

Now, let $\varphi : X \to Y$ be a morphism of algebraic sets as above. This morphism defines the 'dual' morphism $\varphi^* : k[Y] \to k[X]$ of coordinate algebras, as follows:

$$\varphi^* : k[Y] \to k[X] : \ f \mapsto f \circ \varphi.$$

It is clear that φ^* is a homomorphism of k-algebras. Moreover, $(\varphi \circ \psi)^* = \psi^* \circ \varphi^*$ and $\mathrm{id}^* = \mathrm{id}$, i.e. we have a contravariant functor $\mathcal{F}$ from the category of algebraic sets to the category of affine k-algebras. To reiterate: $\mathcal{F}(X) = k[X]$ and $\mathcal{F}(\varphi) = \varphi^*$.

Theorem 3.5.1 *The functor $\mathcal{F}$ from the category of algebraic sets (over k) to the category of affine k-algebras is a (contravariant) equivalence of categories.*

Proof In view of Theorem 1.0.2 (for contravariant functors) and Proposition 3.3.3(ii) we just need to show that $\varphi \mapsto \varphi^*$ establishes a one-to one correspondence between regular maps $\varphi : X \to Y$ and algebra homomorphisms $k[Y] \to k[X]$, for arbitrary fixed algebraic sets $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$. Let $T_1, \dots, T_n$ and $S_1, \dots, S_m$ be the coordinate functions on $\mathbb{A}^n$ and $\mathbb{A}^m$, respectively.

Let $\alpha : k[Y] \to k[X]$ be an k-algebra homomorphism. Set $s_j := S_j|_Y \in k[Y]$, $1 \leq j \leq m$. Then $\alpha(s_j)$ are regular functions on X. Define the regular map $\alpha_* : X \to \mathbb{A}^m$ as follows:

$$\alpha_* := (\alpha(s_1), \dots, \alpha(s_m)).$$

We claim that in fact $\alpha_*(X) \subseteq Y$. Indeed, let $x \in X$ and $f = \sum_{\mathbf{k}} c_{\mathbf{k}} S_1^{k_1} \dots S_m^{k_m} \in I(Y)$, where $\mathbf{k}$ stands for the m-tuple $(k_1, \dots, k_m)$. It suffices to prove that $f(\alpha_*(x)) = 0$. Using $f(s_1, \dots, s_m) = 0$ and the fact that α is an algebra homomorphism, we have

$$\begin{aligned} f(\alpha_*(x)) &= f(\alpha(s_1)(x), \dots, \alpha(s_m)(x)) \\ &= \sum_{\mathbf{k}} c_{\mathbf{k}} (\alpha(s_1)(x))^{k_1} \dots (\alpha(s_m)(x))^{k_m} \\ &= \alpha(\sum_{\mathbf{k}} c_{\mathbf{k}} s_1^{k_1} \dots s_m^{k_m})(x) \\ &= \alpha(f(s_1, \dots, s_m))(x) = 0. \end{aligned}$$

Now, to complete the proof of the theorem, it suffices to check that $(\varphi^*)_* = \varphi$ and $(\alpha_*)^* = \alpha$ for any regular map $\varphi : X \to Y$ and any k-algebra homomorphism $\alpha : k[Y] \to k[X]$. Well,

$$(\varphi^*)_* = (\varphi^*(s_1), \dots, \varphi^*(s_m)) = (\varphi_1, \dots, \varphi_m) = \varphi.$$

On the other hand,

$$((\alpha_*)^*)(s_i) = s_i \circ \alpha_* = \alpha(s_i)$$

for any $1 \le i \le m$. Since the s_i generate $k[Y]$, this implies that $(\alpha_*)^* = \alpha$. ☐

Corollary 3.5.2 *Two (affine) algebraic sets are isomorphic if and only if their coordinate algebras are isomorphic.*

Lemma 3.5.3 *Regular maps are continuous in the Zariski topology.*

Proof Let $\varphi : X \to Y \subseteq \mathbb{A}^m$ be a regular map. As the topology on Y is induced by that on $\mathbb{A}^m$, it suffices to prove that any regular map $\varphi : X \to \mathbb{A}^m$ is continuous. Let $Z = Z(I)$ be a closed subset of $\mathbb{A}^m$. We claim that $\varphi^{-1}(Z) = Z(J)$ where J is the ideal of $k[X]$ generated by $\varphi^*(I)$. Well, if $x \in Z(J)$, then $f(\varphi(x)) = \varphi^*(f)(x) = 0$ for any $f \in I$, so $\varphi(x) \in Z(I)$, i.e. $x \in \varphi^{-1}(Z)$. The argument is easily reversed. ☐

Remark 3.5.4 Note that regular maps from X to Y usually do not exhaust all continuous maps from X to Y, so the category of algebraic sets is not a full subcategory of the category of topological spaces. For example, if $X = Y = \mathbb{C}$, the closed subsets in X and Y are exactly the finite subsets, and there are lots of non-polynomial maps from $\mathbb{C}$ to $\mathbb{C}$ such that inverse image of a finite subset is finite (describe one!).

Remark 3.5.5 The proof of Proposition 3.3.3 allows us to 'find' X from $k[X]$. More careful look at the proof however shows that we do not have a functor from affine algebras to algebraic sets, as 'recovering' X from $k[X]$ is not canonical—it depends on the choice of generators in $k[X]$, so only 'recover X up to isomorphism'. The problem here is that our definition of algebraic sets is not a 'right one'—it relies on embedding into some $\mathbb{A}^n$, and this is something which we want to eventually avoid.

At this stage, we can at least canonically recover X from $k[X]$ as a *topological space*. Indeed, we know that as a set, X is in bijection with the set $\operatorname{Specm} k[X]$ of maximal ideals of the algebra $k[X]$. So if we want to construct a reasonable quasi-inverse functor $\mathcal{G}$ to the functor $\mathcal{F}$, we could associate $\operatorname{Specm} k[X]$ to $k[X]$. Now make $\operatorname{Specm} k[X]$ into a topological space by considering the topology whose basis consists of all $X_f := \{M \in \operatorname{Specm} \mid f \notin M\}$. Then $x \mapsto M_x$ is a homeomorphism from X to $\operatorname{Specm} X$. Finally, if $\alpha : k[Y] \to k[X]$ is an algebra homomorphism define $\mathcal{G}(\alpha) : \operatorname{Specm} k[X] \to \operatorname{Specm} k[Y]$ as follows: if $M \in \operatorname{Specm} k[X]$ then $\mathcal{G}(M)$ is the maximal ideal N in $k[Y]$ containing $\alpha^{-1}(M)$. Note that if we identify X with $\operatorname{Specm} k[X]$ as above, and $\varphi : X \to Y$ is a morphism, then $\varphi = \mathcal{G}(\varphi^*)$—in other words, $M_{\varphi(x)}$ is the maximal ideal of $k[Y]$ containing $(\varphi^*)^{-1}(M_x)$.

Example 3.5.6

(i) The notion of a regular function on X and a regular map from X to k coincide.

(ii) Projection $f(T_1, T_2) = T_1$ is a regular map of the curve $T_1T_2 = 1$ to k.

(iii) The map $f(t) = (t, t^k)$ is an isomorphism from k to the curve $y = x^k$.

(iv) The map $\alpha(t) = (t^2, t^3)$ is a regular map from k to the curve $X \subset \mathbb{A}^2$ given by $x^3 = y^2$. This map is clearly one-to-one, but it is *not* an isomorphism (even though it is a homeomorphism!) Indeed, any regular function on X has a representative $p(x) + q(x)y$ in $k[x, y]$ for some $p, q \in k[x]$. Now $\alpha^*(p(x)+q(x)y) = p(t^2)+q(t^2)t^3$, which is never equal to t, for example. So α^* is not surjective.

Moreover, one can see that X is not isomorphic to $\mathbb{A}^1$, since $k[X] \not\cong k[T]$.

Example 3.5.7 Let X be an algebraic set, and G be its finite group of automorphisms. Then G is also a group of automorphisms of the algebra $A = k[X]$. Suppose that $\operatorname{char} k \not| |G|$. Then the invariant algebra A^G is an affine algebra (the only non-trivial thing here is that it is finitely generated, which can be looked up in [Sh, Appendix].) So there is an algebraic set Y with $k[Y] = A^G$, and the regular map $\pi : X \to Y$ with π^* being the embedding of A^G into A. This algebraic set Y is called the *quotient* of X by G and is denoted X/G. The map π leads to a natural one-to-one correspondence between the elements of X/G and the G-orbits on X.

Indeed, we claim that for $x_1, x_2 \in X$, one has $\pi(v_1) = \pi(v_2)$ if and only if x_1 and x_2 are in the same G-orbit. Well, if $x_2 = gx_1$, then $f(x_1) = f(x_2)$ for all $f \in A^G = k[Y]$, and so $\pi(x_1) = \pi(x_2)$. Conversely, if x_1 and x_2 are not in the same orbit, then let $f \in k[X]$ be a function with $f(gT_2) = 1$ and $f(gT_1) = 0$ for all $g \in G$ (why does it exist?). Then the average function $S(f) := \frac{1}{|G|}\sum_{g\in G} g^* f$ belongs to A^G and 'separates' x_1 from x_2. So $\pi(x_1) \neq \pi(x_2)$.

Finally, in view of Remark 3.5.5, the surjectivity of π follows from the Lying Over Theorem and the Maximality Theorem 2.2.21, if we can establish that A is integral over A^G. Well, for any element $f \in A$, the coefficients of the polynomial

$$t^N + a_1 t^{N-1} + \cdots + a_N = \prod_{g\in G}(t - g \cdot f) =: P_f(t)$$

belong to A^G, as they are elementary symmetric functions in $g \cdot f$. On the other hand $P_f(f) = 0$.

3.6 Products

Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be algebraic sets. Then the cartesian product $X \times Y$ is an algebraic set in $\mathbb{A}^{n+m}$. Indeed, if we identify $k[T_1, \dots, T_{m+n}]$ with $k[T_1, \dots, T_n] \otimes k[T_1, \dots, T_m]$, then it is easy to see that $I(X \times Y) = I(X) \otimes k[T_1, \dots, T_m] + k[T_1, \dots, T_n] \otimes I(Y)$ (check it!).

From Proposition 2.1.2 we get

$$k[X \times Y] \cong k[X] \otimes k[Y]. \tag{3.2}$$

Lemma 3.6.1 *Tensor product $A \otimes B$ of affine k algebras is an affine k-algebra. Moreover, if A and B are domains, then so is $A \otimes B$.*

Proof The first statement follows from (3.2) and Proposition 3.3.3. Assume A and B are domains and $\alpha, \alpha' \in A \otimes B$ be such that $\alpha\alpha' = 0$. Write $\alpha = \sum a_i \otimes b_i$ and $\alpha' = \sum a'_i \otimes b'_i$ with the sets $\{b_i\}$ and $\{b'_i\}$ each linearly independent. Let M be a maximal ideal in A, and $\bar{a}$ denote $a + M \in A/M = k$. As $(\sum a_i \otimes b_i)(\sum a'_i \otimes b'_i) = 0$ in $A \otimes B$, in $A/M \otimes B = k \otimes B = B$ we have $(\sum \bar{a}_i \otimes b_i)(\sum \bar{a}'_i \otimes b'_i) = 0$. As B is domain and the sets $\{b_i\}$ and $\{b'_i\}$ are linearly independent, it follows that either all $a_i \in M$ or all $a'_i \in M$. Now, recall from Proposition 3.3.3 that $A \cong k[X]$ for some irreducible variety X. Consider the subvarieties Y and Y' of X which are zero sets of the functions $\{a_i\}$ and $\{a'_i\}$, respectively. $\square$

Corollary 3.6.2 *If X and Y are irreducible then so is $X \times Y$.*

Remark 3.6.3 Zariski topology on $X \times Y$ is *not* the product topology of those on X and Y.

Example 3.6.4 This is a generalization of Example 3.5.6(ii). Let X be a closed set in $\mathbb{A}^n$ and $f \in k[X]$. Consider the set $X' \subseteq X \times \mathbb{A}^1 \subset \mathbb{A}^{n+1}$ given by the equation $T_{n+1} f(T_1, \dots, T_n) = 1$. Note that $k[X'] \cong k[X]_f$. Then the projection $\pi(T_1, \dots, T_n, T_{n+1}) = (T_1, \dots, T_n)$ defined a regular map $\pi : X' \to X$. This map defines a homeomorphism between X' and the principal open set X_f. This idea will be used to consider a principal open set as an algebraic variety. In fact, it will turn out that $k[X_f] = k[X]_f$.

3.7 Rational functions

In algebraic geometry we need more functions than just globally defined regular functions on a variety X. In fact, if we were planning to deal only with affine algebraic sets such globally defined functions would be 'enough' in view of Theorem 3.5.1. However, we will see that constant functions are the only globally defined regular functions on a projective variety. So, as in complex analysis we are going to allow some 'poles' and consider functions which are not defined everywhere on X.

Definition 3.7.1 Let X be an irreducible algebraic set. The field of fractions of the ring $k[X]$ is denoted $k(X)$ and is called the *field of rational functions* on X, its elements being *rational functions* on X. A rational function $\varphi \in k(X)$ is *regular* at the point $x \in X$ if it can be written in the form $\varphi = \frac{f}{g}$ for $f, g \in k[X]$ with $g(x) \neq 0$. In this case (the well-defined number) $\frac{f(x)}{g(x)}$ is called the *value* of φ at x and is denoted $\varphi(x)$.

Note that the set of points on which a rational function φ on X is regular is non-empty and open, and hence dense in X. This set is called the *domain* of φ. As the intersection of two non-empty open sets in an irreducible space is non-empty and open again, we can compare a finite set of rational functions on a non-empty open set. Another useful remark is that a rational function is uniquely determined by its values on a non-empty open set. Indeed, if $\varphi = 0$ on such a set U, then taking some presentation $\varphi = \frac{f}{g}$ for φ, we see that f is zero on a non-empty open set $U \cap (X \setminus Z(g))$, which is dense in X, so $f = 0$.

Theorem 3.7.2 *Rational function φ regular at all points of an irreducible affine algebraic set X is a regular function on X.*

Proof By assumption, for every $x \in X$ we can write $\varphi(x) = \frac{f_x(x)}{g_x(x)}$ for $f_x, g_x \in k[X]$ with $g_x(x) \neq 0$. Then the zero set in X of the ideal generated by all functions g_x is empty, so by the Nullstellensatz the ideal equals $k[X]$. So there exist functions $h_1, \dots h_n \in k[X]$ and points $x_1, \dots, x_n \in X$ such that $\sum_{i=1}^n h_i g_{x_i} = 1$. Multiplying both sides of this equality by φ (in $k(X)$) and using the fact that $\varphi = \frac{f_{x_i}}{g_{x_i}}$, we get $\varphi = \sum_{i=1}^n h_i f_{x_i}$, so $\varphi \in k[X]$. $\square$

The subring of $K(X)$ consisting of all functions regular at the point $x \in X$ is denoted $\mathcal{O}_x$ and called the *local ring* of x. Note that $\mathcal{O}_x \cong k[X]_{M_x}$, the localization of $k[X]$ at the maximal ideal M_x. So $\mathcal{O}_x$ is a local ring in the sense of commutative algebra with the maximal ideal $\mathfrak{m}_x$ consisting of all rational functions representable in the form $\frac{f}{g}$ with $f(x) = 0 \neq g(x)$. Now Theorem 3.7.2 can be interpreted as

$$k[X] = \cap_{x \in X} \mathcal{O}_x. \tag{3.3}$$

Informally speaking the local ring $\mathcal{O}_x$ describes what happens 'near the point x'. This becomes a little more clear if we note that $\mathcal{O}_x$ is the same as the *stalk* of rational functions at x: the elements of the stalk are *germs* of rational functions at x. One can think of germs as equivalence classes of pairs (U, f), where U is an open set containing x, f is a rational function regular at all points of U, and $(U, f) \sim (V, g)$ if there is an open set $W \subset U \cap V$ and $f|W = g|W$.

Now, let $X \subseteq \mathbb{A}^n$ be an arbitrary (not necessarily irreducible) algebraic set and $U \subseteq X$ be an open subset. A function $f : U \to k$ is *regular* if for each $x \in U$ there exist $g, h \in k[T_1, \dots, T_n]$ such that $h(x) \neq 0$ and $f = \frac{g}{h}$ in some open neighborhood of x. The algebra of all regular functions on U is denoted $\mathcal{O}_X(U)$. Now $\mathcal{O}_x$ is defined as the stalk of functions regular in neighborhoods of x.

Now, let $X \subseteq \mathbb{A}^n$ be an affine algebraic set and $0 \neq f \in k[X]$. Then the elements of the localization $k[X]_f$ can be considered as regular functions on the principal open set X_f (we do imply here that different elements of $k[X]_f$ give different functions—check!) We claim that these are precisely all regular functions on X_f:

Theorem 3.7.3 *$k[X]_f$ is the algebra of regular functions on X_f.*

Proof Let g be a regular function on X_f. So we can find an open covering of X_f such that on each element U of this covering g equals $\frac{a}{b}$ for $a, b \in k[T_1, \dots, T_n]$ (with $b(x) \neq 0$ for all $x \in U$). But principal open sets form a basis of Zariski topology on $\mathbb{A}^n$, and the topology is noetherian. So we may assume that $X_f = X_{g_1} \cup \dots \cup X_{g_l}$ and $g = \frac{a_i}{b_i}$ on X_{g_i} for $i = 1, \dots, l$. Then $X_{g_i} \subseteq X_{b_i}$. From now on we consider all functions as functions on X via restriction. By the Nullstellensatz, for each i, we have $g_i^{n_i} = b_i h_i$ for some $n_i \in \mathbb{Z}_{\geq 0}$ and $h_i \in k[X]$. Note that $h_i(x) \neq 0$ for any $x \in X_{g_i}$, so

$$\frac{a_i}{b_i} = \frac{a_i h_i}{b_i h_i} = \frac{a_i h_i}{g_i^{n_i}}.$$

on X_{g_i}. As $X_{g_i} = X_{g_i^{n_i}}$, renaming $a_i h_i$ as a_i and $g_i^{n_i}$ as g_i we have that $g = \frac{a_i}{g_i}$ on X_{g_i}.

Now, on $X_{g_i} \cap X_{g_j} = X_{g_i g_j}$ we have $\frac{a_i}{g_i} = \frac{a_j}{g_j}$, whence $a_i g_j - a_j g_i = 0$, therefore $(a_i g_j - a_j g_i) g_i g_j = 0$ everywhere on X. So $a_i g_i g_j^2 = a_j g_i^2 g_j$. Moreover, on X_{g_i} we have $\frac{a_i}{g_i} = \frac{a_i g_i}{g_i^2}$. Renaming $a_i g_i$ as a_i and g_i^2 as g_i, we are reduced to the case $g = \frac{a_i}{g_i}$ on X_{g_i} and $a_i g_j = a_j g_i$ on X. Now the condition $X_f = X_{g_1} \cup \dots \cup X_{g_l}$ and the Nulstellensatz imply $f^n = \sum_i c_i g_i$ for some $c_i \in k[X]$ for some n. So

$$g f^n | X_{g_j} = \frac{a_j}{g_j} f^n = \frac{a_j}{g_j} \sum_i c_i g_i = \sum_i \frac{a_j g_i c_i}{g_j} = \sum_i \frac{a_i g_j c_i}{g_j} = \sum_i a_i c_i.$$

Since X_{g_i}'s cover X_f, it follows that $gf^n = \sum_i c_i a_i$ on X_f. So $g = \frac{\sum_i c_i a_i}{f^n} \in k[X]_f$, as required. $\square$

3.8 Projective n-space

The objects that algebraic geometry can study are much more diverse than just affine algebraic set. To extend our horizons we now demonstrate how *projective algebraic sets* can be studied. Algebraically, this just means considering *homogeneous* polynomials instead of all polynomials.

Define the *projective n-space* $\mathbb{P}^n$ as the set of equivalence classes on $k^{n+1} \setminus \{(0, \dots, 0)\}$ with respect to the following equivalence relation: $(x_0, x_1, \dots, x_n) \sim (y_0, y_1, \dots, y_n)$ if and only if there exists an element $c \in k^\times$ such that $y_i = cx_i$ for all $i = 0, 1, \dots, n$.

Thus every point of $\mathbb{P}_n$ has $n + 1$ coordinates $x_0, \dots, x_n$, which are only defined up to a non-zero scalar multiple. To emphasize this fact we will refer to the coordinates of this point as the *homogeneous coordinates* and denote them by

$$(x_0 : x_1 : \cdots : x_n).$$

If we want to consider subsets of $\mathbb{P}^n$ which are zero sets of polynomials in the homogeneous coordinate functions $S_0, S_1, \dots, S_n$ we have to require that these polynomials are homogeneous.

Definition 3.8.1 Let S be a set of homogeneous polynomials in $k[S_0, S_1, \dots, S_n]$. A *zero* of the set S is an element $(x_0 : x_1 : \cdots : x_n)$ of $\mathbb{P}^n$ such that $f(x_0, x_1, \dots, x_n) = 0$ for all $f \in S$. The *zero set* of S is the set $Z(S)$ of all zeros of S. An *algebraic set* in $\mathbb{P}^n$ (or *projective algebraic set*) is the zero set of some set of homogeneous polynomials $S \subseteq k[S_0, S_1, \dots, S_n]$, in which case S is called a set of *equations* of the algebraic set.

Note that $Z(S) = Z((S))$, where (S) is the ideal of $k[S_0, S_1, \dots, S_n]$ generated by S. Therefore every algebraic set is the zero set of some *homogeneous* ideal. Now, by Hilbert's Basis Theorem, every algebraic set is the sero set of a finite set of homogeneous polynomials.

As in the affine case, one proves that the algebraic sets are closed sets of a topology on $\mathbb{P}^n$, which again is called the *Zariski topology.* Principal open sets form a base of this topology.

The map

$$I : \{\text{algebraic sets in } \mathbb{P}^n\} \to \{\text{homogeneous ideals in } k[S_0, \dots, S_n]\}$$

is defined in the obvious way (you need to check that $I(X)$ is homogeneous!).

Definition 3.8.2 The ideal M_0 of $k[S_0, \dots, S_n]$ generated by $S_0, \dots, S_n$ is called the *superfluous ideal*.

The following projective version of the Nullsellensatz follows easily from the classical one.

Theorem 3.8.3 (Projective Nullstellensatz) *The maps I and Z induce an order-reversing bijection between algebraic sets in $\mathbb{P}^n$ and non-superfluous homogeneous radical ideals in $k[S_0, \dots, S_n]$. Under this correspondence, irreducible algebraic sets correspond to the prime ideals.*

Let $U_i \subset \mathbb{P}^n$ be the subset consisting of all points with non-zero ith homogeneous coordinate. This is the principal open set corresponding to the function S_i. We call the U_i (the ith) *affine open set* in $\mathbb{P}^n$. The terminology is justified by the following. The map

$$\alpha_i : (x_0, \dots, x_n) \mapsto (x_0/x_i, \dots, x_{i-1}/x_i, x_{i+1}/x_i, \dots, x_n/x_i)$$

is a bijection between U_i and $\mathbb{A}^n$. We will refer to the functions

$$T_j : (x_0, \dots, x_n) \mapsto x_j/x_i, \qquad (j = 0, \dots, i-1, i+1, \dots, n)$$

as the *affine coordinates* on U_i.

We claim that α_i is not just a bijection but a homeomorphism between U_i and $\mathbb{A}^n$. Indeed, to each polynomial $f(T_0, \dots, T_{i-1}, T_{i+1}, \dots, T_n)$ we associate its *homogenization*

$$\hat{f}(S_0, \dots, S_n) := S_i^{\deg f} f(S_0/S_i, \dots, S_{i-1}/S_i, S_{i+1}/S_i, \dots, S_n/S_i),$$

which is clearly a homogeneous polynomial in $S_0, \dots, S_n$. Now, if X in $\mathbb{A}^n$ is the zero set of polynomials $f_1, \dots, f_m \in k[T_0, \dots, T_{i-1}, T_{i+1}, \dots, T_n]$, then

$$\alpha^{-1}(X) = U_i \cap Z(\hat{f}_1, \dots, \hat{f}_m).$$

We note in passing, that $Z(\hat{f}_1, \dots, \hat{f}_m)$ is the closure in $\mathbb{P}^n$ of $\alpha^{-1}(X)$ (why?). Conversely, to each homogeneous polynomial $g(S_0, \dots, S_n)$ we associate the polynomial

$$\bar{g}(T_0, \dots, T_{i-1}, T_{i+1}, \dots, T_n) := g(T_0, \dots, T_{i-1}, 1, T_{i+1}, \dots, T_n).$$

Now

$$\alpha(Z(g_1, \dots, g_l) \cap U_i) = Z(\bar{g}_1, \dots, \bar{g}_l).$$

Lemma 3.8.4 (Affine Criterion) *Let X be a topological space with an open cover $X = \cup_{i \in I} U_i$, and $Y \subseteq X$. Then Y is closed if and only $Y \cap U_i$ is closed in U_i for all i. In particular, a subset Y of $\mathbb{P}^n$ is closed if and only if its intersection $Y \cap U_i$ with the ith affine open set is closed in U_i for all i.*

Proof The 'only-if' part is obvious. For the 'if' part, by assumption each $Y \cap U_i = Z_i \cap U_i$ for some closed set Z_i in $\mathbb{P}^n$. It suffices to check that

$$Y = \cap_{i \in I} (Z_i \cup (\mathbb{P}^n \setminus U_i)).$$

Well, let $y \in Y$ and $i \in I$. Either $y \in U_i$ and then $y \in Y \cap U_i \subset Z_i$, or $y \in \mathbb{P}^n \setminus U_i$. Conversely, if $y \in Z_i \cup (\mathbb{P}^n \setminus U_i)$ for all i. As $\mathbb{P}^n = \cup U_i$, there is an i with $y \in U_i$. Then $y \notin \mathbb{P}^n \setminus U_i$, hence $y \in Z_i$, and $x \in Z_i \cap U_i \subset Y$. $\square$

3.9 Functions

A rational expression $f = \frac{p(S_0,\dots,S_n)}{q(S_0,\dots,S_n)}$ can be considered as a function on $\mathbb{P}^n$ (defined at the points where $q(S_0, \dots, S_n) \neq 0$) only if p and q are homogeneous of the same degree, in which case we will refer to f as a rational function of degree 0. Let $X \subset \mathbb{P}^n$ be a projective algebraic set, $x = (x_0, \dots, x_n) \in X$, and $f = \frac{p}{q}$ be of degree 0. If $q(x_0, \dots, x_n) \neq 0$, then we say that f is *regular* at x. If a degree 0 rational function is regular at x, then it is also regular on some neighborhood of x. For any set $Y \subseteq \mathbb{P}^n$, a function f on Y is called *regular* if for any $x \in Y$ there exists a rational function g regular at x and such that $f = g$ on some open neighborhood of x in Y. If U is an open subset of X we write $\mathcal{O}_X(U)$ for the set of all regular functions on U.

We will prove later that the only functions regular on projective algebraic sets are constants. This underscores the importance of considering rational functions regular only on some open subsets.

Let U be an open subset of $\mathbb{P}^n$ contained in some affine open set U_i. Then U is also open in U_i, which is canonically identified with $\mathbb{A}^n$. We claim that $\mathcal{O}_{\mathbb{P}^n}(U) = \mathcal{O}_{\mathbb{A}^n}(U)$. Indeed, assume for example that $i = 0$, and let $f \in \mathcal{O}_{\mathbb{P}^n}(U)$. This means that there is an open cover $U = W_1 \cup \dots \cup W_l$ in $\mathbb{P}^n$ and rational functions $\frac{p_j(S_0,\dots,S_n)}{q_j(S_0,\dots,S_n)}$ defined on W_j such that $f = \frac{p_j}{q_j}$ on W_j, $j = 1, \dots, l$. Then we also have $f = \frac{p_j(1,T_1,\dots,T_n)}{q_j(1,T_1,\dots,T_n)}$ on W_j, where $T_1, \dots, T_n$ are the affine coordinates on U_0. Conversely, let $f \in \mathcal{O}_{\mathbb{A}^n}(U)$. This means that there is an open cover $U = V_1 \cup \dots \cup V_m$

of U and rational functions $\frac{g_j(T_1,\dots,T_n)}{h_j(T_1,\dots,T_n)}$ defined on V_j such that $f = \frac{g_j}{h_j}$ on V_j, $j = 1, \dots, m$. Now, on V_j we can also write $f = \frac{S_0^{\deg h_j} \hat{g}_j}{S_0^{\deg g_j} \hat{h}_j}$, where $\hat{g}_j$ and $\hat{h}_j$ are homogenizations.

Let $X \subseteq \mathbb{P}^n$ be a projective algebraic set, and $U_0, \dots, U_n$ be the affine open sets in $\mathbb{P}^n$. Put $V_i := X \cap U_i$. Then $X = V_0 \cup \dots \cup V_l$ is an open cover of X. Moreover, V_i an affine algebraic set in U_i, and U_i is canonically identified with $\mathbb{A}^n$. Let U be an open subset of X which is contained in some V_i. Then U is an open subset of V_i. The argument as in the previous paragraph can be modified to prove the following more general result: a function on U is regular in the sense of the projective algebraic set X if and only if it is regular in the sense of the affine algebraic set V_i, i.e. $\mathcal{O}_X(U) = \mathcal{O}_{V_i}(U)$.

3.10 Product of projective algebraic sets

Let $X \subset \mathbb{P}^n$ and $Y \subset \mathbb{P}^m$ be projective algebraic sets. We would like to consider $X \times Y$ as a projective algebraic set in a natural way. For example, we could have $X = \mathbb{P}^n$ and $Y = \mathbb{P}^m$. It is quite clear that there is no natural identification of $\mathbb{P}^n \times \mathbb{P}^m$ with $\mathbb{P}^{n+m}$ (play with that!). But there is a natural *Segre embedding* of $\mathbb{P}^n \times \mathbb{P}^m$ into $\mathbb{P}^{(n+1)(m+1)-1}$:

$$\varphi : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^{(n+1)(m+1)-1},$$
$$((T_0, \dots, T_n), (S_0, \dots, S_m)) \mapsto (T_0S_0, \dots, T_0S_m, \dots, T_nS_0, \dots, T_nS_m)$$

It is easy to see that φ is injective. We next show that $\operatorname{im} \varphi$ is closed in $\mathbb{P}^{(n+1)(m+1)-1}$. Let w_{ij}, $0 \le i \le n$, $0 \le j \le m$ be the homogeneous coordinates in $\mathbb{P}^{(n+1)(m+1)-1}$. We claim that $\operatorname{im} \varphi$ is the zero set of the following equations:

$$w_{ij}w_{kl} = w_{kj}w_{il} \qquad (0 \le i, k \le n,\ 0 \le j, l \le m). \tag{3.4}$$

That all points of $\operatorname{im} \varphi$ satisfy these equations is clear. Conversely, if the numbers w_{ij} satisfy these equations, and $w_{kl} \neq 0$, then

$$(\dots : w_{ij} : \dots) = \varphi(x, y)$$

where $x = (w_{0l} : \dots : w_{nl})$ and $y = (w_{k0} : \dots : w_{km})$.

So, we have proved that the image of $\mathbb{P}^n \times \mathbb{P}^m$ under the Segre embedding is a projective algebraic set, and this is what we will understand by the *product* of $\mathbb{P}^n$ and $\mathbb{P}^m$. More generally, let X be an algebraic set in $\mathbb{P}^n$ and Y be an algebraic set in $\mathbb{P}^m$. By the product of X and Y we understand $\varphi(X \times Y)$, which we show to be algebraic. Well, if X is given by the equations $F_\alpha(T_0, \ldots, T_n) = 0$ and Y is given by the equations $G_\beta(S_0, \ldots, S_m) = 0$, then $X \times Y$ is the zero set of the equations (3.5) together with $\mathbb{F}_\alpha(w_{0j}, \ldots, w_{nj})$ for $1 \le j \le m$ and $G_\beta(w_{i0}, \ldots, w_{im})$ for $1 \le i \le n$.

3.11 Example: Grassmann varieties and flag varieties

Let V be an n-dimensional vector space. As a set, the *Grassmann variety* $G_r(V)$ (or $G_r(n)$) is just the set of all r-dimensional (linear) subspaces in V. However, we need to explain how is $G_r(V)$ a projective algebraic set. Of course, we already know that for $r = 1$ when $G_r(V)$ is nothing but the projective space $\mathbb{P}(V) = \mathbb{P}^{n-1}$. In general we are going to realize $G_r(V)$ as an algebraic set in the projective space $\mathbb{P}(\Lambda^r(V))$.

Define the map

$$\psi : G_r(V) \to \mathbb{P}(\Lambda^r(V))$$

as follows. Let $l_1, \ldots, l_r$ be a basis of a subspace $L \subset V$. Then $\psi(L)$ is defined to be the span of the vector $l_1 \wedge \cdots \wedge l_r \in \Lambda^r(V)$. It is easy to check that ψ is a well defined embedding. We claim that the image of ψ is an algebraic set. In order to see that, let us fix a basis $\{v_1, \ldots, v_n\}$ of V. Then the basis of $\Lambda^r(V)$ is

$$\{v_{i_1} \wedge \cdots \wedge v_{i_r} \mid 1 \le i_1 < \cdots < i_r \le n\}.$$

Denote the $v_{i_1} \wedge \cdots \wedge v_{i_r}$-coefficient of $l_1 \wedge \cdots \wedge l_r$ by $\mu_{i_1 \ldots i_r}$. Then the homogeneous coordinates of $\psi(L)$ are $(\cdots : \mu_{i_1 \ldots i_r} : \ldots)$. These homogeneous coordinates are called the *Plükker coordinates* of L. We accept the following convention: given a collection of numbers $\{\mu_{i_1 \ldots i_r} \mid 1 \le i_1 < \cdots < i_r \le n\}$ we assume that $\mu_{i_1 \ldots i_r}$ are also defined for *any* $i_1, \ldots, i_r$ with $1 \le i_1, \ldots, i_r \le n$ in such a way that after two indices are interchanged, $\mu_{i_1 \ldots i_r}$ gets multiplied by -1; in particular, if two indices are the same, it is zero.

With these assumptions the Plükker coordinates can be described as follows. Write $l_i = \sum_{j=1}^n a_{ij} v_j$. Then $\mu_{i_1 \ldots i_r}$ is the determinant of the matrix formed by the columns of $A := (a_{ij})$ with indices $i_1, \ldots, i_r$.

Theorem 3.11.1 *Numbers $\mu_{i_1 \ldots i_r}$ are Plükker coordinates of some r-dimensional subspace $L \subset V$ if and only if they are not simultaneously zero and if for all $i_1, \ldots, i_{r+1}, j_1, \ldots, j_{r-1}$ the following relation (called*

Plücker relation*) holds:*

$$\sum_{k=1}^{r+1}(-1)^k \mu_{i_1\dots\widehat{i_k}\dots i_{r+1}}\mu_{i_k j_1\dots j_{r-1}} = 0.$$

Proof Expanding the determinant $\mu_{i_k j_1\dots j_{r-1}}$ along the first column, we obtain

$$\mu_{i_k j_1\dots j_{r-1}} = \sum_{s=1}^{r} a_{si_k} N_s,$$

where N_s does not depend on k. Thus, it suffices to prove that

$$\sum_{k=1}^{r+1}(-1)^k \mu_{i_1\dots\widehat{i_k}\dots i_{r+1}} a_{si_k} = 0 \tag{3.5}$$

for all s. Add the sth row to A to obtain an $(r+1)\times n$ matrix A_s. Then the left hand side of (3.5) is, up to a sign, the expansion of the determinant of the matrix formed by the columns of A_s with indices $i_1,\dots,i_{r+1}$ along the last row. But this determinant is zero.

Conversely, assume that $\mu_{i_1\dots i_r}$ are not simultaneously zero and the Plücker relations hold. It suffices to prove that there exists an $r\times n$ matrix A such that

$$\mu_{i_1\dots i_r} = M_{i_1\dots i_r} \qquad (1\le i_1,\dots,i_r\le n), \tag{3.6}$$

where $M_{i_1\dots i_r}$ is the minor formed by the columns of A with indices $i_1,\dots,i_r$. We may assume that $\mu_{1\dots r}=1$. We will look for A in the form

$$\begin{pmatrix} 1 & 0 & \dots & 0 & a_{1,r+1} & \dots & a_{1n} \\ 0 & 1 & \dots & 0 & a_{2,r+1} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & a_{r,r+1} & \dots & a_{rn} \end{pmatrix}.$$

Note that for $j>r$ we have $M_{1\dots\hat{i}\dots rj} = (-1)^{r-i}a_{ij}$. Thus , we must set $a_{ij} = (-1)^{r-i}\mu_{1\dots\hat{i}\dots rj}$, in which case the equality (3.6) holds at least for the sets $\{i_1,\dots,i_r\}$ which differ from $\{1,\dots,r\}$ in no more than one element.

Now it remains to prove that (3.6) holds if the set $\{i_1,\dots,i_r\}$ differs from $\{1,\dots,r\}$ in m elements for any m. We use induction on m. We may assume that $i_1\notin\{1,\dots,r\}$. Then, using the Plücker relations, we get

$$\mu_{i_1\dots i_r} = \mu_{1\dots r}\mu_{i_1\dots i_r} = \sum_{k=1}^{r}(-1)^{k+1}\mu_{i_1 1\dots\hat{k}\dots r}\mu_{k i_2\dots i_r}. \qquad (3.7)$$

On the other hand, it follows from the first part of the theorem that the same condition holds for the minors of A:

$$M_{i_1\dots i_r} = \sum_{k=1}^{r}(-1)^{k+1}M_{i_1 1\dots\hat{k}\dots r}M_{k i_2\dots i_r}. \qquad (3.8)$$

By the induction hypothesis, the right hand sides of (3.7) and (3.8) coincide. Therefore $M_{i_1\dots i_r} = \mu_{i_1\dots i_r}$. □

A *flag* in the n-dimensional vector space V is a chain

$$0 \subset V_1 \subset V_2 \subset \cdots \subset V_n = V$$

of subspaces with $\dim V_i = i$ for all $i = 1, \dots, n$. Let $\mathcal{F}(V)$ be the set of all flags in V. This set can be given a natural structure of a projective algebraic set called *flag variety.* Note that $V_i \in G_i(V)$, so we can consider $\mathcal{F}(V)$ as a subset of $G_1(V) \times \cdots \times G_n(V)$, and we claim that this is a closed subset.

Indeed, it suffices to prove that the condition for V_d to be contained in V_{d+1} is a closed condition for each d. In checking that we may forget about other spaces and work in $\mathbb{P}(\Lambda^d(V)) \times \mathbb{P}(\Lambda^{d+1}(V))$. Let us apply Affine Criterion. The open covering we are going to use is the direct products of the affine open sets in $\mathbb{P}(\Lambda^d(V))$ and $\mathbb{P}(\Lambda^{d+1}(V))$. The affine open sets in $\mathbb{P}(\Lambda^d(V))$ are given by conditions $\mu_{i_1\dots i_d} \neq 0$. As they are all the same we may work with the set U given by $\mu_{1\dots r} \neq 0$. Then $V_d \in U$ if and only if V_d is spanned by the vectors of the form $v_i + \sum_{j=d+1}^{n} a_{ij}v_j$, $i = 1, \dots, d$. In fact, $U \cap G_d(V) \cong \mathbb{A}^{d(n-d)}$ and the a_{ij} can be considered as the affine coordinates on $U \cap G_d(V)$. Now, let U' be the affine open set in $\mathbb{P}(\Lambda^{d+1}(V))$ containing V_{d+1} given by $\mu_{i_1\dots i_{d+1}} \neq 0$. As $V_d \subset V_{d+1}$, we must have that $i_1 = 1, \dots, i_d = d$, for otherwise the intersection with $U \times U'$ is empty. We may also assume without loss of generality that $i_{d+1} = d+1$. Now, V_{d+1} is spanned by the vectors of the form $v_i + \sum_{j=d+2}^{n} b_{ij}v_j$, $i = 1, \dots, d+1$. In fact, the b_{ij} can be considered as the affine coordinates on $U' \cap G_{d+1}(V)$. Now the condition that V_d is contained in V_{d+1} can be written by the polynomial equations $a_{ij} = b_{ij} + a_{i,d+1}b_{d+1,i}$ for all $1 \leq i \leq d$ and $d+2 \leq j \leq n$.

3.12 Example: Veronese variety

Consider all homogeneous polynomials of degree m in $S_0, S_1, \dots, S_n$. They form a vector space of dimension $\binom{n+m}{m}$. The corresponding projective space is $\mathbb{P}^{\nu_{n,m}}$ where $\nu_{n,m} := \binom{n+m}{m} - 1$. To each point of $\mathbb{P}^{\nu_{n,m}}$ there corresponds a hypersurface of degree m in $\mathbb{P}^n$ (since proportional polynomials define the same hypersurface).

Denote the homogeneous coordinates in $\mathbb{P}^{\nu_{n,m}}$ by $v_{i_0 \dots i_n}$ for all tuples $(i_0, \dots, i_n)$ of non-negative integers with $i_0 + \dots + i_n = m$. Consider the map $\alpha_m : \mathbb{P}^n \to \mathbb{P}^{\nu_{n,m}}$, defined by

$$v_{i_0 \dots i_n}(\alpha_m((a_0 : \dots : a_n))) = a_0^{i_0} \dots a_n^{i_n}. \tag{3.9}$$

The map is well-defined, as among the monomials in the right hand side of (3.9) there are a_i^m which all turn into 0 only if all $a_i = 0$. The map α_m is clearly injective. It is called *Veronese map*, and $\alpha_m(\mathbb{P}^n)$ is called *Veronese variety*.

Formulas (3.9) imply that all points of the Veronese variety satisfy equations

$$\begin{aligned} v_{i_0 \dots i_n} v_{j_0 \dots j_n} &= v_{k_0 \dots k_n} v_{l_0 \dots l_n} \\ \text{if} \quad i_0 + j_0 = k_0 + l_0, \dots, i_n + j_n &= k_n + l_n. \end{aligned} \tag{3.10}$$

Conversely, it follows from the relations (3.10) that at least one of the coordinates of the form $v_{0 \dots m \dots 0}$ is non-zero. Indeed, assume otherwise, and prove by induction on the amount k of non-zeros among $\{i_0, \dots, i_n\}$ that all $v_{i_0 \dots i_n} = 0$. The induction base $k = 1$ follows from our assumption. On the other hand, let $k \geq 2$ and assume that the statement is true for $k - 1$. Let i_r be the minimal non-zero element in $\{i_0, \dots, i_n\}$ and i_s be the minimal non-zero element of $\{i_0, \dots, i_n\} \setminus \{i_r\}$. Now, the relation

$$v^2_{i_0 \dots i_r \dots i_s \dots i_n} = v_{i_0 \dots 0 \dots i_s + i_r \dots i_n} v_{i_0 \dots i_r \dots i_s - i_r \dots i_n}$$

is among the relations (3.9). By the inductive assumption, the right hand side of it is zero, so $v_{i_0 \dots i_n}$ is also zero, completing the induction step.

Now, let, for example, $v_{m0 \dots 0} \neq 0$. Then our point with homogeneous coordinates $(v_{i_0 \dots i_n})$ is the image under the Veronese map of the point with coordinates

$$u_0 = v_{m0 \dots 0}, \; u_1 = v_{m-1,1,0 \dots 0}, \; \dots, \; u_n = v_{m-1,0 \dots 0,1}.$$

Indeed, it suffices to check that

$$\frac{(v_{m0\dots 0})^{i_0}(v_{m-1,1,0\dots 0})^{i_1}\dots(v_{m-1,0\dots 0,1})^{i_n}}{v_{m0\dots 0}^{m-1}} = v_{i_0\dots i_n}.$$

or, equivalently,

$$(v_{m0\dots 0})^{i_0-m+1}(v_{m-1,1,0\dots 0})^{i_1}\dots(v_{m-1,0\dots 0,1})^{i_n} = v_{i_0\dots i_n}. \tag{3.11}$$

We prove this by induction on the lexicographical order on the tuples $(i_0 \dots i_n)$. For the highest tuple $(m0\dots 0)$ the result is obvious. Every other $(i_0 \dots i_n)$ has some $i_r \neq 0$. Now,

$$v_{i_0\dots i_r\dots i_n}v_{m0\dots 0} = v_{i_0+1\dots i_r-1\dots i_n}v_{m-1\dots 1\dots 0}. \tag{3.12}$$

If $v_{m-1\dots 1\dots 0} = 0$, it follows that $v_{i_0\dots i_n} = 0$, in which case (3.11) is clear. Otherwise, substituting (3.12) into (3.11), we reduce (3.11) for $(i_0, \dots i_n)$ to (3.11) for $(i_0+1, \dots, i_r-1, \dots, i_n)$, which is true by induction.

Let $F = \sum a_{i_0\dots i_n}u_0^{i_0}\dots u_n^{i_n}$ be a form of degree m and H be a hypersurface in $\mathbb{P}^n$ defined by the equation $F = 0$. Then $\alpha_m(H)$ is the intersection of $\alpha_m(\mathbb{P}^n)$ with the hyperplane given by the equation

$$\sum a_{i_0\dots i_n}v_{i_0\dots i_n} = 0.$$

Let us now concentrate on the special case

$$\alpha_3 : \mathbb{P}^1 \to \mathbb{P}^3 : (a_0 : a_1) \mapsto (a_0^3 : a_0^2a_1 : a_0a_1^2 : a_1^3).$$

The corresponding Veronese variety C is called the *twisted cubic*. It is described by the equations

$$F_0 = F_1 = F_2 = 0, \tag{3.13}$$

where

$$F_0 = v_{30}v_{12} - v_{21}^2, \quad F_1 = v_{21}v_{12} - v_{30}v_{03}, \quad F_2 = v_{21}v_{03} - v_{12}^2.$$

The twisted cubic consists of all points of the form $(1 : c : c^2 : c^3)$ for $c \in k$ together with the point $(0 : 0 : 0 : 1)$. Let Q_i be the hypersurfaces described by $F_i = 0$. Then $C = Q_0 \cap Q_1 \cap Q_2$, but $C \neq Q_i \cap Q_j$ for any two hypersurfaces Q_i and Q_j. In fact the following beautiful geometric fact is true: the intersection $Q_i \cap Q_j$ equals $C \cup L_{ij}$ for some (projective) line L_{ij} (it is easy to see that no line is contained in C).

In order to prove this we consider a more general problem. For $\lambda = (\lambda_0 : \lambda_1 : \lambda_2) \in \mathbb{P}_2$ define the hypersurface Q_λ by F_λ, where

$$F_\lambda := \lambda_0F_0 + \lambda_1F_1 + \lambda_2F_2.$$

We claim that for $\lambda \neq \mu$, one has $Q_\lambda \cap Q_\mu = C \cup L_{\lambda,\mu}$ for some line $L_{\lambda,\mu}$.

Note that the equations (3.13) are equivalent to the requirement that the matrix

$$\begin{pmatrix} v_{30} & v_{21} & v_{12} \\ v_{21} & v_{12} & v_{03} \end{pmatrix}$$

has rank less than 2. Now note that F_λ is the determinant of the matrix

$$\begin{pmatrix} v_{30} & v_{21} & v_{12} \\ v_{21} & v_{12} & v_{03} \\ \lambda_2 & \lambda_1 & \lambda_0 \end{pmatrix}.$$

So the locus outside of C of $F_\lambda = F_\mu = 0$ is the rank ≤ 2 locus of the matrix

$$\begin{pmatrix} v_{30} & v_{21} & v_{12} \\ v_{21} & v_{12} & v_{03} \\ \lambda_2 & \lambda_1 & \lambda_0 \\ \mu_2 & \mu_1 & \mu_0 \end{pmatrix},$$

which as λ and μ are linearly independent is the same as the locus of

$$\begin{vmatrix} v_{30} & v_{21} & v_{12} \\ \lambda_2 & \lambda_1 & \lambda_0 \\ \mu_2 & \mu_1 & \mu_0 \end{vmatrix} = \begin{vmatrix} v_{21} & v_{12} & v_{03} \\ \lambda_2 & \lambda_1 & \lambda_0 \\ \mu_2 & \mu_1 & \mu_0 \end{vmatrix} = 0,$$

which is a line.

3.13 Problems

Problem 3.13.1 True or false? Let I, J be ideals in $k[T_1, \ldots, T_n]$. Then $Z(I) \cup Z(J) = Z(IJ)$.

Solution. True. By the Nullstellensatz, it suffices to prove that $\sqrt{I \cap J} = \sqrt{IJ}$. Well, $IJ \subset I \cap J$ implies $\sqrt{IJ} \subset \sqrt{I \cap J}$. Conversely, let $x \in \sqrt{I \cap J}$. Then $x^n \in I \cap J$, whence $x^{2n} \in IJ$.

Problem 3.13.2 True or false? Let I, J be ideals in $k[T_1, \ldots, T_n]$. Then $\sqrt{I \cap J} = \sqrt{IJ}$.

Solution. True. See the previous problem.

Problem 3.13.3 Let I and J be ideals of $A = \mathbb{C}[x, y]$ and $Z(I) \cap Z(J) = \varnothing$. Show that $A/(I \cap J) \cong A/I \times A/J$.

Solution. In view of the Chinese Remainder Theorem, we need only to show that $I + J = A$. Otherwise, let M be a maximal ideal containing $I + J$. By the Nullstellensatz, $M = M_a$ for some $a \in \mathbb{C}^2$. Then $a \in Z(I) \cap Z(J)$.

Problem 3.13.4 True or false? Any decreasing sequence of algebraic sets in $\mathbb{A}^n$ stabilizes.

Solution. True by the Nullstellensatz and Hilbert Basis Theorem.

Problem 3.13.5 True or false? Any increasing sequence of algebraic sets in $\mathbb{A}^n$ stabilizes.

Solution. False. Take "increasing sets of points".

Problem 3.13.6 If $X = \cup U_\alpha$ is an open covering of an algebraic set, then $X = U_{\alpha_1} \cup \cdots \cup U_{\alpha_l}$ for some $\alpha_1, \ldots, \alpha_l$.

Solution. Otherwise we would have an infinite strictly decreasing sequence of closed subsets, which contradicts Problem 3.13.4.

Problem 3.13.7 True or False?

(i) $\{(x, y) \in \mathbb{A}^2 \mid x^2 + y^2 = 1\}$ is homeomorphic to k (in Zariski topology).
(ii) The set $k \setminus \{(0)\}$ with induced Zariski topology is not homeomorphic to any variety.

Solution. (i) True. Our variety has the same cardinality as k and cofinite topology, see Lemma 2.1.1 (even characteristic 2 is O.K., because then $Z(x^2 + y^2 - 1) = Z(x + y - 1)$).

(ii) False. This set and k have the same cardinality and cofinite topology.

Problem 3.13.8 True or false? A system of polynomial equations

$$f_1(T_1, \ldots, T_n) = 0$$
$$\vdots$$
$$f_m(T_1, \ldots, T_n) = 0$$

over k has no solutions in $\mathbb{A}^n$ if and only if 1 can be expressed as a linear combination $1 = \sum_i p_i f_i$ with polynomial coefficients p_i.

Solution. True. The first condition is equivalent to $(f_1, \dots, f_m) = k[T]$, in view of the Nullstellensatz.

Problem 3.13.9 Let $\operatorname{char} k \neq 2$. Decompose

$$Z(x^2 + y^2 + z^2,\, x^2 - y^2 - z^2 + 1)$$

into irreducible components.

Solution. An easy calculation shows that $Z(x^2+y^2+z^2,\, x^2-y^2-z^2+1)$ equals

$$Z(x = i/\sqrt{2}, y^2 + z^2 = 1/2) \cup Z(x = -i/\sqrt{2}, y^2 + z^2 = 1/2),$$

union of two irreducible sets, since $y^2 + z^2 = 1/2$ is an irreducible polynomial.

Problem 3.13.10 True or false? The Zariski topology on $\mathbb{A}^{m+n}$ is the product topology of the Zariski topologies on $\mathbb{A}^m$ and $\mathbb{A}^n$.

Solution. False. Consider the case $m = n = 1$.

Problem 3.13.11 Let k have characteristic $p > 0$, and $\mathrm{Fr} : k \to k, a \mapsto a^p$ be the Frobenius homomorphism. True or false:

(i) Fr is a homeomorphism in the Zariski topology.
(ii) Fr is an isomorphism of algebraic sets.

Solution. (i) is true, as Fr is a bijection. (ii) is false as Fr^* is not an isomorphism.

Problem 3.13.12 Prove that the hyperbola $xy = 1$ and k are not isomorphic.

Solution. If $\psi : k[x, y]/(xy - 1) \to k[T]$ is an isomorphism, then $\psi(x)$ and $\psi(y)$ must be invertible, which leads to a contradiction.

Problem 3.13.13 For the regular map $f : \mathbb{A}^2 \to \mathbb{A}^2,\ (x, y) \mapsto (x, xy)$ describe $\operatorname{im} f$. Is the image dense in $\mathbb{A}^2$? Open? Closed?

Solution. The image is $\mathbb{A}^2 \setminus \{(0, b) \mid b \neq 0\}$. It is dense because it contains a non-empty open set $x \neq 0$. So it is not closed. It is also not open, as the origin belongs to the closure of the complement C (in fact, $I(C) = (x)$).

Problem 3.13.14 Let X consist of two points. Prove that $k[X] \cong k \oplus k$.

Solution. Use the Nullstellensatz and the Chinese Remainder Theorem (cf. Problem 3.13.3).

Problem 3.13.15 Describe all automorphisms of the algebraic set k.

Solution. All automorphisms are linear of the form $x \mapsto ax + b$ with $a \neq 0$. This follows by considering automorphisms of $k[T]$. By the way, the automorphism group is isomorphic to the semidirect product of $k^\times$ and k.

Problem 3.13.16 The graph of a morphism $\varphi : X \to Y$ of affine algebraic sets is a closed set in $X \times Y$ isomorphic to X.

Solution. Let $s_1, \ldots, s_n$ be coordinate functions on Y. Then the graph is the zero locus of the functions $\varphi^*(s_i) \otimes 1 - 1 \otimes s_i \in k[X] \otimes k[Y] = k[X \times Y]$. Next, check that the maps $x \mapsto (x, f(x))$ and $(x, f(x)) \mapsto x$ are morphisms between X and the graph which are inverse to each other.

Problem 3.13.17 Let $\varphi : X \to Y$ be a morphism of affine algebraic sets. Show that inverse image of a principal open set in Y is a principal open set in X.

Solution. $\varphi^{-1}(Y_f) = X_{\varphi^*(f)}$.

Problem 3.13.18 Let X, X' be topological spaces.

(i) A subspace $Y \subseteq X$ is irreducible if and only if $\bar{Y}$ is irreducible.
(ii) If $\varphi : X \to X'$ is a continuous map and X is irreducible, then $\varphi(X)$ is irreducible.

Solution. See *Humphreys*.

Problem 3.13.19 Let $\varphi : X \to Y$ be a regular map. Then $\varphi(X)$ is dense in Y if and only if φ^* is injective. Give an example when $\varphi(X)$ is dense in Y but $\varphi(X) \neq Y$.

Solution. $I(\operatorname{im} \varphi) = \{g \in k[Y] \mid g(\varphi(x)) = 0 \text{ for any } x \in X\} = \{g \in k[Y] \mid \varphi^*(g) = 0\} = \ker \varphi^*$. Now the result follows from $Z(I(\operatorname{im} \varphi)) = \overline{\operatorname{im} \varphi}$. For the example see Problem 3.13.13.

Problem 3.13.20 Let $X, Y \subset \mathbb{A}^r$ be closed subsets, and $\Delta \subset \mathbb{A}^{2r}$ be the *diagonal*, i.e. a subset given by equations $T_1 = S_1, \ldots, T_r = S_r$. If $z \in X \cap Y$ define $\varphi(z) = (z, z)$. Prove that φ defines an isomorphism from $X \cap Y$ onto $(X \times Y) \cap \Delta$.

Solution. $(x, y) \mapsto x$ defines the inverse morphism.

Problem 3.13.21 True or false? Let X be an affine algebraic set with irreducible components $X_1, \dots, X_l$. Then a function f on X is in $k[X]$ if and only if $f|X_i \in k[X_i]$ for all i.

Solution. This is actually false! Let $X = X_1 \cup X_2$, where X_1 is the line in $\mathbb{A}^2$ given by $x = 0$, and $X_2 \subset \mathbb{A}^2$ is the parabola $x = y^2$. Consider the function f which is 0 on X_1, and which maps the point (y^2, y) of X_2 to y. Then clearly $f|X_1$ and $f|X_2$ are regular. Now assume that there is a polynomial $F(x, y)$ with $F|X = f$. Since $F|X_1$=0, it follows that $F(x, y) = xg_1(x, y) + x^2 g_2(x, y) + \dots$. Now, $F|X_2 = f|X_2$ gives $y = F(y^2, y) = y^2 g_1(y^2, y) + y^4 g_2(y^2, y) + \dots$, which is impossible by degrees.

4
Varieties

4.1 Affine varieties

In this section we will define affine varieties which can be thought of as a 'coordinate-free version' of affine algebraic sets and functions on them.

Definition 4.1.1 A *sheaf of functions* on a topological space X is a function $\mathcal{F}$ which assigns to every non-empty open subset $U \subset X$ a k-algebra $\mathcal{F}(U)$ of k-valued functions on U (with respect to the usual point-wise operations) such that the following two conditions hold:

(i) If $U \subset V$ are two non-empty open sets and $f \in \mathcal{F}(V)$, then the restriction $f|U \in \mathcal{F}(U)$.

(ii) Given a family of open sets U_i, $i \in I$, covering U and functions $f_i \in \mathcal{F}(U_i)$ for each $i \in I$, such that f_i and f_j agree on $U_i \cap U_j$, there must exist a function $f \in \mathcal{F}(U)$ whose restriction to U_i equals f_i.

Definition 4.1.2 A topological space X together with a sheaf of functions $\mathcal{O}_X$ is called a *geometric space*. We refer to $\mathcal{O}_X$ as the *structure sheaf* of the geometric space.

Definition 4.1.3 Let $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ be geometric spaces. A *morphism*

$$f : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$$

is a continuous map $f : X \to Y$ such that for every open subset U of Y and every $\varphi \in \mathcal{O}_Y(U)$ the function

$$f^*(\varphi) := \varphi \circ f$$

belongs to $\mathcal{O}_X(f^{-1}(U))$.

Remark 4.1.4 We will often use a shorthand $f : X \to Y$ for the morphism $f : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$.

Example 4.1.5 Let X be an affine or a projective algebraic set. To each non-empty open subset $U \subset X$ we assign the ring $\mathcal{O}_X(U)$ which consists of all regular functions on U. Then $(X, \mathcal{O}_X)$ is a geometric space. Moreover the notion of a morphism agrees with the one we had before (think about it!).

Let $(X, \mathcal{O}_X)$ be a geometric space and Z be a subset of X with induced topology. We can make Z into a geometric space by defining $\mathcal{O}_Z(V)$ for an open $V \subset Z$ as follows: $f : V \to k$ is in $\mathcal{O}_Z(V)$ if and only if there exists an open covering $V = \cup_i V_i$ in Z such that for each i we have $f|V_i = g_i|V_i$ for some $g_i \in \mathcal{O}_X(U_i)$ where U_i is an open subset of X containing V_i. It is not difficult to see that $\mathcal{O}_Z$ is a sheaf of functions on Z (see it!). We will refer to it as the *induced* structure sheaf and denote it by $\mathcal{O}_X|Z$. Note that if Z is open in X then a subset $V \subset Z$ is open in Z if and only if it is open in X, and $\mathcal{O}_X(V) = \mathcal{O}_Z(V)$.

Let X be a topological space and $X = \cup_i U_i$ be its open cover. Given sheaves of functions $\mathcal{O}_{U_i}$ on U_i for each i, which agree on each $U_i \cap U_j$, we can define a natural sheaf of functions $\mathcal{O}_X$ on X by 'gluing' the $\mathcal{O}_{U_i}$. Let U be an open subset in X. Then $\mathcal{O}_X(U)$ consists of all functions on U, whose restriction to each $U \cap U_i$ belongs to $\mathcal{O}_{U_i}(U \cap U_i)$.

If $x \in X$ we denote by ev_x the map from functions on X to k obtained by evaluation at x:

$$\mathrm{ev}_x(f) = f(x).$$

Definition 4.1.6 A geometric space $(X, \mathcal{O}_X)$ is called an *affine (algebraic) variety* if the following three conditions hold:

(i) $k[X] := \mathcal{O}_X(X)$ is a finitely generated k-algebra, and the map

$$X \to \mathrm{Hom}_{k-\mathrm{alg}}(k[X], k), \quad x \mapsto \mathrm{ev}_x$$

is a bijection.

(ii) For each $0 \neq f \in k[X]$ the set

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

is open, and every non-empty open set in X is a union of some X_f.

(iii) $\mathcal{O}_X(X_f) = k[X]_f$.

Example 4.1.7 It follows from the results of chapter 3 (in particular, Theorem 3.7.3) that affine algebraic sets with sheaves of regular functions are affine varieties. We claim that, conversely, every affine variety is isomorphic (as a geometric space) to an affine algebraic set with the sheaf of regular functions. Indeed, let $(X, \mathcal{O}_X)$ be an affine variety. Since $k[X]$ is a finitely generated algebra of functions, we can write

$$k[X] = k[T_1, \dots, T_n]/I$$

for some radical ideal I. By the property (i) of affine varieties and the Nulstellensatz, we can identify X with $Z(I)$ as a set, and $k[X]$ with the regular functions on $Z(I)$. The Zariski topology on $Z(I)$ has the principal open sets as its base, so it now follows from (ii) that the identification of X and $Z(I)$ is a homeomorphism. Finally, by (iii), $\mathcal{O}_X(X_f)$ and the regular functions on the principal open set X_f are also identified. This is enough to identify $\mathcal{O}_X(U)$ with regular functions on U for any open set U, as regularity is a local condition.

Remark 4.1.8 The argument of Example 4.1.7 shows that the affine variety can be recovered completely from its algebra $A := k[X]$ of regular functions, and conversely. We make it precise as follows. Define a functor $\mathcal{F}$ from the category of affine varieties to the category of affine algebras via $\mathcal{F}(X) = k[X] := \mathcal{O}_X(X)$, $\mathcal{F}(f) = f^*$. We now describe a quasi-inverse functor $\mathcal{G}$ from the affine algebras to the affine varieties (this means that $\mathcal{F} \circ \mathcal{G} \cong \mathrm{Id}$ and $\mathcal{G} \circ \mathcal{F} \cong \mathrm{Id}$, i.e. $\mathcal{F}$ and $\mathcal{G}$ establish an equivalence of categories, see Problem 4.6.1. In particular, if $(X, \mathcal{O}_X), (Y, \mathcal{O}_Y)$ are affine varieties and $f : X \to Y$ is a map, then f is a morphism if and only if f^* maps $k[Y]$ to $k[X]$, and $f : X \to Y$ is an isomorphism if and only if f^* is an isomorphism from $k[Y]$ to $k[X]$.

So let A be an affine k-algebra. We define $\mathcal{G}(A)$ to be the affine variety $\operatorname{Specm} A = (X, \mathcal{O}_X)$, where

$$X := \mathrm{Hom}_{k\text{-alg}}(A, k)$$

(which in view of Hilbert's Nulstellensatz, can be identified with the set of the maximal ideals of A, whence the name). Note that the elements of a can be considered as k-valued functions on X via

$$f(x) := x(f) \qquad (f \in A, x \in X = \mathrm{Hom}_{k\text{-alg}}(A, k)).$$

Now consider the topology on X whose basis consists of all $X_f := \{x \in X \mid f(x) \neq 0\}$ for $f \in A$. In order to define a structure sheaf on the topological space X, set

$$\mathcal{O}_X(X_f) := A_f \qquad (f \in A \setminus \{0\})$$

(again elements of A_f can be considered as functions on X_f in a natural way). Now for any $U = \cup_f X_f$ a function on U is in $\mathcal{O}_X(U)$ if and only if its restriction to each X_f is in $\mathcal{O}_X(X_f)$.

Example 4.1.9 In view of Example 4.1.7, a closed subset of an affine variety is an affine variety (as usual, with the induced sheaf), cf. Problem 4.6.6.

Example 4.1.10 If $(X, \mathcal{O}_X)$ is an affine variety, then it is easy to check that the principal open set X_f is also an affine variety (think why this does not contradict what was claimed in Example 4.1.7.) On the other hand, not every open subset of X is an affine variety, see Problem 4.6.4.

4.2 Prevarieties

Definition 4.2.1 An *(algebraic) prevariety* is a geometric space $(X, \mathcal{O}_X)$ such that X has an open covering $X = U_1 \cup \dots \cup U_l$, and each geometric space $(U_i, \mathcal{O}_{U_i})$ with the induced structure sheaf $\mathcal{O}_{U_i}$ is an affine variety.

Example 4.2.2 In view of §3.9, each projective algebraic set with the sheaf of regular functions is a prevariety. We will refer to varieties isomorphic to projective algebraic sets with sheaves of regular functions as *projective varieties*.

Lemma 4.2.3 *Let $(X, \mathcal{O}_X)$ be a prevariety with affine open covering $X = U_1 \cup \dots \cup U_l$.*

(i) *X is a noetherian topological space.*
(ii) *Any open subset U of X is again a prevariety.*
(iii) *Any closed subset Z of X is again a prevariety.*

Proof (i) follows from the fact that each U_i is noetherian.

(ii) As $U = \cup_i(U \cap U_i)$, it suffices to prove that each $U \cap U_i$ has an affine open covering. But $U \cap U_i$ is an open subset of an affine U_i, so it is a union of the principal open sets in U_i, which are affine by Example 4.1.10.

(iii) $Z = \cup_i (Z \cap U_i)$, and closed subsets $Z \cap U_i$ of affine varieties are affine. $\square$

A subset of a topological space is called *locally closed* if it is an intersection of an open set and a closed set. It follows from above that a locally closed subset of a prevariety is again a prevariety. We will refer to the locally closed subsets as *subprevarieties*.

Theorem 4.2.4 (Affine Criterion) *Let X, Y be prevarieties, and $\varphi : X \to Y$ be a map. Assume that there is an affine open covering $Y = \cup_{i \in I} V_i$ and an open covering $X = \cup_{i \in I} U_i$ such that*

(i) *$\varphi(U_i) \subset V_i$ for each $i \in I$;*
(ii) *$f \circ \varphi \in \mathcal{O}_X(U_i)$ whenever $f \in \mathcal{O}_Y(V_i)$.*

Then φ is a morphism.

Proof An *affine* open covering of X induces that of each U_i. So, by extending the index set if necessary we reduce to the case where U_i are also affine. Now by assumption, $\varphi_i := \varphi|U_i : U_i \to V_i$ is a morphism of affine varieties. In particular, φ_i is continuous, whence φ is continuous.

Let $V \subset Y$ be an open subset, $f \in \mathcal{O}_Y(V)$, and $U := \varphi^{-1}(V)$. By (ii), $f \circ \varphi \in \mathcal{O}_X(\varphi^{-1}(V \cap V_i))$. But $\varphi^{-1}(V \cap V_i) \supseteq U \cap U_i$, so $f \circ \varphi \in \mathcal{O}_X(U \cap U_i)$ for all i. Now, since U is the union of the $U \cap U_i$ and since $\mathcal{O}_X$ is a sheaf, $f \circ \varphi \in \mathcal{O}_X(U)$. $\square$

Let X be an irreducible prevariety. Consider pairs (U, f) where U is an open subset of X and $f \in \mathcal{O}_X(U)$. We call two such pairs (U, f) and (U', f') equivalent if there is a non-empty open subset $V \subset U \cap U'$ such that $f|V = f'|V$ (in which case we will also have $f|(U \cap U') = f'|(U \cap U')$). It is easy to check using the irreducibility of X that this defines an equivalence relation. Moreover, the set of equivalence classes is a field with respect to the obvious operations. (For example, $(U, f)^{-1} = (U \cap U_f, 1/f)$). This field is called the *field of rational functions* on X and denoted $k(X)$. It is easy to see that if X is affine then this definition agrees with the one we had before. Moreover, if $U \subset X$ is a non-empty open subset, then $k(X) = k(U)$.

Let $\mathcal{F}$ be a sheaf of functions on a topological space X and $x \in X$. The open sets in X containing x form inverse system with respect to inclusion. The *stalk* $\mathcal{F}_x$ of $\mathcal{F}$ at x is defined to be the corresponding limit of algebras

$$\mathcal{F}_x = \lim_{U} \mathcal{F}(U).$$

The elements of the stalk $\mathcal{F}_x$ are called *germs* of functions at x. One can think of germs as equivalence classes of pairs (U, f), where U is an open set containing x, $f \in \mathcal{F}(U)$, and $(U, f) \sim (V, g)$ if there is an open set $W \subset U \cap V$ containing x such that $f|W = g|W$. If $(X, \mathcal{O}_X)$ is a prevariety, we write simply $\mathcal{O}_x$ for $(\mathcal{O}_X)_x$ and call it the *local ring* of x. It is easy to see that the ring $\mathcal{O}_x$ is local in the sense of commutative algebra. Its unique maximal ideal is denoted $\mathfrak{m}_x$—it consists of the germs of functions equal to zero at x.

If X is an irreducible affine variety, this definition agrees with the one given in §3.7. Note also that $\mathcal{O}_x$ is a 'local notion', which means that if $x \in U$ for an open subset $U \subset X$, and $\mathcal{O}_U$ is the induced sheaf on U, then $\mathcal{O}_x$ defined using U is the same as the one defined using X.

4.3 Products

Theorem 4.3.1 *Finite products exist in the category of prevarieties.*

Proof It suffices to deal with two prevarieties $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$. We need to prove that there exists a prevariety $(Z, \mathcal{O}_Z)$ together with morphisms $\pi_1 : Z \to X$ and $\pi_2 : Z \to Y$ such that the following universal property holds: if $(W, \mathcal{O}_W)$ is another prevariety with morphisms $\varphi_1 : W \to X$ and $\varphi_2 : W \to Y$, then there exists a unique morphism $\psi : W \to Z$ such that $\pi_i \psi = \varphi_i$ for $i = 1, 2$.

For any set S denote by $\mathrm{Map}(S, k)$ the algebra of all functions from S to k. Observe that for any open $U \subset X$ and $V \subset Y$ the natural map of algebras

$$\mathcal{O}_X(U) \otimes \mathcal{O}_Y(V) \to \mathrm{Map}(U \times V, k).$$

is injective. So we will identify elements of $\mathcal{O}_X(U) \otimes \mathcal{O}_Y(V)$ as functions on $U \times V$.

Now define a topology on the set $X \times Y$ by saying that the open sets will be the unions of the sets of the form

$$(U \times V)_h := \{x \in U \times V \mid h(x) \neq 0\},$$

where $U \subset X$, $V \subset Y$ are arbitrary open subsets and $h \in \mathcal{O}_X(U) \otimes \mathcal{O}_Y(V)$. We will refer to such $(U \times V)_h$ as principal open sets. Checking that this is a topology boils down to

$$(U \times V)_h \cap (U' \times V')_{h'} = ((U \cap U') \times (V \cap V'))_{hh'}.$$

Next we define a structure sheaf on $X \times Y$. Let W be an open set in $X \times Y$ and $f \in \mathrm{Map}(W, k)$. Then we say that f is regular if and only if there is an open cover of W by the principal open sets $(U \times V)_h$ so that on each of them we have

$$f|(U \times V)_h = \frac{a}{h^m}$$

for some $a \in \mathcal{O}_X(U) \otimes \mathcal{O}_Y(V)$ and some non-negative integer m.

This defines a sheaf $\mathcal{O}_{X\times Y}$. Indeed, let $W' \subset W$ be an open subset. We have $W = \cup(U \times V)_h$ and $W' = \cup(U' \times V')_{h'}$. So

$$W' = \cup((U \times V)_h \cap (U' \times V')_{h'}) = \cup((U \cap U') \times (V \cap V'))_{hh'}.$$

Moreover,

$$\frac{a}{h^m}|((U \cap U') \times (V \cap V'))_{hh'} = \frac{(a{\downarrow})h'^m}{(hh')^m},$$

where $a{\downarrow}$ denotes the restriction of a from $U \times V$ to $(U \cap U') \times (V \cap V')$, which belongs to $\mathcal{O}_X(U \cap U') \otimes \mathcal{O}_Y(V \cap V')$. So $f|W'$ is regular. The second axiom of sheaf is obvious.

Now we want to show that $(X \times Y, \mathcal{O}_{X\times Y})$ is a prevariety.

First, it is easy to see that for the case where X, Y are affine, our definition agrees with the one from §3.6. So if $X = \cup_i U_i$, $Y = \cup_j V_j$ are open affine covers, then $X \times Y = \cup_{i,j} U_i \times V_j$ is an open affine cover.

Let $\pi_1 : X \times Y \to X$ and $\pi_2 : X \times Y \to Y$ be the natural projections, and let us check the universal property. First of all, we need to check that the projections are morphisms. They are continuous: for example, for an open $U \subset X$, we have $\pi^{-1}(U) = U \times V$, which is open. Moreover, let $f \in \mathcal{O}_X(U)$. Then $(\pi_1^*(f))(x, y) = f(x)$. So $\pi_1^*(f) = f \otimes 1 \in \mathcal{O}_X(U) \otimes \mathcal{O}_Y(Y)$ is regular.

Finally, let $\varphi_1 : W \to X$ and $\varphi_2 : W \to Y$ be morphisms. It is clear that if ψ required in the universal property exists, then it must send $w \in W$ to $(\varphi_1(w), \varphi_2(w))$. To show that ψ is a morphism, we use the affine criterion. We know that the products $U \times V$ of the affine open subsets cover $X \times Y$. Open subsets of the form $W' = \varphi_1^{-1}(U) \cap \varphi_2^{-1}(V)$ cover W, and ψ^* maps a function $\sum a_i \otimes a_i'$ from $\mathcal{O}_{X\times Y}(U \times W)$ to the function $\sum \varphi_1^*(a_i)\varphi_2^*(a_i') \in \mathcal{O}_W(W')$. By the affine criterion, ψ is a morphism. $\square$

4.4 Varieties

Definition 4.4.1 A prevariety X is called an *(algebraic) variety* if the diagonal $\Delta(X) = \{(x, x) \mid x \in X\}$ is closed in $X \times X$.

An equivalent condition is as follows: for any prevariety Y and any two morphisms $\varphi, \psi : Y \to X$ the set $\{y \in Y \mid \varphi(y) = \psi(y)\}$ is closed in Y. Indeed, applying this condition to $\pi_1, \pi_2 : X \times X \to X$ we conclude that Δ is closed; conversely, the preimage of Δ under $\varphi \times \psi : Y \to X \times X$ is $\{y \in Y \mid \varphi(y) = \psi(y)\}$.

It follows from the previous paragraph that a subprevariety of a variety is variety. We will refer to it a *subvariety* from now on.

In the category of topological spaces with usual product topology on $X \times X$ the Definition 4.4.1 is equivalent to the Hausdorff axiom. So we can think of varieties as prevarieties with some sort of an unusual Hausdorff axiom.

Example 4.4.2 An example of a prevariety which is not a variety is given by the affine line with a doubled point, see Problem 4.6.7.

Lemma 4.4.3 *Let Y be a variety and X be a prevariety.*

(i) *If $\varphi : X \to Y$ is a morphism, then the graph*

$$\Gamma_\varphi := \{(x, \varphi(x)) \mid x \in X\}$$

is closed in $X \times Y$.

(ii) *If $\varphi, \psi : X \to Y$ are morphisms which agree on a dense subset of X then $\varphi = \psi$.*

Proof (i) Γ_φ is the inverse image of $\Delta(Y)$ with respect to the morphism $X \times Y \to Y \times Y,\ (x, y) \to (\varphi(x), y)$.

(ii) The set of all points where φ and ψ agree is closed. $\square$

Lemma 4.4.4 *Affine varieties are varieties.*

Proof Note that

$$\begin{aligned}
\Delta(X) &= \{(x, y) \in X \times X \mid \mathrm{ev}_x = \mathrm{ev}_y\} \\
&= \{(x, y) \in X \times X \mid f(x) = f(y) \text{ for all } f \in k[X]\} \\
&= Z(f \otimes 1 - 1 \otimes f \mid f \in k[X]\}.
\end{aligned}$$

$\square$

Lemma 4.4.5 *The product of two varieties is a variety.*

Proof Under the isomorphism $(X \times Y) \times (X \times Y) \tilde{\to} (X \times X) \times (Y \times Y)$, $\Delta(X \times Y)$ maps to $\Delta(X) \times \Delta(Y)$, which is closed. $\square$

Lemma 4.4.6 *Let X be a prevariety. If every pair of points $x, y \in X$ lie in an open affine subset, then X is a variety.*

Proof Let Y be a prevariety and $\varphi, \psi : Y \to X$ be morphisms. Set $Z := \{y \in Y \mid \varphi(y) = \psi(y)\}$. In oprder to show that Z is closed, let $z \in \bar{Z}$, and $x_1 = \varphi(z), x_2 = \psi(z)$. By assumption, x_1 and x_2 lie in an open affine subset V of X. Then $U := \varphi^{-1}(V) \cap \psi^{-1}(V)$ is an open neighborhood of z, which must have a non-trivial intersection with Z. But $Z \cap U = \{y \in U \mid \varphi'(y) = \psi'(y)\}$ where $\varphi', \psi' : U \to V$ are restrictions of φ, ψ to U. As V is a variety, $Z \cap U$ is closed in U. So $U \setminus (Z \cap U)$ is open subset whose intersection with Z is empty. Hence $z \in Z$. $\square$

It follows easily from Lemma 4.4.6 that projective varieties are varieties, see Problem 4.6.16.

4.5 Dimension

Recall that we have assigned to every irreducible variety its field of rational functions $k(X)$. As $k(X)$ is a finitely generated field extension of k, it has a finite transcendence degree $\operatorname{tr.deg}_k k(X)$ over k. This degree is called the *dimension* of X and denoted $\dim X$. In general dimension of X is defined as the maximum of the dimensions of its irreducible components.

Example 4.5.1

(i) $\dim \mathbb{A}^n = \dim \mathbb{P}^n = n$.

(ii) Dimension of a finite set is 0. Conversely, if $\dim X = 0$, then X is finite. Indeed, let X be an irreducible affine variety $X \subset \mathbb{A}^n$ of dimension 0. Let $t_1, \dots, t_n$ be coordinates on $\mathbb{A}^n$ considered as functions on X. Then t_i are algebraic over k, so can take only finitely many values. So X is finite.

Example 4.5.2 Grassmann variety $G_r(n)$ is covered by the open subsets $\mu_{i_1 \dots i_r} \neq 0$, isomorphic to $\mathbb{A}^{r(n-r)}$, so $\dim G_r(n) = r(n-r)$.

Proposition 4.5.3 *Let X and Y be irreducible varieties of dimensions m and n, respectively. Then* $\dim X \times Y = m + n$.

Proof We may assume that X and Y are affine. Let $s_1, \ldots, s_p$ and $t_1, \ldots, t_q$ be generators of the algebras $k[X]$ and $k[Y]$, respectively. Then $s_1, \ldots, s_p$ and $t_1, \ldots, t_q$ generate the fields $k(X)$ and $k(Y)$ over k, respectively. So we can choose transcendence bases out of them. After renumbering, if necessary, transcendence bases are $s_1, \ldots, s_m$ and $t_1, \ldots, t_n$.

Recall that $k[X \times Y] = k[X] \otimes k[Y]$. Let us write s_i for $s_i \otimes 1$ and t_j for $1 \otimes t_j$. As $s_1, \ldots, s_p, t_1, \ldots, t_q$ generate $k[X \times Y]$, they also generate the field $k(X \times Y)$ over k. Moreover, these generators depend algebraically on $s_1, \ldots, s_m, t_1, \ldots, t_n$. So it suffices to prove that $s_1, \ldots, s_m, t_1, \ldots, t_n$ are algebraically independent.

Assume there is an algebraic dependence $f(s_1, \ldots, s_m, t_1, \ldots, t_n) = 0$. Then for each fixed $x \in X$ the function $f(s_1(x), \ldots, s_m(x), t_1, \ldots, t_n)$ is zero on Y. As $t_1, \ldots, t_n$ are algebraically independent, all coefficients $g(s_1(x), \ldots, s_m(x))$ of the polynomial $f(s_1(x), \ldots, s_m(x), T_1, \ldots, T_n) \in k[T_1, \ldots, T_n]$ are zero. As x was arbitrary and $s_1, \ldots, s_m$ are algebraically independent, it follows that the polynomial $g(S_1, \ldots, S_m) \in k[S_1, \ldots, S_m]$ is zero. Hence $f(S_1, \ldots, S_m, T_1, \ldots, T_n) = 0$. □

Proposition 4.5.4 *Let X be an irreducible variety and Y be a proper closed subvariety. Then* $\dim Y < \dim X$.

Proof We may assume that Y is irreducible and that X is affine, say of dimension d. Let $A = k[X]$, $\bar{A} = k[Y]$. Then $\bar{A} = A/P$ for some non-zero prime ideal P of A. The transcendence bases of $k(X)$ and $k(Y)$ can be found in A and $\bar{A}$. Assume that $\dim Y \geq d$. Then we can choose d algebraically independent elements $\bar{a}_1, \ldots, \bar{a}_d \in \bar{A}$. These elements are cosets of some $a_1, \ldots, a_d \in A$ which are of course also algebraically independent. Let $b \in P$ be a non-zero element. As $\dim X = d$, there must exist a non-trivial algebraic dependence $f(b, a_1, \ldots, a_d) = 0$, where $f(T_0, T_1, \ldots, T_d) \in k[T_0, T_1, \ldots, T_d]$. Since $b \neq 0$ we may assume that T_0 does not appear in all monomials of the polynomial f, i.e. the polynomial $g(T_1, \ldots, T_n) = f(0, T_1, \ldots, T_n)$ is non-zero. But then $g(\bar{a}_1, \ldots, \bar{a}_d) = 0$, giving a contradiction. □

Corollary 4.5.5 *Let X be an irreducible affine variety and Y is an irreducible closed subvariety of codimension* 1. *Then Y is a component of the variety $Z(f)$ for some $f \in k[X]$.*

Proof By assumption $Y \neq X$, so there exists a non-zero function $f \in k[X]$ with $f|Y = 0$. Then $Y \subseteq Z(f) \subsetneq X$. Let Z be an irreducible component of $Z(f)$ containing Y. By Proposition 4.5.4, $\dim Z < \dim X$. So $\dim Z = \dim Y$, and by Proposition 4.5.4 again, $Y = Z$. □

Lemma 4.5.6 If X is an irreducible affine variety for which $k[X]$ is a u.f.d., then every closed subvariety of codimension 1 has form $Z(f)$ for some $f \in k[X]$.

Proof Let Y be the subvariety, and $Y_1, \dots, Y_l$ be the components of Y. Then $I(Y) = \cap I(Y_i)$. So, if we can prove that $I(Y_i) = (f_i)$, then $I(Y) = (f_1 \dots f_l)$ (as the f_i must be powers of different irreducible elements). Thus we may suppose that Y is irreducible. Let $P = I(Y)$, a non-zero prime ideal in $k[X]$. It therefore contains an irreducible element f. So (f) is a prime ideal contained in P. If $(f) \subsetneq P$, then $Y = Z(P) \subsetneq Z\big((f)\big) \subsetneq X$, which contradicts the assumption that codimension of Y is 1, thanks to Proposition 4.5.4. □

Remark 4.5.7 The statement of Lemma 4.5.6 fails if $k[X]$ is not a u.f.d. For example, let $X = Z(T_1T_4 - T_2T_3) \subset \mathbb{A}^4$. It contains the planes L and L' given by the equations $T_2 = T_4 = 0$ and $T_1 = T_3 = 0$, respectively. Clearly, $L \cap L' = \{(0,0,0,0)\}$. We claim that L is not $Z(f)$ for any $f \in k[X]$. Otherwise, $Z(f|L') = \{(0,0,0,0)\}$, which is impossible, because it has codimension 2 in Z'.

If X is an affine variety and $f \in k[X]$ is a non-invertible element, then the zero set $Z(f)$ is called a *hypersurface* in X. If $k[X]$ is a u.f.d., the irreducible components of this hypersurface are precisely hypersurfaces defined by the irreducible components of f.

Proposition 4.5.8 *All irreducible components of a hypersurface in $\mathbb{A}^n$ have codimension* 1.

Proof It suffices to consider the zero set X of an irreducible polynomial $p(T_1, \dots, T_n)$. We may assume that (say) T_n appears in p, as p is non-scalar. Let $t_i := T_i|X$. So $k(X) = k(t_1, \dots, t_n)$. In view of Proposition 4.5.4 it suffices to prove that $t_1, \dots, t_{n-1}$ are algebraically independent.

Assume that there is a non-trivial polynomial relation $g(t_1, \dots, t_{n-1}) =$

0, so the polynomial $g(T_1, \dots, T_{n-1})$ is zero on X. It follows that g is divisible by p, which is impossible since T_n appears in p. $\square$

The proof of the following more general fact requires more powerful commutative algebra:

Theorem 4.5.9 *Let X be an irreducible affine variety, $0 \neq f \in k[X]$ be a non-invertible elemet, and Y be an irreducible component of $Z(f)$. Then Y has codimension 1 in X.*

Proof Let $Y_1, \dots, Y_l$ be the components of $Z(f)$ different from Y, and $P := I(Y), P_i := I(Y_i)$ be the corresponding (prime) ideals in $k[X]$. As the intersection of prime ideals is radical, it follows from the Nullstellensatz that

$$\sqrt{(f)} = P \cap P_1 \cap \dots \cap P_l.$$

Note by the Nullstellensatz that $P \not\supset P_1 \cap \dots \cap P_l$. Take $g \in P_1 \cap \dots \cap P_l$ with $g \notin P$. Note that X_g is an irreducible affine variety of the same dimension as X, and, by the choice of g, $Y \cap X_g$ is the zero set of f in X_g. On the other hand, $Y \cap X_g$ is a principal open sunset of Y, so it suffices to prove that its codimension in X_g is 1. So from the very beginning we may assume that $Y = Z(f)$ and $P = \sqrt{(f)}$.

Now, apply Noether's Normalization Lemma 2.2.28 to the domain $R := k[X]$: R is integral over some subring S isomorphic to $k[T_1, \dots, T_d]$, where $d = \dim X$. Let $E = k(X)$ and F be the field of fractions of S. Then E/F is finite (generated by fnitely many algebraic elements). By Corollary 2.2.27, the norm map $N_{E/F}$ takes values in S on elements of R.

Denote $N_{E/F}(f) =: f_0 \in S$. We claim that $f_0 \in P$. Let $\mathrm{irr}\,(f, F) = x^k + a_1 x^{k-1} + \dots + a_k \in S[x]$, see Lemma 2.2.26. By Lemma 2.2.25, f_0 is $\pm a_k^m$ for some m. Now $f_0 \in (f) \subseteq P$, in view of

$$\begin{aligned} 0 &= (f^k + a_1 f^{k-1} + \dots + a_k) a_k^{m-1} \\ &= f(f^{k-1} a_k^{m-1} + a_1 f^{k-2} a_k^{m-1} + \dots + a_{k-1} a_k^{m-1}) \pm f_0. \end{aligned}$$

Let Q be the radical of the ideal (f_0) in S. Then $Q \subseteq S \cap P$. We claim that $Q = S \cap P$. Indeed, let $g \in S \cap P$. Since $g \in P$, we have $g^l = fh$ for some $l \in \mathbb{N}$ and $h \in R$. Computing the norms, we get

$$g^{l[E:F]} = N_{E/F}(f) N_{E/F}(h) = f_0 N_{E/F}(h).$$

As $N_{E/F}(h) \in S$, we deduce that $g \in Q$.

We conclude that Q is a prime ideal in S. Since S is a UFD, it follows that f_0 is a power of an irreducible polynomial p in S, whence $Q = (p)$. Clearly p is not a scalar. Considering S as the algebra of regular functions on $\mathbb{A}^d$, we now conclude that $Z(Q)$ is an irreducible hypersurface of codimension 1, thanks to Proposition 4.5.8. So the transcendence degree of the quotient field of S/Q over k is $d-1$. On the other hand, R is integral over S implies that R/P is integral over $S/(P \cap S) = S/Q$. So the quotient field of R/P also has transcendence degree $d-1$ over k. But the last quotient field is $k(Y)$, so $\dim Y = d - 1$. □

Corollary 4.5.10 *Let X be an irreducible variety, U be an open subset of X, and $f \in \mathcal{O}_X(U)$ be a non-invertible element. Then every irreducible component of the zero set of f in U has codimension 1 in X.*

Proof Let Y be an irreducible component of the zero set of f in U, and V be an affine open subset in X contained in U with $Y \cap V \neq \varnothing$. Then using Theorem 4.5.9, we have $\dim Y = \dim(Y \cap V) = \dim V - 1 = \dim X - 1$. □

Corollary 4.5.11 *Let X be an irreducible variety, and $Y \subseteq X$ be an irreducible closed subset of codimension r. Then there exist irreducible closed subsets Y_i of codimension $1 \leq i \leq r$, such that $Y = Y_r \subset Y_{r-1} \subset \cdots \subset Y_1$.*

Proof By passing to the affine open subset which intersects Y, we may assume that X is affine. Apply induction on r. If $r = 1$, there is nothing to prove. Since $Y \neq X$, there exists a function $f \neq 0$ in $I(Y)$, and Y lies in an irreducible component Y_1 of $Z(f)$. By Theorem 4.5.9, codim $Y_1 = 1$, and we can apply induction. □

Corollary 4.5.12 (Topological Characterization of Dimension) *The dimension of an irreducible variety X is the largest integer d for which there exist a chain of non-empty irreducible closed subsets*

$$X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_d = X.$$

Proof This follows from Corollary 4.5.11 and the fact that the dimension of a proper closed subset of a variety is strictly smaller than the dimension of the variety. □

Remark 4.5.13 The topological characterization shows that, when X is irreducible affine, $\dim X$ is the Krull dimension $\dim k[X]$ of $k[X]$, i.e. the maximal length d of the chain of prime ideals $0 \subsetneq P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_d \subsetneq k[X]$. Now Theorem 4.5.9 can be restated as follows: let A be an affine k-algebra which is a domain, and $f \in A$ be neither zero nor a unit, and let P be a prime ideal minimal among those containing (f); then $\dim A/P = \dim A - 1$. This statement is a version *Krull's principal ideal theorem*.

Corollary 4.5.14 *Let X be an irreducible variety, $f_1, \dots, f_r \in \mathcal{O}_X(X)$. Then each irreducible component of the set $Z(f_1, \dots, f_r)$ has codimension at most r.*

Proof Apply Theorem 4.5.9. □

Remark 4.5.15 Let $X = \mathbb{A}^n$, $f_1 = T_1$, $f_2 = T_1 + 1$. Then $Z(f_1, f_2) = \varnothing$, which is of codimension ∞, because by agreement $\dim \varnothing = -\infty$. Think why this does not contradict Corollary 4.5.14.

Corollary 4.5.16 *Let X be an irreducible affine variety, and $Y \subset X$ be a closed irreducible subset of codimension $r \geq 1$. Then Y is a component of $Z(f_1, \dots, f_r)$ for some $f_1, \dots, f_r \in k[X]$.*

Proof We prove more generally that for closed irreducible subsets $Y_1 \supset Y_2 \supset \cdots \supset Y_r$ with codim $Y_i = i$ there exist functions $f_i \in k[X]$ such that all components of $Z(f_1, \dots, f_i)$ have codimension i, and Y_i is one of those components $(1 \leq i \leq r)$. This is indeed a more general statement in view of Corollary 4.5.11.

Apply induction on i. For $i = 1$ we use Corollary 4.5.5 to find a function f_1 such that Y_1 is a component of $Z(f_1)$, and then Theorem 4.5.9 to deduce that all components of $Z(f_1)$ have codimension 1.

Assume that the functions $f_1, \dots f_{i-1}$ have been found, and let $Y_{i-1} = Z_1, Z_2, \dots, Z_m$ be the irreducible components of $Z(f_1, \dots, f_{i-1})$. Each of them has codimension $i-1$, so none of them lies in Y_i. So $I(Z_j) \not\supset I(Y_i)$ for all $j = 1, \dots, m$. The ideals $I(Z_j)$ are prime, so it follows from Theorem 2.1.5 that their union also does not contain in $I(Y_i)$. Let f_i be a function which is zero on Y_i but which is not identically zero on all Z_j.

If Z is a component of $Z(f_1, \dots, f_i)$, then Z lies in one of the components Z_j of the set $Z(f_1, \dots, f_{i-1})$, and also in $Z(f_i)$. So Z is a component of $Z(f_i) \cap Z_j$, which by Theorem 4.5.9, has codimension 1 in

Z_j, and hence codimension i in X. Finally, the function f_i is zero on Y_i, and Y_i has codimension i, so Y_i is one of the components of $Z(f_1, \dots, f_i)$. $\square$

Remark 4.5.17 The statement shows that for a prime ideal P in an affine k-algebra which is a domain, if P has height r , then there exist elements $f_1, \dots, f_r$ such that P is minimal among the prime ideals containing $(f_1, \dots, f_r)$.

Remark 4.5.18 A closed subvariety X of $\mathbb{A}^n$ (resp. $\mathbb{P}^n$) of codimension r is called a *set theoretic complete intersection* if there exist r polynomials $f_i \in k[T_1, \dots, T_n]$ (resp. r homogeneous polynomials $f_i \in k[S_0, S_1, \dots, S_n]$) such that $X = Z(f_1, \dots, f_r)$. Moreover, X is called an *ideal theoretic complete intersection* if the f_i can be chosen so that $I(X) = (f_1, \dots, f_r)$.

4.6 Problems

Problem 4.6.1 Prove that the functors $\mathcal{F} : (X, \mathcal{O}_X) \mapsto k[X]$ and $\mathcal{G} : A \mapsto \operatorname{Specm} A$ are quasi-inverse equivalences of categories between affine varieties over k and affine k-algebras (this means $\mathcal{F}\mathcal{G} \cong \mathrm{Id}$ and $\mathcal{G}\mathcal{F} \cong \mathrm{Id}$).

Solution. To prove that $\mathcal{F}\mathcal{G} \cong \mathrm{Id}$, let A be an affine k-algebra. By definition, $k[\operatorname{Specm} A] \cong A$, where A is considered as an algebra of functions on $\operatorname{Specm} A$ via $a(x) = x(a)$, see Remark 4.1.8. It is easy to see that the isomorphism $k[\operatorname{Specm} A] \cong A$ is natural.

Now, let $(X, \mathcal{O}_X)$ be an affine variety. It follows from the axioms of the affine variety and the definition of $\operatorname{Specm} k[X]$ that

$$X \to \operatorname{Specm} k[X], \ x \mapsto \mathrm{ev}_x$$

is an isomorphism of varieties, which is clearly natural. So $\mathcal{G}\mathcal{F} \cong \mathrm{Id}$.

Problem 4.6.2 True or false? Let X be a prevariety and $U \subset X$ is a non-empty open subset. If $f \in \mathcal{O}_X(U)$ then f is a morphism from the prevariety U to $k = \mathbb{A}^1$.

Problem 4.6.3 Principal open sets in affine varieties are affine varieties.

Problem 4.6.4 Prove that $\mathbb{A}^2 \setminus \{(0,0)\}$ is not an affine variety.

Problem 4.6.5 Intersection of affine open subsets is affine.

Problem 4.6.6 Prove that a closed subset of an affine variety is again an affine variety without using affine algebraic sets.

Problem 4.6.7 Make sense out of Example 4.4.2.

Problem 4.6.8 The product of irreducible prevarieties varieties is irreducible.

Problem 4.6.9 Let $\varphi_1 : X_1 \to Y_1$ and $\varphi_2 : X_2 \to Y_2$ be morphisms of prevarieties. Then $\varphi_1 \times \varphi_2 : X_1 \times X_2 \to Y_1 \times Y_2,\ (x_1, x_2) \mapsto (\varphi_1(x_1), \varphi_2(x_2))$ is also a morphism of prevarieties.

Problem 4.6.10 Let X, Y be prevarieties. Prove that the projections $X \times Y \to X$ and $X \times Y \to Y$ are open maps, i.e. map open maps to open maps. Do they have to map closed sets to closed sets?

Problem 4.6.11 Let $\varphi : X \to Y$ be prevarieties. Prove that the projection π_1 induces an isomorphism from $\Gamma_\varphi \subset X \times Y$ onto X.

Problem 4.6.12 Let X, Y be prevarieties, and $X' \subset X, Y' \subset Y$ be subprevarieties. Explain how $X' \times Y'$ can be considered as a subprevariety of $X \times Y$.

Problem 4.6.13 Prove that any morphism $\mathbb{P}^1 \to \mathbb{A}^1$ must be constant.

Problem 4.6.14 Let $f : \mathbb{A}^1 \to \mathbb{A}^1$ be a morphism. Then there is a unique extension morphism $\tilde{f} : \mathbb{P}^1 \to \mathbb{P}^1$ such that $f|\mathbb{A}^1 = f$.

Problem 4.6.15 Show that every isomorphism $f : \mathbb{P}^1 \to \mathbb{P}^1$ is of the form $f(x) = \frac{ax+b}{cx+d}$ for some $a, b, c, d \in k$, where x is the coordinate on $\mathbb{A}^1$.

Problem 4.6.16 Prove that $\mathbb{P}^n$ is a variety.

Problem 4.6.17 Prove that the Veronese embedding is an isomorphism of $\mathbb{P}^n$ onto its image.

Problem 4.6.18 Let $X \subset \mathbb{P}^n$ be a projective algebraic set considered as a variety and $f \in k[S_0, \ldots, S_n]$ be a non-constant homogeneous polynomial. Then $X \setminus Z(f)$ is an affine variety. (*Hint:* Reduce to the case where f is linear using the Veronese embedding).

Problem 4.6.19 Prove that the product of projective varieties defined in §3.10 using Segre embedding is the categorical product.

Problem 4.6.20 Irreducible closed subvarieties of a variety X satisfy A.C.C.

Problem 4.6.21 The dimension of a linear subvariety of $\mathbb{A}^n$ (that is a subvariety defined by linear equations) has the value predicted by linear algebra.

Problem 4.6.22 Let X and Y be closed subvarieties of $\mathbb{A}^n$. For any non-empty irreducible component Z of $X \cap Y$, we have $\operatorname{codim} Z \le \operatorname{codim} X + \operatorname{codim} Y$.

Problem 4.6.23 Fill in the details for Example 4.5.2

Problem 4.6.24 Prove that $X \times \{\text{point}\} \cong X$.

5

Morphisms

5.1 Fibers

A *fiber* of a morphism $\varphi : X \to Y$ is a subset of the form $\varphi^{-1}(y)$ for $y \in Y$. As φ is continuous, fibers of φ are closed subvarieties in Y. Of course $\varphi^{-1}(y)$ is empty if $y \notin \operatorname{im} \varphi$.

If X is irreducible and $\varphi(X)$ is dense in Y we say that the morphism φ is *dominant.* In this case Y will also have to be irreducible, as the image of an irreducible topological space under a continuous map is irreducible and the closure of an irreducible subspace is irreducible. More generally, if X is not necessarily irreducible, then a morphism $\varphi : X \to Y$ is *dominant*, if φ maps every component of X onto a dense subset of some component of Y, and $\operatorname{im} \varphi$ is dense in Y.

If φ is a dominant morphism of irreducible varieties then the comorphism φ^* induces an embedding of $k(Y)$ into $k(X)$. In particular, $\dim X \geq \dim Y$.

Let $\varphi : X \to Y$ be a morphism, and $W \subseteq Y$ be an irreducible closed subset. If the restriction of φ to an irreducible component Z of $\varphi^{-1}(W)$ is dominant as a morphism from Z to W, then we say that Z *dominates* W. If $\operatorname{im} \varphi \cap W$ is dense in W then at least one of the components of $\varphi^{-1}(W)$ dominates W.

Theorem 5.1.1 *Let $\varphi : X \to Y$ be a dominant morphism of irreducible varieties, and let $r = \dim X - \dim Y$. Let W be a closed irreducible subset of Y, and Z be a component of $\varphi^{-1}(W)$ which dominates W. Then $\dim Z \geq \dim W + r$. In particular, if $y \in \operatorname{im} \varphi$, then the dimension of each component of the fiber $\varphi^{-1}(y)$ is at least r.*

Proof Let U be an affine open subset of Y which intersects W. Then

$U \cap W$ is dense in W, and hence irreducible. Also, $\varphi(Z) \cap U$ is dense in W. So for the purpose of comparing dimensions we can consider U instead of Y, $W \cap U$ instead of W, $\varphi^{-1}(U) \cap Z$ instead of Z, and $\varphi^{-1}(U)$ instead of X. Thus we may assume that Y is affine.

Let $s = \operatorname{codim}_Y W$. By Corollary 4.5.16, W is an irreducible component of $Z(f_1, \dots, f_s)$ for some $f_1, \dots, f_s \in k[Y]$. Setting $g_i = \varphi^*(f_i) \in \mathcal{O}_X(X)$, we have $Z \subseteq Z(g_1, \dots, g_s)$. As Z is irreducible, it actually lies in some component Z_0 of $Z(g_1, \dots, g_s)$. But by assumption $W = \overline{\varphi(Z)}$, and $\overline{\varphi(Z)} \subseteq \overline{\varphi(Z_0)} \subseteq Z(f_1, \dots, f_s)$. As W is a component of $Z(f_1, \dots, f_s)$, it follows that $\overline{\varphi(Z)} = \overline{\varphi(Z_0)} = W$, whence $Z_0 \subseteq \varphi^{-1}(W)$. But Z is a component of $\varphi^{-1}(W)$, so $Z = Z_0$, i.e. Z is a component of $Z(g_1, \dots, g_s)$. In view of Corollary 4.5.14, $\operatorname{codim}_X Z \leq s$. The theorem follows. □

The theorem says that the non-empty fibers of a morphism are not 'too small'. The following example shows that they can be 'too large'.

Example 5.1.2 Let $\varphi : \mathbb{A}^2 \to \mathbb{A}^2$ be the morphism given by $\varphi(x, y) = (x, xy)$. Then φ is dominant. The fiber $\varphi^{-1}((0,0))$ is the y-axis, so it is 1-dimensional. On the other hand, all other non-empty fibers have the 'right' dimension 0.

5.2 Finite morphisms

Let $\varphi : X \to Y$ be a morphism of affine varieties. If the ring $k[X]$ is integral over the subring $\varphi^*(k[Y])$, then we say that the morphism φ is *finite*. The main case is when X and Y are irreducible and φ is dominant and finite. Then we can consider $k[Y]$ as a subring of $k[X]$ and then $k(Y)$ as a subfield of $k(X)$. Moreover, since $k[X]$ is integral and finitely generated over $k[Y]$, $k(X)$ is a finite algebraic extension of $k(Y)$, so $\dim X = \dim Y$.

Fibers of finite maps are finite sets (which explains the terminology). Indeed, let $\varphi : X \to Y$ be finite, $X \subset \mathbb{A}^n$, and $t_1, \dots, t_n$ be the coordinates on $\mathbb{A}^n$ as functions on X. By definition, each t_i satisfies some equation of the form $t_i^k + \varphi^*(a_1)t_i^{k-1} + \dots + \varphi^*(a_k) = 0$ with $a_i \in k[Y]$. Let $y \in Y$ and $x \in \varphi^{-1}(y)$. Then

$$t_i(x)^k + a_1(y)t_i(x)^{k-1} + \dots + a_k(y) = 0,$$

which has only finitely many roots.

Note that the morphism φ from Example 5.1.2 is dominant but not finite. Indeed, T_2 is not integral over $\varphi^*(k[Y]) = k[T_1, T_1T_2]$.

Remark 5.2.1 If $\varphi : X \to Y$ is a surjective morphism of irreducible affine varieties, and all fibers are finite, then it can be proved that φ is finite, see [Sp, §5.2]. We will not pursue this now.

Example 5.2.2 Let X be an affine variety and G be a finite group of automorphisms of X, whose order N is prime to $\operatorname{char} k$. We claim that the projection map $\pi : X \to X/G$ is finite, cf. Example 3.5.7.

Theorem 5.2.3 *Let $\varphi : X \to Y$ be a finite morphism of affine varieties with $f(X)$ dense in Y. Then $\varphi(X) = Y$.*

Proof Let $y \in Y$, and let M_y be the corresponding maximal ideal of $k[Y]$. If $t_1, \dots, t_n$ are the coordinate functions on Y and $y = (a_1, \dots, a_n)$, then $M_y = (t_1 - a_1, \dots, t_n - a_n)$. Defining equations of the variety $\varphi^{-1}(y)$ are $\varphi^*(t_1) = a_1, \dots, \varphi^*(t_n) = a_n$, and $\varphi^{-1}(y)$ is empty if and only if $(\varphi^*(t_1) - a_1, \dots, \varphi^*(t_n) - a_n) = k[X]$. If we identify $k[Y]$ with the subring of $k[X]$ via φ^*, the last condition is equivalent to the condition $M_y k[X] = k[X]$.

Note that $k[X]$ is a finitely generated $k[Y]$-module in view of Proposition 2.2.7(ii). So by Corollary 2.1.7, $M_y k[X] \neq k[X]$. □

Corollary 5.2.4 *Finite maps are closed, i.e. they map closed sets onto closed sets. To be more precise, let $\varphi : X \to Y$ be a finite map, and let $Z \subset X$ be a closed subset. Then $\varphi|Z : Z \to \overline{\varphi(Z)}$ is finite. In particular, $\varphi(Z) = \overline{\varphi(Z)}$.*

Proof We may assume that $\overline{\varphi(X)} = Y$. Denote $R = k[X], S = k[Y]$. As φ^* is injective, we can identify S with a subring of R, and then R is integral over S, since φ is finite. If I is an ideal of R then $R/I \supset S/(I \cap S)$ is another integral ring extension.

Let $I = I(Z)$. Then $\overline{\varphi(Z)} = Z'$, where $Z' = Z(I \cap S)$. Moreover, $I' := I \cap S$ is radical, so $I' = I(Z')$. The affine algebras of Z and Z' are R/I and R/I', so the remarks in the previous paragraph show that $\varphi|Z : Z \to Z'$ is again finite and dominant. It remains to apply Theorem 5.2.3 to this map. □

Corollary 5.2.5 *Let $\varphi : X \to Y$ be a finite dominant morphism of irreducible affine varieties. Suppose that $k[Y]$ is integrally closed. If W is a closed irreducible subset of Y and Z is any component of $\varphi^{-1}(W)$, then $\varphi(Z) = W$.*

Proof Keep the notation of the proof of Corollary 5.2.4, and let $J = I(W)$. Then $I \cap S = I(\overline{\varphi(Z)}) = I(\varphi(Z))$ and I is a minimal prime ideal of R for which $I \cap S \supseteq J$. It follows from the Going Down Theorem 2.2.29 that $I \cap S = J$. So $\overline{\varphi(Z)} = W$. □

5.3 Image of a morphism

Let $S \subset R$ be two finitely generated domains over k with quotient fields $E \subset F$. Set $r := \operatorname{tr.deg}_E F$. Let R' be the localization of R with respect to the multiplicative system S^* of non-zero elements of S. Note that F is also field of fractions of R'. On the other hand R' contains E, so it can be considered as an E-algebra. By Noether's normalization lemma, R' is integral over a ring $E[T_1, \dots, T_r]$ for some algebraically independent elements $T_1, \dots, T_r$ over E. Note that $T_1, \dots, T_r$ can be chosen in R, as all possible denominators are in E.

Now compare the integral extension $E[T_1, \dots, T_r] \subset R'$ with the extension $S[T_1, \dots, T_r] \subset R$. The latter extension is not necessarily integral, but R is finitely generated over S as a ring. Moreover, each generator of R satisfies a monic polynomial equation over $E[T_1, \dots, T_r]$. If f is a common denominator of all coefficients appearing in such equations for all generators, then it is clear that R_f is integral over $S_f[T_1, \dots, T_r]$ (and $T_1, \dots, T_r$ are algebraically independent over S_f, because they are algebraically independent even over E). These remarks will be used in the proof of the following theorem.

Theorem 5.3.1 *Let $\varphi : X \to Y$ be a dominant morphism of irreducible varieties, and $r = \dim X - \dim Y$. Then*

(i) $\operatorname{im} \varphi$ *contains an open subset U of Y.*

(ii) *if all local rings of points of Y are integrally closed, then we can choose U in part* (i) *so that it has the following property: if $W \subset Y$ is an irreducible closed subset which meets U, and Z is a component of $\varphi^{-1}(W)$, which meets $\varphi^{-1}(U)$, then* $\dim Z = \dim W + r$.

Proof By passing to an open affine subset of Y, we may assume that Y is affine (cf. the proof of Theorem 5.1.1). We may also reduce to the case where X is affine. Indeed, let $X = \cup V_i$ be an open affine covering. As V_i is dense in X, we have $\varphi(V_i)$ is dense in X, so the restriction $\varphi|V_i : V_i \to Y$ is a dominant morphism of irreducible affine varieties.

Now, if U_i is an open subset of Y as in (i) or (ii) for $\varphi|V_i$, then $U = \cap_i V_i$ satisfies (i) and (ii), respectively.

Let $R = k[X], S = k[Y]$. Consider S as a subring of R in a usual way, and find elements $T_1, \dots, T_r \in R$, $f \in S$, such that R_f is integral over $S_f[T_1, \dots, T_r]$. Recall that $R_f = k[X_f]$ and $S_f = k[Y_f]$. So the affine algebra $S_f[T_1, \dots, T_r] \cong S_f \otimes k[T_1, \dots, T_r]$ can be considered as $k[Y_f \times \mathbb{A}^r]$. Then the restriction $\varphi|X_f : X_f \to Y_f$ can be decomposed as a composition $X_f \xrightarrow{\psi} Y_f \times \mathbb{A}^r \xrightarrow{\pi_1} Y_f$ where ψ is a finite dominant morphism. Set $U = Y_f$ and note that $\varphi^{-1}(U) = X_f$. Moreover, ψ is surjective by Theorem 5.2.3, and π_1 is obviously surjective, so $U \subseteq \varphi(X)$, which proves (i).

To prove (ii), we also set $X = X_f$, $U = Y = Y_f$. Then as above $\varphi = \pi_1 \circ \psi$, where ψ is a finite morphism. It follows from the assumption and (3.3) that the ring $k[Y] = S_f$ is integrally closed. Now by Theorem 2.2.15, $S_f[T_1, \dots, T_r]$ is also integrally closed. If W is a closed irreducible subset of Y and Z is any component of $\varphi^{-1}(W)$, then Z is a component of $\psi^{-1}(W \times \mathbb{A}^r)$. Hence $\psi(Z) = W \times \mathbb{A}^r$, and $\dim Z = \dim \psi(Z) = \dim W + r$, see Corollary 5.2.5. $\square$

In (ii) above it would be enough to assume that local rings are integrally closed only for some non-empty open subset of Y (we could pass from Y to this open subset in the very beginning of the proof). It will later turn out that this condition is always satisfied, see Theorem 6.3.1. So the assumption can actually be dropped.

Proposition 5.3.2 *Let $\varphi : X \to Y$ be a bijective morphism of irreducible varieties. Then $\dim X = \dim Y$, and there are open subsets $U \subset X$ and $V \subset Y$ such that $\varphi(U) = V$ and $\varphi|U : U \to V$ is a finite morphism.*

Proof We may assume that Y is affine. Let $W \subset X$ be an open affine subset. As W is dense in X, we have $\varphi(W)$ is dense in Y, so the restriction $\varphi|W : W \to Y$ is a dominant morphism of irreducible affine varieties. Let $R = k[W], S = k[Y]$. Consider S as a subring of R via $(\varphi|W)^*$, and find elements $x_1, \dots, x_r \in R$, $f \in S$, such that R_f is integral over $S_f[x_1, \dots, x_r]$. Recall that $R_f = k[W_f]$ and $S_f = k[Y_f]$. So the affine algebra $S_f[x_1, \dots, x_r] \cong S_f \otimes k[x_1, \dots, x_r]$ can be considered as $k[Y_f \times \mathbb{A}^r]$. Then the restriction $\varphi|W_f : W_f \to Y_f$ can be decomposed as a composition $W_f \xrightarrow{\psi} Y_f \times \mathbb{A}^r \xrightarrow{\pi_1} Y_f$ where ψ is a finite dominant morphism. Now, ψ is surjective by Theorem 5.2.3. Hence $\varphi|W_f : W_f \to$

Y_f is surjective, and hence bijective by our assumption. This is only possible if $r = 0$, so $\varphi|W_f : W_f \to Y_f$ is finite, and $\dim X = \dim Y$. $\square$

Recall that a subset of a topological space is called locally closed if it is an intersection of an open set and a closed set. A finite union of locally closed sets is called a *constructible set*.

Theorem 5.3.3 *Let $\varphi : X \to Y$ be a morphism of varieties. Then φ maps constructible sets onto constructible sets. In particular,* $\operatorname{im}\varphi$ *is constructible.*

Proof Locally closed subset of a variety is itself a variety, so it suffices to prove that $\operatorname{im}\varphi$ is constructible. We can also assume that X and Y are irreducible. Apply induction on $\dim Y$. If $\dim Y = 0$, there is nothing to prove. By inductive assumption, we may assume that φ is dominant.

Let U be an open subset contained in $\operatorname{im}\varphi$, see Theorem 5.3.1(i). Then the irreducible components W_i of $Y \setminus U$ have dimensions less than $\dim Y$. By induction, the restriction of φ to $Z_i := \varphi^{-1}(W_i)$ has image constructible in W_i, so also constructible in Y. Now, $\varphi(X)$ is a union of U and the constructible sets $\varphi(Z_i)$, so $\varphi(X)$ is also constructible. $\square$

Proposition 5.3.4 *Let $\varphi : X \to Y$ be a dominant morphism of irreducible varieties.*

(i) *The set $\{y \in Y \mid \dim\varphi^{-1}(y) \geq n\}$ is closed for any n.*
(ii) *For $x \in X$ let $\varepsilon_\varphi(x)$ denote the maximal dimension of any component of the set $\varphi^{-1}(\varphi(x))$ containing x. Then for all $n \geq 0$, the set $E_n(\varphi) := \{x \in X \mid \varepsilon_\varphi(x) \geq n\}$ is closed in X.*

Proof We prove (ii), the proof of (i) is very similar (and easier). Apply induction on $\dim Y$, the case $\dim Y = 0$ being clear. Let $r = \dim X - \dim Y$, and let U be an open subset contained in $\operatorname{im}\varphi$, see Theorem 5.3.1(i). By Theorem 5.1.1, $\varepsilon_\varphi(x) \geq r$ for all x, so $E_n(\varphi) = X$ for $n \leq r$, in particular $E_n(\varphi)$ is closed in this case. Let $n > r$. By Theorem 5.3.1, $E_n(\varphi) \subset X \setminus \varphi^{-1}(U)$. Let W_i be the irreducible components of the set $Y \setminus U$, W_{ij} be the irreducible components of $\varphi^{-1}(W_i)$ and $\varphi_{ij} : Z_{ij} \to W_i$ be the restriction of φ. Since $\dim W_i < \dim Y$, the set $E_n(\varphi_{ij})$ is closed in Z_{ij}, and hence in X. But for $n > r$ we have $E_n(\varphi) = \cup_{i,j} E_n(\varphi_{ij})$. $\square$

5.4 Open and birational morphisms

Example 5.1.2 shows that the image of an open set under a morphism does not have to be open.

Theorem 5.4.1 *Let $\varphi : X \to Y$ be a dominant morphism of irreducible varieties, and $r = \dim X - \dim Y$. Assume that for each closed irreducible subset $W \subset Y$ all irreducible components of $\varphi^{-1}(W)$ have dimension $r + \dim W$. Then φ is open.*

Proof Let $y \in Y$. By assumption, all irreducible components of $\varphi^{-1}(y)$ have dimension r. In particular, $\varphi^{-1}(y) \neq \varnothing$, whence φ is surjective. Moreover, let $W \subset Y$ be a closed irreducible subset and Z be an irreducible component of $\varphi^{-1}(W)$. By assumption, $\dim Z = r + \dim W$. Note that $\overline{\varphi(Z)} = W$, as otherwise $\dim \overline{\varphi(Z)} < \dim W$, and Z is an irreducible component of $\varphi^{-1}(\overline{\varphi(Z)})$, so we get a contradiction with our assumptions.

Now, let U be an open subset of X, $V = \varphi(U)$, and $y \in V$. Then $y = \varphi(x)$ for some $x \in U$. It suffices to prove that y is in the interior of V. Otherwise $y \in \overline{Y \setminus V}$. By Theorem 5.3.3, V is constructible, so $Y \setminus V$ is also constructible. It follows that y lies in the closure of some locally closed subset $O \cap C$ contained in $Y \setminus V$, where O is open and C is closed. We may assume that $C = \overline{O \cap C}$. Moreover, we may assume that C is irreducible, so $O \cap C$ is dense in C.

Now, each of the irreducible components of the set $C' := \varphi^{-1}(C)$ dominates C. So the set $O' := \varphi^{-1}(O)$ intersects each of the components non-trivially. So $O' \cap C'$ is dense in C'. But the set $O' \cap C' = \varphi^{-1}(O \cap C)$ lies in a closed subset $X \setminus U$, whence $C' \subset X \setminus U$. This contradicts the fact that $x \in C'$. □

Irreducible varieties X and Y are called *birationally isomorphic*, if $k(X)$ is k-isomorphic to $k(Y)$. A birationally isomorphic varieties do not have to be isomorphic, for example $\mathbb{A}^1$ is birationally isomorphic to $\mathbb{P}^1$. On the other hand:

Proposition 5.4.2 *Let X and Y be irreducible varieties. Then X and Y are birationally isomorphic if and only if there exist non-empty open subsets $U \subset Y$ and $V \subset X$ which are isomorphic.*

Proof The 'if-part' is clear. In the other direction, let $\varphi : k(Y) \to k(X)$ be a k-isomorphism. We may assume that X and Y are affine. Let

$f_1, \dots, f_n$ generate the ring $k[X]$ over k. Then for each i we can write $f_i = \frac{\varphi(g_i)}{\varphi(h)}$ $(g_i, h \in k[Y])$. So φ induces an isomorphism $k[Y]_h \xrightarrow{\sim} k[X]_{\varphi(h)}$. So we may take $U = Y_h$ and $V = X_{\varphi(h)}$. $\square$

A bijective morphism does not have to be an isomorphism. In fact its topological behavior and the effect of its comorphism on functions can be quite subtle. A typical example is the Frobenius map $\mathrm{Fr} : \mathbb{A}^1 \to \mathbb{A}^1$. But even in characteristic 0 one cannot assert that a bijective map is an isomorphism, see Problem 5.5.4. However, *Zariski's Main Theorem* claims that a bijective birational morphism $\varphi : X \to Y$ of irreducible varieties has to be an isomorphism if Y is smooth. (The smoothness will be defined in the next chapter. We will not prove Zariski's theorem).

Theorem 5.4.3 *Let $\varphi : X \to Y$ be a dominant, injective morphism of irreducible varieties. Then $k(X)$ is a finite purely inseparable extension of $\varphi^* k(Y)$.*

Proof See *Humhreys*, Theorem 4.6. $\square$

5.5 Problems

Problem 5.5.1 Give an example of a constructible set which is not locally closed.

Problem 5.5.2 Prove that the following are equivalent descriptions of the constructible sets in a topological space X:

(i) Constructible sets are finite *disjoint* union of locally closed sets.
(ii) Constructible sets are the sets expressible as

$$X \setminus (X_2 \setminus (X_3 \setminus \cdots \setminus X_n)) \dots)$$

for a nested sequence $X_1 \supset X_2 \supset X_3 \supset \cdots \supset X_n$ of closed subsets.
(ii) The class of constructible sets of X is the smallest class including open subsets and closed under the operations of finite intersections and complementation.

Problem 5.5.3 Prove that a constructible subset of a variety contains a dense open subset of its closure.

Problem 5.5.4 Define a morphism $\varphi : \mathbb{A}^1 \to \mathbb{A}^2$ by $\varphi(x) = (x^2, x^3)$. Then $X := \operatorname{im} \varphi$ is closed in $\mathbb{A}^2$ and the morphism $\varphi : \mathbb{A}^1 \to X$ is bijective, birational and homeomorphism, but it is not an isomorphism.

6
Tangent spaces

In this chapter, unless otherwise stated all varieties are assumed to be irreducible.

6.1 Definition of tangent space

If X is the curve $f(T_1, T_2) = 0$ in $\mathbb{A}^2$ then our 'multivariable calculus intuition' tells us the tangent space to X at $x = (x_1, x_2) \in X$ is the set of solutions of the linear equation

$$\frac{\partial f}{\partial T_1}(x)(T_1 - x_1) + \frac{\partial f}{\partial T_2}(x)(T_2 - x_2) = 0.$$

This 'tangent space' is a line unless both partial derivatives are zero at x. More generally, if $f \in k[T_1, \dots, T_n]$ set

$$d_x f = \sum_{i=1}^{n} \frac{\partial f}{\partial T_i}(x)(T_i - x_i).$$

Now, if $X \subset \mathbb{A}^n$ is a closed subset and $I = I(X)$ we define the *geometric tangent space* $\mathrm{Tan}(X)_x$ to X at x to be the linear variety $Z(J) \subset \mathbb{A}^n$ where the ideal J is generated by all $d_x f$ for $f \in I$. We consider $\mathrm{Tan}(X)_x$ as a verctor space with the origin at x. Problem 6.8.1 is handy for explicit calculations of geometric tangent spaces.

For any $f(T) \in k[T]$, $d_x f$ can be considered as a linear function on $\mathbb{A}^n$ with the origin at x, so on restriction to $\mathrm{Tan}(X)_x$, $d_x f$ is a linear function on $\mathrm{Tan}(X)_x$. By definition, $d_x f = 0$ on $\mathrm{Tan}(X)_x$ for $f \in I(X)$, so we can define the linear function $d_x f$ on $\mathrm{Tan}(X)_x$ for $f \in k[X]$. Thus d_x becomes a linear map from $k[X]$ to $\mathrm{Tan}(X)_x^*$. It is surjective, as any $g \in \mathrm{Tan}(X)_x^*$ is the restriction of a linear polynomial f on $\mathbb{A}^n$ (as usual, origin at x), and $d_x f = f$. Let M be the maximal ideal of $k[X]$

corresponding to x. As $k[X] = k \oplus M$, and d_x maps constants to zero, d_x induces a surjective map from M to $\mathrm{Tan}(X)_x^*$. We claim that the kernel of this map is M^2. By the product rule, $M^2 \subseteq \ker d_x$. Conversely, let $f \in M$ and $d_x f = 0$ on $\mathrm{Tan}(X)_x$. Assume that f is the image of some polynomial function $f(T)$ on $\mathbb{A}^n$. By Problem 6.8.1 and linear algebra, we have $d_x f = \sum_i a_i d_x f_i$ for some $a_i \in k$ and $f_i \in I(X)$. Then for $g := f - \sum_i a_i f_i$ we have $d_x g = 0$ on $\mathbb{A}^n$, which means that g does not contain linear terms $(T_i - x_i)$, i.e. g belongs to the square of the ideal generated by all $T_i - x_i$. The image of this ideal in $k[X]$ is M, and the image of g is f, so $f \in M^2$.

Thus, we have identified the vector space $\mathrm{Tan}(X)_x^*$ with M/M^2 or $\mathrm{Tan}(X)_x$ with $(M/M^2)^*$. Now, in view of Lemma 2.1.11, the vector space M/M^2 can be identified with $\mathfrak{m}_x/\mathfrak{m}_x^2$, where $\mathfrak{m}_x$ is the maximal ideal of the local ring $\mathcal{O}_x$. So, we have motivated the following 'invariant' definition.

Definition 6.1.1 The *tangent space* to the variety X at $x \in X$, denoted $T_x X$ is the k-vector space $(\mathfrak{m}_x/\mathfrak{m}_x^2)^*$.

We now give another description of $T_x X$. A *derivation at x* is a k-linear map $\delta : \mathcal{O}_x \to k$ such that $\delta(fg) = \delta(f)g(x) + f(x)\delta(g)$. We claim that the vector space of derivations at x is naturally isomorphic to $T_x X$. Indeed, if $\delta : \mathcal{O}_x \to k$ is a derivation, it follows easily that $\delta(f) = 0$ if f is a constant or if $f \in \mathfrak{m}_x^2$. So δ defines an element of $(\mathfrak{m}_x/\mathfrak{m}_x^2)^*$. This defines a map from the space of derivations at x to $T_x X$, which is easily shown to be an isomorphism.

Let X be an irreducible affine variety. We claim that in this case we can also identify $T_x X$ with the derivations of $k[X]$ at x, i.e. the linear maps $\delta : k[X] \to k$ such that $\delta(fg) = \delta(f)g(x) + f(x)\delta(g)$. Indeed, recall that under our assumptions $\mathcal{O}_x$ can be identified with the subring of $k(X)$ consisting of all rational functions which are regular at x. Now, if $\delta : \mathcal{O}_x \to k$ is a derivation, we get a derivation $\bar{\delta} : k[X] \to k$ on restriction. Conversely, if $\delta : k[X] \to k$ is a derivation and $h = \frac{f}{g} \in \mathcal{O}_x$ define $\hat{\delta}(h) = \frac{\delta(f)g(x) - f(x)\delta(g)}{g(x)^2}$ (the 'quotient rule'). It is easy to check that the maps $\delta \mapsto \bar{\delta}$ and $\delta \mapsto \hat{\delta}$ are inverse to each other.

Example 6.1.2 Let $X = \mathbb{A}^n$. The map $\frac{\partial}{\partial T_i}|_x : k[X] \to k,\ f \mapsto \frac{\partial f(x)}{\partial T_i}$ is a derivation of $k[X] = k[T_1, \dots, T_n]$ at x. It is easy to check that the derivations $\frac{\partial}{\partial T_1}|_x, \dots, \frac{\partial}{\partial T_n}|_x$ form a basis of $T_x X$, so $T_x X \cong k^n$. It follows that $T_x \mathbb{P}^n \cong k^n$ for any $x \in \mathbb{P}^n$.

Example 6.1.3 Let $X \subset \mathbb{A}^n$ be an affine irreducible variety. Then any derivation δ of $k[X] = k[T_1, \dots, T_n]/I(X)$ can be lifted to a derivation $\hat{\delta}$ of $k[X]$ at x. So by Example 6.1.2 any derivation of X at x looks like $\sum_{i=1}^n a_i \frac{\partial}{\partial T_i}|_x$ for some constants $a_i \in k$. Moreover, if $I(X) = (f_1, \dots, f_l)$, then $\sum_{i=1}^n a_i \frac{\partial}{\partial T_i}|_x$ is zero on $I(X)$ if and only if

$$\sum_{i=1}^n a_i \frac{\partial f_j(x)}{\partial T_i} \qquad (j = 1, \dots, l). \tag{6.1}$$

So $T_x X$ is a linear space of all tuples $(a_1, \dots, a_n) \in k^n$ satisfying the equations (6.1).

Example 6.1.4 Let X be given by the equation $y^2 = x^3$. Then $I(X) = (y^2 - x^3)$, and X is one-dimensional. On the other hand, using Example 6.1.3, one sees that the tangent space $T_x X$ is one-dimensional for all x, except for $x = (0, 0)$ when $T_x X$ is two-dimensional. Soon we will see that in general $\dim T_x X \geq \dim X$, and that the equality holds for 'almost all' points $x \in X$.

Proposition 6.1.5 *Let X, Y be irreducible varieties, $x \in X, y \in Y$. Then $T_{(x,y)}(X \times Y) \cong T_x X \oplus T_y Y$.*

Proof We may assume that X and Y are affine. If $\delta_1 : k[X] \to k$ is a derivation at x and $\delta_2 : k[Y] \to k$ is a derivation of $k[Y]$ at y, define the derivation

$$(\delta_1, \delta_2) : k[X \times Y] = k[X] \otimes k[Y] \to k, \ f \otimes g \mapsto \delta_1(f) g(y) + f(x) \delta_2(y)$$

of $k[X \times Y]$ at (x, y). This defines an isomorphism from $T_x X \oplus T_y Y$ to $T_{(x,y)}(X \times Y)$ (check!). $\square$

6.2 Simple points

Definition 6.2.1 Let X be an irreducible variety and $x \in X$. Then x is called a *simple* point if $\dim T_x X = \dim X$. Otherwise x is called *singular*. If all points of X are simple, then X is called *smooth* (or *non-singular*).

So $\mathbb{A}^n$ and $\mathbb{P}^n$ are smooth and the product of smooth varieties is smooth.

Lemma 6.2.2 *Let $X = Z(f)$ be an irreducible hypersurface in $\mathbb{A}^n$. Then* $\dim T_x X = \dim X$ *for all points x from some open dense subset of X.*

Proof We may assume that f is an irreducible polynomial. The tangent space $T_x X$ is the set of all n-tuples $(a_1, \dots, a_n) \in k^n$ satisfying the linear equation $\sum_{i=1}^n a_i \frac{\partial f(x)}{\partial T_i} = 0$. Since $\dim X = n-1$, a point x is singular if and only if all $\frac{\partial f(x)}{\partial T_i} = 0$. If the polynomial $\frac{\partial f}{\partial T_i}$ is non-zero, then it is not identically zero on X, as otherwise it would be divisible by f, which is impossible by degrees. So we may assume that $\operatorname{char} k = p$ and all degrees of all variables T_i in f are divisible by p, but then $f = g^p$ by 'Freshman's Dream', which contradicts the irreducibility of f. □

Theorem 6.2.3 *Let X be an irreducible variety. Then* $\dim T_x X \geq \dim X$ *for any $x \in X$, and the equality holds for all points x from some open dense subset of X.*

Proof By Theorem 2.1.12, $k(X)$ is separably generated over k, i.e. $k(X)$ is a finite separable extension of $L = k(t_1, \dots, t_d)$, which in turn is a purely transcendental extension of k. Note that $d = \dim X$. By the Primitive Element Theorem 2.1.13, $K = L(t_0)$ for some element $t_0 \in K$. Let $f(T_0) := \operatorname{irr}(t_0; L) \in L[T_0]$ be the minimal polynomial. Since the coefficients of f are rational functions in $k(t_1, \dots, t_d)$, this polynomial can be considered as a rational function $f(T_0, T_1, \dots, T_d) \in k(T_0, T_1, \dots, T_d)$. This rational function is defined on a principal open subset of $\mathbb{A}^{d+1}$, and the zero locus Y of f is an irreducible hypersurface in this principal open subset.

We claim that $k(Y) \cong k(X)$. Indeed, let s_i be the restriction of the coordinate function T_i to Y for $0 \leq i \leq n$. Then $k(Y) = k(s_0, s_1, \dots, s_d)$. As $\dim Y = d$ and s_0 is algebraic over $k(s_1, \dots, s_d)$, we conclude that $s_1, \dots, s_d$ are algebraically independent over k. Now, it is clear that the minimal polynomial of s_0 over $k(s_1, \dots, s_d)$ is f, whence the claim.

By Proposition 5.4.2, there exist non-empty open subsets in X and Y which are isomorphic. By Lemma 6.2.2, the set of points $y \in Y$ for which $\dim T_y Y = \dim Y$ form an open subset in Y, so the same follows for X.

Let x be an arbitrary point of X. In order to find the dimension of $T_x X$ we may pass to an affine open neighborhood of x. So we may assume that X is a closed subset of some $\mathbb{A}^n$. Then $T_x X$ can be considered as a vector subspace of k^n. By shifting the origin to x we have $T_x X$ as an affine subspace of $\mathbb{A}^n$ through x. Let T be the subset of all $(x, y) \in X \times \mathbb{A}^n$ for which $y \in T_x X$. Note that T is a closed subset. Indeed, it is given by the equations for X together with the polynomial equations of the form $\sum_{i=1}^{n} \frac{\partial f_j(x)}{\partial T_i}(S_i - x_i)$, where S_i are the coordinates in $\mathbb{A}^n$. Projection pr_1 defines a morphism $\varphi : T \to X$ whose fiber $\varphi^{-1}(x)$ has dimension $\dim T_x X$. For each m the subset $X_m = \{x \in X \mid \dim \varphi^{-1}(x) \geq m\}$ is closed in X, see Proposition 5.3.4(i). But we saw that X_d is dense in X, so $X_d = X$. $\square$

6.3 Local ring of a simple point

Let X be an irreducible variety and $x \in X$. By Corollary 2.1.10, the minimal number n of generators of the ideal $\mathfrak{m}_x$ equals the dimension of $\mathfrak{m}_x/\mathfrak{m}_x^2$ or $\dim T_x X$. So the point x is simple if and only if $n = \dim X$. Recall that the *Krull dimension* of a Noetherian ring R is defined to be the largest length k of a chain

$$0 \subsetneqq P_1 \subsetneqq P_2 \subsetneqq \cdots \subsetneqq P_k \subsetneqq R$$

of prime ideals.

We claim that the Krull dimension of $\mathcal{O}_x$ equals $\dim X$. Indeed, we may assume that X is affine, in which case $\mathcal{O}_x = k[X]_{M_x}$. But the prime ideals of $k[X]_{M_x}$ are in one-to-one correspondence with prime ideals of $k[X]$ contained in M_x, and it follows from Corollaries 4.5.11 and 4.5.12 that $\dim X$ is the largest length k of a chain

$$0 \subsetneqq P_1 \subsetneqq P_2 \subsetneqq \cdots \subsetneqq P_k = M_x$$

of prime ideals in $k[X]$.

A local ring (R, M) is called *regular* if its Krull dimension equals the number of generators of the maximal ideal M. We have established that a point $x \in X$ is simple if and only if its local ring $\mathcal{O}_x$ is regular. So, in view of Theorem 2.1.15, we have:

Theorem 6.3.1 *Let x be a simple point of an irreducible variety X. Then $\mathcal{O}_x$ is a regular local ring. In particular, it is a UFD and is integrally closed.*

Theorem 6.3.2 *Let X be an irreducible variety and $x \in X$ be a point such that $\mathcal{O}_x$ is integrally closed. Let $f \in K(X) \setminus \mathcal{O}_x$. Then there exists a subvariety $Y \subset X$ containing x and such that $f' := \frac{1}{f} \in \mathcal{O}_y$ for some $y \in Y$, and f' is equal to zero on Y everywhere where it is defined.*

Proof Let $R = \mathcal{O}_x$. Then $I := \{g \in R \mid gf \in R\}$ is a proper ideal of R, as $1 \notin I$, and so $I \subset \mathfrak{m}_x$. Let $P = P_1, P_2, \dots, P_t$ be the distinct minimal prime ideals containing I. Then $P_1 \cap \dots \cap P_t/I$ is nilpotent, i.e. $P^n P_2^n \dots P_t^n \subset I$. For $i > 1$, P_i generates in the local ring $R_P \subset k(X)$ the ideal coinciding with the whole R_P. So $P^n R_P \subset IR_P$. In particular, since $If \subset R$, we have $P^n f \subset (If)R_p \subset R_P$. Choose $k \geq 0$ the minimal possible so that $P^k f \subset R_P$, and let $g \in P^{k-1}f \setminus R_P$. Then $Pg \subset R_P$.

By assumption R is integrally closed, so R_P is integrally closed, see Proposition 2.2.13. As $g \notin R_P$, the element g is not integral over R_P. Now, if $PR_Pg \subseteq PR_P$, then the ring $R_P[g]$ acts faithfully on the finitely generated R_P-module PR_P, giving a contradiction, see Proposition 2.2.5(iii). So $Pg \subset R_P$ generates the ideal R_P in R_P, hence contains an invertible element from R_P. So $\frac{1}{g} \in PR_P$, and $PR_P = \frac{1}{g}R_P$.

Now, $h := \frac{f}{g^k} \in fP^kR_P \subset R_P$. We claim that h is a unit in R_P. Otherwise $h \in PR_P = \frac{1}{g}R_P$ or $\frac{f}{g^{k-1}} \in R_P$, which contradicts the choice of k. So $\frac{1}{f} = h^{-1}\frac{1}{g^k} \in PR_P$.

Let P be generated by the elements $f_1, \dots, f_l \in \mathcal{O}_x$. Then f_i are rational functions regular in some neighborhood of x, so also in some affine neighborhood of x. Now let Y be the zero locus of the functions $f_1, \dots, f_l$ in this affine neighborhood. Then all functions of P are zero everywhere on Y where they are defined. So this is also true for the function $\frac{1}{f} \in PR_P$. Also $x \in Y$, as $P \subset \mathfrak{m}_x$. $\square$

6.4 Differential of a morphism

Let $\varphi : X \to Y$ be a morphism of (irreducible) varieties, $x \in X$, $y = \varphi(x)$. Then $\varphi^*(\mathcal{O}_y) \subset \mathcal{O}_x$, and $\varphi^*(\mathfrak{m}_y) \subset \mathfrak{m}_x$. So φ^* induces a map $\mathfrak{m}_y/\mathfrak{m}_y^2 \to \mathfrak{m}_x/\mathfrak{m}_x^2$, which in turn induces a map $(\mathfrak{m}_x/\mathfrak{m}_x^2)^* \to (\mathfrak{m}_y/\mathfrak{m}_y^2)^*$. This map is denoted $d\varphi_x$ and is called the *differential* of φ at x. Thus:

$$d\varphi_x : T_xX \to T_{\varphi(x)}Y.$$

In terms of derivations, $d\varphi_x$ can be described similarly: if $\delta : \mathcal{O}_x \to k$ is a derivation, then $d\varphi_x(\delta)$ is defined to be $\delta \circ \varphi^* : \mathcal{O}_y \to k$. The following natural properties are easy to check:

$$d_x \,\mathrm{id} = \mathrm{id} \quad \text{and} \quad d(\psi \circ \varphi)_x = d\psi_{\varphi(x)} \circ d\varphi_x.$$

Example 6.4.1 Let $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ be affine algebraic sets and $\varphi : X \to Y$ be the restriction of $\varphi = (\varphi_1, \dots, \varphi_m)$ with $\varphi_i \in k[T_1, \dots, T_n]$. Take $x \in X$ and let $y = \varphi(x)$. We identify T_xX and T_yY

with subspaces of k^n and k^m, respectively, following Example 6.1.3. If $a = (a_1, \dots, a_n) \in T_xX$, then $d\varphi_x(a) = (b_1, \dots, b_m)$, where

$$b_j = \sum_i \frac{\partial \varphi_j}{\partial T_i}(x) a_i,$$

i.e. $d\varphi_x$ is the linear map whose matrix is the Jacobian of φ at x.

Example 6.4.2 Let $X = GL_n(k)$, $Y = GL_1(k) = k^\times$, and $\varphi = \det$. Note that X is the principal open set in $\mathbb{A}^{n^2}$ which we identify with $M_n(k)$, all $n \times n$ matrices. It is easy to see that at every point $x \in GL_n(k)$ the tangent space $T_xGL_n(k)$ can be identified with $M_n(k)$. Let e be the identity matrix. Under our identification, $d\det_e : M_n(k) \to M_1(k) = k$ is tr, the *trace* map.

Let $\varphi : X \to Y$ be a dominant morphism of irreducible varieties. Then $k(Y)$ can be considered as a subfield of $k(X)$ via φ^*. If the extension $k(X)/k(Y)$ is separable, we say that the morphism φ is *separable*.

In characteristic 0 all morphisms are separable. An example of a non-separable morphism is given by the Frobenius morphism.

We are going to develop some machinery which will help us to establish a differential criterion for separability and to consider tangent spaces from a new point of view.

6.5 Module of differentials

For a k-algebra A and an A-module M, we write

$$\mathrm{Der}_k(A, M)$$

for the space of all *k-linear derivations* from A to M, i.e. k-linear maps $f : A \to M$ such that $f(ab) = af(b) + bf(a)$ for all $a, b \in A$.

Let $m : A \otimes_k A \to A$ be the multiplication, and let $I := \ker m$, the ideal generated by all $a \otimes 1 - 1 \otimes a$ $(a \in A)$. Define the *module of differentials* $\Omega_{A/k}$ to be

$$\Omega_{A/k} := I/I^2.$$

This is an $A \otimes_k A$-module annihilated by I, so it can be considered as a module over $A \cong (A \otimes A)/I$. Let da denote the image of $a \otimes 1 - 1 \otimes a$ in $\Omega_{A/k}$. Note that the map $d : a \mapsto da$ is a derivation from A to the

A-module $\Omega_{A/k}$:

$$\begin{aligned} ad(b) + d(a)b &= a(b \otimes 1 - 1 \otimes b) + (a \otimes 1 - 1 \otimes a)b + I^2 \\ &= ab \otimes 1 - 1 \otimes ab + I^2 = d(ab). \end{aligned}$$

The elements da for $a \in A$ generate $\Omega_{A/k}$ as an A-module. One should think of $\Omega_{A/k}$ as the universal module for derivations of A:

Theorem 6.5.1 *Suppose that M is an A-module and $D : A \to M$ is a k-derivation. Then there exists a unique A-module homomorphism $\varphi : \Omega_{A/k} \to M$ such that $D = \varphi \circ d$, i.e. the map*

$$\mathrm{Hom}_A(\Omega_{A/k}, M) \to \mathrm{Der}_k(A, M), \quad \varphi \mapsto \varphi \circ d$$

is an isomorphism.

Proof Define the linear map

$$\psi : A \otimes A \to M, a \otimes b \mapsto bD(a).$$

One checks that for arbitrary elements $x, y \in A \otimes A$,

$$\psi(xy) = m(x)\psi(y) + m(y)\psi(x),$$

hence ψ vanishes on I^2. Therefore it induces a map $\varphi : \Omega_{A/k} \to M$ which is actually an A-module map, such that $\varphi(da) = \psi(a \otimes 1 - 1 \otimes a) = D(a)$ (here we have used that $D(1) = 0$). For uniqueness use the fact that the da generate $\Omega_{A/k}$ as an A-module. □

The theorem gives a universal property for the pair $(\Omega_{A/k}, d)$ which as usual characterizes it up to a unique A-module isomorphism.

Example 6.5.2 (i) Let F be any field, $A = F[T_1, \ldots, T_n]/(f_1, \ldots, f_m)$, and $t_i = T_i + (f_1, \ldots, f_m) \in A$. Then the dt_i generate $\Omega_{A/F}$ as an A-module, since the t_i generate A as an algebra. Moreover, the kernel of the A-module homomorphism

$$A^n = \bigoplus_{i=1}^{n} Ae_i \to \Omega_{A/F}, \; e_i \mapsto dt_i$$

is the submodule K of A^n generated by the elements

$$\sum_{i=1}^{n} \frac{\partial f_j}{\partial T_i}(t_1, \ldots, t_n)e_i \qquad (1 \le j \le m).$$

Indeed, consider the map

$$d' : A \to A^n/K,\ f \mapsto \sum_{i=1}^{n} \frac{\partial f}{\partial T_i}(t_1, \ldots, t_n)e_i$$

($\frac{\partial f}{\partial T_i}(t_1, \ldots, t_n)$ means: take any representative $\tilde{f}(T_1, \ldots, T_n)$ in $F[T]$, take the partial derivative of $\tilde{f}$, and pass to the quotient again.) The result follows from the fact that $(A^n/K, d')$ satisfy the universal property of the theorem.

(ii) Consider two special cases of (i): when $A = k[T_1, \ldots, T_n]$, then $\Omega_{A/k}$ is a *free* module on the basis $dT_1, \ldots, dT_n$; when $A = k[T_1, T_2]/(T_1^2 - T_2^3)$, then $\Omega_{A/k} = (Ae_1 \oplus Ae_2)/(2t_1e_1 - 3t_2^2e_2)$, which is not a free A-module.

(iii) Let A be an integral domain with quotient field E. Then $\Omega_{E/k} = E \otimes_A \Omega_{A/k}$. Indeed, the derivation $d : A \to \Omega_{A/k}$ induces a derivation $\hat{d} : E \to E \otimes_A \Omega_{A/k}$. We claim that $E \otimes_A \Omega_{A/k}$ together with $\hat{d}$ has the correct universal property. Take an E-module M and a derivation $\hat{D} : E \to M$. Its restriction D to A is a derivation $A \to M$. Hence there exists a unique A-module homomorphism $\varphi : \Omega_{A/k} \to M$ with $D = \varphi \circ d$. Hence since M is an E-module, there is a unique E-module homomorphism $\hat{\varphi} : E \otimes_A \Omega_{A/k} \to M$ with $\hat{D} = \hat{\varphi} \circ \hat{d}$.

(iv) Suppose that $E = k(x_1, \ldots, x_n)$ is a finitely generated field extension of k. By (iii) and (i), $\Omega_{E/k}$ is the E-vector space spanned by $dx_1, \ldots, dx_n$. In particular, it is finite dimensional.

Example 6.5.3 Let X be an affine variety, $x \in X$, and $k_x = k$ be the 1-dimensional $k[X]$-module with action $f \cdot c = f(x)c$ for $f \in k[X], c \in k$. Denote $\Omega_X := \Omega_{k[X]/k}$. By the theorem,

$$\mathrm{Hom}_{k[X]}(\Omega_X, k_x) \cong \mathrm{Der}_k(k[X], k_x) \cong T_xX$$

Now, if $X \subset \mathbb{A}^n$ is closed and $I(X) = (f_1, \ldots, f_m)$, it follows from Example 6.5.2(i) that Ω_X is generated by $dt_1, \ldots, dt_m$ and the relations

$$\sum_{i=1}^{n} \frac{\partial f_j}{\partial T_i}(t_1, \ldots, t_n)dt_i = 0 \qquad (1 \le j \le m).$$

Now, it is clear that $\mathrm{Hom}_{k[X]}(\Omega_X, k_x)$ is the vector space of all n-tuples $(a_1, \ldots, a_n)$ satisfying equations

$$\sum_{i=1}^{n} \frac{\partial f_j}{\partial T_i}(x)a_i = 0 \qquad (1 \le j \le m).$$

So we recover the description of the tangent space from Example 6.1.3.

Now for the remainder of the section we will be concerned with the following situation: we are given finitely generated field extensions $F/E/k$. Then there exists an exact sequence

$$0 \to \mathrm{Der}_E(F, F) \to \mathrm{Der}_k(F, F) \to \mathrm{Der}_k(E, F).$$

The first map is the obvious inclusion and the second map is induced by restriction of functions from F to E. To check the exactness in the second term, note that any $D \in \mathrm{Der}_E(F, F)$ maps E to zero, and conversely, any $f \in \mathrm{Der}_k(F, F)$ that maps elements of E to zero is E-linear.

Applying the universal property we have an exact sequence

$$0 \to \mathrm{Hom}_F(\Omega_{F/E}, F) \to \mathrm{Hom}_F(\Omega_{F/k}, F) \to \mathrm{Hom}_E(\Omega_{E/k}, F).$$

Also note that $\mathrm{Hom}_E(\Omega_{E/k}, F) \cong \mathrm{Hom}_F(F \otimes \Omega_{E/k}, F)$. So we have an exact sequence of finite dimensional F-vector spaces

$$0 \to \mathrm{Hom}_F(\Omega_{F/E}, F) \to \mathrm{Hom}_F(\Omega_{F/k}, F) \to \mathrm{Hom}_F(F \otimes \Omega_{E/k}, F).$$

Dualizing we get

$$F \otimes \Omega_{E/k} \xrightarrow{\alpha} \Omega_{F/k} \xrightarrow{\beta} \Omega_{F/E} \longrightarrow 0,$$

where α sends $1 \otimes d_{E/k}a$ to $d_{F/k}a$, viewing $a \in E$ as an element of F, and β is induced by the derivation $d_{F/E} : F \to \Omega_{F/E}$ according to the universal property of $\Omega_{F/k}$.

Lemma 6.5.4 *If F is a finite dimensional separable extension of E then α is injective.*

Proof By the above discussion, this is equivalent to the restriction map $\mathrm{Der}_k(F, F) \to \mathrm{Der}_k(E, F)$ being surjective. Equivalently, every k-derivation from E to F can be extended to a derivation from F to F. By the Primitive Element Theorem, we may assume that $F = E[T]/(f(T))$, where

$$f(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$$

is an irreducible polynomial and (this is what separability means) $f'(x) \neq 0$, where x is the image under the quotient map of T in F.

Let $D : E \to F$ be a derivation. To extend D to a derivation $\hat{D}$ from F to F, we just need to decide what $\hat{D}(x)$ should be: then the derivation formula means that there is no choice for defining $\hat{D}$ applied to any other element of $F = E[x]$. To decide on $\hat{D}(x)$ we need for well-definedness that $\hat{D}(f(x)) = 0$, i.e.

$$f'(x)\hat{D}(x) + \sum D(a_i)x^i = 0.$$

Since $f'(x) \neq 0$, we can solve this equation for $\hat{D}(x)$ in the field F. $\square$

Lemma 6.5.5 *Let $F = E(x)$. Then $\dim_F \Omega_{F/E} \leq 1$. Moreover, $\Omega_{F/E} = 0$ if and only if F/E is a finite separable extension.*

Proof By Example 6.5.2(iii), $\Omega_{F/E} = F \otimes_{E[x]} \Omega_{E[x]/E}$. If x is transcendental over E, we have $\Omega_{E[x]/E}$ is free of rank 1, cf. Example 6.5.2(i). If x is algebraic, by Example 6.5.2(i) again we have $\Omega_{E[x]/E} = E[x]/(f'(x))$, where $f(x) = \mathrm{irr}\,(x; E)$. If F/E is not separable, then $f'(x) = 0$, and we again get that $\Omega_{F/E}$ is one-dimensional. Finally, if F/E is separable, then $f'(x) \neq 0$, and $\Omega_{F/E} = F \otimes_{E[x]} \Omega_{E[x]/E} = 0$, since it is generated by $1 \otimes 1 = f'(x)^{-1}f'(x) \otimes 1 = 0$. $\square$

Theorem 6.5.6 (Differential Criterion for Separability) *Let $F = E(x_1, \dots, x_m)$ be a finitely generated field extension. Then:*

(i) $\dim_F \Omega_{F/E} \geq \mathrm{tr.deg}_E F$.
(ii) *Equality in* (i) *holds if and only if F/E is a separable extension.*

Proof Proceed by induction on $d = \dim_F \Omega_{F/E}$. If $d = 0$, i.e. $\Omega_{F/E} = 0$ to get (i) and (ii), we just need to show that F/E is a finite separable extension. For this we use induction on m, the case $m = 1$ being Lemma 6.5.5. Now suppose $m > 1$. Set $E' = E(x_m)$, so $F = E'(x_1, \dots, x_{m-1})$. Using the exact sequence

$$F \otimes \Omega_{E'/E} \xrightarrow{\alpha} \Omega_{F/E} \xrightarrow{\beta} \Omega_{F/E'} \longrightarrow 0,$$

we see that $\Omega_{F/E'} = 0$. Hence by induction F/E' is a finite separable extension. So by Lemma 6.5.4, α is injective, whence $\Omega_{E'/E} = 0$, and E'/E is a finite separable extension. By transitivity, F/E is a finite separable extension.

Now suppose $d > 0$. Pick $x \in F$ with $d_{F/E}x \neq 0$, and let $E' := E(x)$. We have the exact sequence

$$F \otimes \Omega_{E'/E} \xrightarrow{\alpha} \Omega_{F/E} \xrightarrow{\beta} \Omega_{F/E'} \longrightarrow 0.$$

Since $\alpha(1 \otimes d_{E'/E}x) = d_{F/E}x \neq 0$, we have $\Omega_{E'/E} \neq 0$. So by Lemma 6.5.5,

$\dim_{E'} \Omega_{E'/E} = 1$, which means that α is injective. So $\dim_F \Omega_{F/E} = \dim_F \Omega_{F/E'} + 1$. By induction, $\dim_F \Omega_{F/E} \geq \operatorname{tr.deg}_{E'} F + 1$. Since

$$\operatorname{tr.deg}_E F = \operatorname{tr.deg}_{E'} F + \operatorname{tr.deg}_E E' \leq \operatorname{tr.deg}_{E'} F + 1,$$

we get $\dim_F \Omega_{F/E} \geq \operatorname{tr.deg}_E F$, which is (i). With a little further argument along the same lines, one gets (ii). □

Corollary 6.5.7 *Assume that $E \subset F$ are finitely generated field extensions of k. Then F/E is separable if and only if the natural map* $\operatorname{Der}_k(F, F) \to \operatorname{Der}_k(E, F)$ *is surjective.*

Proof As above, $\operatorname{Der}_k(F, F) \to \operatorname{Der}_k(E, F)$ is surjective if and only if the map

$$\alpha : F \otimes_E \Omega_{E/k} \to \Omega_{F/k}$$

is injective. Consider the exact sequence

$$F \otimes \Omega_{E/k} \xrightarrow{\alpha} \Omega_{F/k} \xrightarrow{\beta} \Omega_{F/E} \longrightarrow 0.$$

As k is algebraically closed, every extension of k is separable, so by the theorem, $\dim_F F \otimes_E \Omega_{E/k} = \dim_E \Omega_{E/k} = \operatorname{tr.deg}_k E$ and $\dim_F \Omega_{F/k} = \operatorname{tr.deg}_k F$. Hence α is injective if and only if

$$\dim_F \Omega_{F/E} = \operatorname{tr.deg}_k F - \operatorname{tr.deg}_k E = \operatorname{tr.deg}_E F.$$

By the theorem, this is if and only if F/E is separable. □

6.6 Simple points revisited

Suppose that A is an integral domain with field of fractions F. Let $R = (r_{i,j})$ be an $m \times n$ matrix with entries in A. Consider the A-module

$$M_A(R) := \bigoplus_{j=1}^{n} Ae_i / \langle \sum_{j=1}^{n} r_{i,j} e_j \mid i = 1, \dots, m \rangle$$

given by generators and relations. If Y is an invertible $m \times m$ matrix with entries in A, then the change of basis argument gives $M_A(YR) \cong M_A(R)$. Similarly, if Z is an invertible $n \times n$ matrix with entries in A, then $M_A(RZ) \cong M_A(R)$. Now by linear algebra we can find invertible matrices Y and Z *with entries in F* such that

$$R = Y \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} Z,$$

where r is the rank of R. Putting all entries of Y and Z over a common denominator, we may assume that Y and Z have entries in A_f for some non-zero $f \in A$. Note that

$$M_A(R)_f \cong M_{A_f}(R).$$

So $M_A(R)_f$ is a free A_f-module of rank $n - r$.

Recall that if X is an affine variety, we write Ω_X for $\Omega_{k[X]/k}$. If $x \in X$, let us also write $\Omega_X(x)$ for the vector space $k_x \otimes_{k[X]} \Omega_X$. This is called *cotangent space* for $\Omega_X(x) \cong (T_xX)^*$. Indeed, using Example 6.5.3, we have

$$T_xX = \mathrm{Hom}_{k[X]}(\Omega_X, k_x) \cong \mathrm{Hom}_k(k_x \otimes_{k[X]} \Omega_X, k) = \Omega_X(x)^*.$$

If $k[X] = k[T_1, \ldots, T_n]/(f_1, \ldots, f_m)$, let R be the $m \times n$ matrix $(\frac{\partial f_j}{\partial T_i}(t))$ and $R(x) = (\frac{\partial f_j}{\partial T_i}(x))$. Then $\Omega_X = M_{k[X]}(R)$ and $\Omega_X(x) = M_k(R(x))$.

Lemma 6.6.1 *Assume that X is an irreducible affine variety.*

(i) $\dim_{k(X)} M_{k(X)}(R) = \dim X$.
(ii) *If $x \in X$ is a simple point, then there is $f \in k[X]$ with $f(x) \neq 0$ such that $M_{k[X]}(R)_f$ is a free $k[X]_f$-module of rank* $\dim X$ *with basis given by* $\dim X$ *out of the images of the e_i.*

Proof (i) Since k is algebraically closed, $k(X)$ is a separable extension of k. So Theorem 6.5.6 tells us that $\dim X = \dim_{k(X)} \Omega_{k(X)/k}$. But $\Omega_{k(X)/k} = k(X) \otimes_{k[X]} \Omega_X \cong M_{k(X)}(R)$.

(ii) In view of (i), the rank of the matrix R is $r := n - \dim X$. Some $r \times r$-minor of $R(x)$ has non-zero determinant. Reordering if necessary we may assume that this is the principal minor in the top left hand corner. Let f be the determinant of this minor, so $f(x) \neq 0$. On localizing at f, the matrix R becomes equivalent to

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}.$$

□

The lemma implies

Theorem 6.6.2 *Let X be an irreducible variety. If $x \in X$ is a simple point, there is an affine neighborhood U of x such that Ω_U is a free $k[U]$-module on basis $dg_1, \ldots, dg_{\dim X}$ for suitable $g_i \in k[U]$.*

6.7 Separable morphisms

Recall that if X is an affine variety, we write Ω_X for $\Omega_{k[X]/k}$ and $\Omega_X(x)$ for the cotangent space $k_x \otimes_{k[X]} \Omega_X$ at X.

Let $\varphi : X \to Y$ be a separable dominant morphism of irreducible affine varieties. The composition of $\varphi^* : k[Y] \to k[X]$ and $d_X : k[X] \to \Omega_X$ is a derivation

$$d_X \circ \varphi^* : k[Y] \to \Omega_X.$$

So by the universal property of the differentials we get induced a $k[Y]$-module map

$$\hat{\varphi}^* : \Omega_Y \to \Omega_X$$

such that $d_X \circ \varphi^* = \hat{\varphi}^* \circ d_Y$.

Let $x \in X$ and $y = \varphi(x)$. The $k[X]$-module k_x viewed as a $k[Y]$-module via φ^* is k_y. After identifying T_xX with $\mathrm{Hom}_{k[X]}(\Omega_X, k_x)$ and T_yY with $\mathrm{Hom}_{k[Y]}(\Omega_Y, k_y)$, the map $d\varphi_x$ becomes:

$$d\varphi_x : \mathrm{Hom}_{k[X]}(\Omega_X, k_x) \to \mathrm{Hom}_{k[Y]}(\Omega_Y, k_y),\ \theta \mapsto \theta \circ \hat{\varphi}^*.$$

Theorem 6.7.1 *Let $\varphi : X \to Y$ be a morphism of irreducible varieties.*

(i) *Assume that $x \in X$ and $y = \varphi(x) \in Y$ are simple points and that $d\varphi_x$ is surjective. Then φ is a dominant separable morphism.*

(ii) *Assume that φ is a dominant separable morphism. Then the simple points $x \in X$ with $\varphi(x)$ simple and $d\varphi_x$ surjective form a non-empty open subset of X.*

Proof (i) We may assume that X and Y are affine and Ω_X, Ω_Y are free $K[X]$-, resp. $k[Y]$-modules of rank $d = \dim X$ resp. $e = \dim Y$. In particular X and Y are smooth. The map $\hat{\varphi}^* : \Omega_Y \to \Omega_X$ of $k[Y]$-modules induces a homomorphism of free $k[X]$-modules

$$\psi : k[X] \otimes_{k[Y]} \Omega_Y \to \Omega_X.$$

We can represent ψ as a $d \times e$-matrix A with entries in $k[X]$, fixing bases for Ω_X and Ω_Y. Suppose that $d\varphi_x$ is surjective. Then $A(x)$, which represents the dual map $d\varphi_x^* : \Omega_Y(y) \to \Omega_X(x)$, is injective, hence a matrix of rank e. Hence the rank of A itself is at least e, hence equal to e since rank cannot be more than the number of columns. This shows that ψ is injective. Hence $\hat{\varphi}^*$ is injective too. Since Ω_X and Ω_Y are free modules, this implies that $\varphi^* : k[Y] \to k[X]$ must be injective. So φ must be dominant.

Moreover, injectivity of ψ implies the injectivity of

$$k(X) \otimes_{k[Y]} \Omega_Y \to k(X) \otimes_{k[X]} \Omega_X.$$

This is the map α in the exact sequence

$$k(X) \otimes_{k(Y)} \Omega_{k(Y)/k} \xrightarrow{\alpha} \Omega_{k(X)/k} \xrightarrow{\beta} \Omega_{k(X)/k(Y)} \longrightarrow 0.$$

Hence $k(X)$ is a separable extension of $k(Y)$ by the differential criterion for separability. $\square$

Example 6.7.2 I will illustarte the usefulness of the theorem by an example from my research. Recently Jon Brundan and I needed to establish the following.

Consider the polynomial algebra

$$\mathbb{C}[x_{ij}^{[r]} \mid 1 \le i, j \le n, r = 1, \ldots, l],$$

and let

$$y_{i,j}^{(r)} = \sum_{1 \le s_1 < \cdots < s_r \le l} \sum_{\substack{1 \le i_0, \cdots, i_r \le n \\ i_0 = i, i_r = j}} x_{i_0,i_1}^{[s_1]} x_{i_1,i_2}^{[s_2]} \cdots x_{i_{r-1},i_r}^{[s_r]}$$

In order to complete the proof of a theorem, we needed to show that the elements $\{y_{i,j}^{(r)}\}_{1 \le i,j \le n, r=1,\ldots,l}$ are algebraically independent.

Let us identify $\mathbb{C}[x_{ij}^{[r]}]$ with the coordinate algebra $\mathbb{C}[M_n^{\times l}]$ of the affine variety $M_n^{\times l}$ of l-tuples $(A_1, \ldots, A_l)$ of $n \times n$ matrices, so that $x_{i,j}^{[r]}$ is the function picking out the ij-entry of the rth matrix A_r. Let $\theta : M_n^{\times l} \to M_n^{\times l}$ be the morphism defined by $(A_1, \ldots, A_l) \mapsto (B_1, \ldots, B_l)$, where B_r is the rth elementary symmetric function

$$e_r(A_1, \ldots, A_l) := \sum_{1 \le s_1 < \cdots < s_r \le l} A_{s_1} \cdots A_{s_r}$$

in the matrices $A_1, \ldots, A_l$. The comorphism θ^* maps $x_{i,j}^{[r]}$ to $y_{i,j}^{(r)}$. So to show that the $y_{i,j}^{(r)}$ are algebraically independent, we need to show that θ^* is injective, i.e. that θ is a dominant morphism of affine varieties. For this it suffices to show that the differential of θ is surjective at some point $x \in M_n^{\times l}$.

Pick pairwise distinct scalars $c_1, \ldots, c_l \in \mathbb{C}$ and consider

$$x := (c_1 I_n, \ldots, c_l I_n).$$

Identifying the tangent space $T_x(M_n^{\times l})$ with the vector space $M_n^{\oplus l}$, a calculation shows that the differential $d\theta_x$ maps $(A_1, \ldots, A_l)$ to $(B_1, \ldots, B_l)$ where

$$B_r = \sum_{s=1}^{l} e_{r-1}(c_1, \ldots, \widehat{c_s}, \ldots, c_l) A_s.$$

Here $e_{r-1}(c_1, \ldots, \widehat{c_s}, \ldots, c_l)$ denotes the $(r-1)$th elementary symmetric function in the scalars $c_1, \ldots, c_l$ excluding c_s. We just need to show this linear map is surjective, for which it clearly suffices to consider the case $n = 1$. But in that case its determinant is the Vandermonde determinant $\prod_{1 \leq r < s \leq l}(c_s - c_r)$, so it is non-zero by the choice of the scalars $c_1, \ldots, c_l$.

6.8 Problems

Problem 6.8.1 Let $X \subset \mathbb{A}^n$ be a closed subset, $I = I(X)$, and J be the ideal of $k[T_1, \ldots, T_n]$ generated by all $d_x f$ for $f \in I$. If $f_1, \ldots, f_l$ generate I, then $d_x f_1, \ldots, d_x f_l$ generate J.

7
Complete Varieties

7.1 Main Properties

A variety X is called *complete* if for any variety Y the projection $\pi_2 : X \times Y \to Y$ is a closed map.

Remark 7.1.1 Completeness is an algebraic analogue of compactness. To be more precise, let X be a locally compact Hausdorff topological space. One can prove that X is compact if and only if for any locally compact space Y the projection $\pi_2 : X \times Y \to Y$ is closed.

Example 7.1.2

(i) A point is complete, as if X is a point, $\pi_2 : X \times Y \to Y$ is an isomorphism.

(ii) $\mathbb{A}^1$ is not complete. Indeed, take $Z = Z(T_1T_2 - 1) \subset \mathbb{A}^1 \times \mathbb{A}^1 = \mathbb{A}^2$. Then π_2 maps Z onto $\mathbb{A}^1 \setminus \{0\}$.

Remark 7.1.3

(i) X is complete if and only if all its irreducible components are complete.

(ii) X is complete if for any *irreducible affine* variety Y the projection $\pi_2 : X \times Y \to Y$ is closed.

Proposition 7.1.4 *Let X, Y be varieties.*

(i) *If X is complete and $Y \subset X$ is closed then Y is complete.*

(ii) *If X and Y are complete, then so is $X \times Y$.*

(iii) *If $\varphi : X \to Y$ is a morphism and X is complete, then $\varphi(X)$ is closed and complete.*

(iv) *If Y is a complete subvariety of X, then Y is closed.*

(v) *If X is complete and irreducible, then $\mathcal{O}_X(X) = k$. In particular, if X is complete and affine, then X is a finite number of points.*

Proof (i) A closed subset of $Y \times Z$ is also closed in $X \times Z$.

(ii) Projection $X \times Y \times Z$ is a composition of $\pi_Y \times \mathrm{id}_Z : X \times Y \times Z \to Y \times Z$ and $\pi_Z : Y \times Z \to Z$.

(iii) Since Y is a variety, the graph of φ is closed in $X \times Y$. Its image is $\varphi(X)$, which is closed by completeness of X. To show completeness of $\varphi(X)$, take a closed subset $K \subset \varphi(X) \times Z$ for some Z. Consider projections $\pi_2 : X \times Z \to Z$, $\pi_2' : \varphi(X) \times Z \to Z$, and note that $\pi_2'(K) = \pi_2((\varphi \times \mathrm{id}_Z)^{-1}(K))$.

(iv) Apply (iii) to the embedding of Y into X.

(v) Let $f \in \mathcal{O}_X(X)$. Then f is a morphism from X to $\mathbb{A}^1$, cf. Problem 4.6.2. By (iii), $f(X)$ is closed complete irreducible subvariety of $\mathbb{A}^1$, and it could not be $\mathbb{A}^1$ itself, since $\mathbb{A}^1$ is not complete, so $f(X)$ is a point, i.e. f is a constant. $\square$

7.2 Completeness of projective varieties

Theorem 7.2.1 *Any projective variety is complete.*

Proof In view of Proposition 7.1.4(i) and Remark 7.1.3(ii), it suffices to prove that $\pi_2 : \mathbb{P}^n \times Y \to Y$ is closed for any irreducible affine variety Y. Set $R := k[Y]$.

For $0 \le i \le n$, let $\mathbb{P}^n_i$ be the affine open set of $\mathbb{P}^n$ given by $X_i \ne 0$, where $X_0, X_1, \dots, X_n$ are the coordinate 'functions' on $\mathbb{P}^n$. Then the affine open sets $U_i := \mathbb{P}^n_i \times Y$ cover $\mathbb{P}^n \times Y$. Moreover, we can identify $k[U_i]$ with $R_i := k[X_0/X_i, \dots, X_n/X_i] \otimes R = R[X_0/X_i, \dots, X_n/X_i]$.

Let Z be any cosed set in $\mathbb{P}^n \times Y$, and $y \in Y \setminus \pi_2(Z)$. We want to find a neighborhood of y in Y of the form Y_f which is disjoint from $\pi_2(Z)$. This amounts to finding $f \in R$ with $f \notin M := M_y$ and such that f vanishes on $\pi_2(Z)$. Let $\pi_2^i := \pi_2|U_i$ and $Z_i := Z \cap U_i$, $0 \le i \le n$. Now $f|\pi_2(Z) \equiv 0$ is equivalent to the statement that the pullback of $(\pi_2^i)^*(f)$ is zero on $Z_i \iff (\pi_2^i)^*(f) \in I(Z_i) \lhd R_i$. The existence of such f will follow from Nakayama's Lemma applied to a suitable R-module, which we now construct.

First consider the polynomial ring $S := R[X_0, \dots, X_n]$ with natural grading $S = \oplus_m S_m$. We construct the homogeneous ideal $I \lhd S$ by letting

I_m consist of all $f(X_0, \ldots, X_n) \in S_m$ such that $f(X_0/X_i, \ldots, X_n/X_i) \in I(Z_i)$ for each i.

Next, fix i and let $f \in I(Z_i)$. We claim that the multiplication of f by a sufficiently high power of X_i will take f into I. Indeed, for large m, $X_i^m f$ becomes a homogeneous polynomial of degree m. Moreover, $(X_i^m/X_j^m)f \in R_j$ vanishes on $Z_i \cap U_j = Z_j \cap U_i$, while $(X_i^{m+1}/X_j^{m+1})f$ vanishes at all points of Z_j not in U_i. So $(X_i^{m+1}/X_j^{m+1})f$ vanishes on Z_j. Since j is arbitrary, we conclude that $X_i^{m+1}f$ lies in I_{m+1}.

Now, Z_i and $\mathbb{P}_i^n \times \{y\}$ are disjoint closed subsets of the affine variety U_i, so their ideals $I(Z_i)$ and MR_i generate R_i, i.e. we can write $1 = f_i + \sum_j m_{ij}g_{ij}$, where $f_i \in I(Z_i)$, $m_{ij} \in M$, and $g_{ij} \in R_i$. By the preceding paragraph, multiplication by a sufficiently high power of X_i takes f_i into I. We can choose this power large enough to work in these equations for all f_i and to take g_{ij} into S as well. So we obtain $X_i^m \in I_m + MS_m$ for all i. Enlarging m even more, we can get all monomials of degree m in $X_0, \ldots, X_n$ to lie in $I_m + MS_m$. This implies $S_m = I_m + MS_m$.

Now apply Corollary 2.1.9 to the finitely generated R-module S_m/I_m, which satisfies $M(S_m/I_m) = S_m/I_m$. The conclusion is that there exists $f \in R \setminus M$ such that f annihilates S_m/I_m, i.e. $fS_m \subset I_m$. In particular, $fX_i^m \in I_m$, so by definition of I_m we have $(fX_i^m)(X_0/X_i, \ldots, X_n/X_i) \in I(Z_i)$, but $(fX_i^m)(X_0/X_i, \ldots, X_n/X_i) \in I(Z_i) = f$. $\square$

Part two

Algebraic Groups

8
Basic Concepts

8.1 Definition and first examples

Definition 8.1.1 An *algebraic group* is an affine variety G equipped with morphisms of varieties $\mu : G \times G \to G$, $\iota : G \to G$ that give G the structure of a group. A *morphism* $f : G \to H$ of algebraic groups is a morphism of varieties that is a group homomorphism too.

It is possible to consider algebraic groups which are not necessarily affine varieties, so strictly speaking one we should have used the term *affine algebraic group* above. As we will only meet affine algebraic groups we will drop the word 'affine'.

The kernel of a morphism $f : G \to H$ of algebraic groups is a closed subgroup of G, so it is an algebraic group in its own right. The same will turn out to be true about the images.

Translation by an element $g \in G$ is an isomorphism of varieties, so all geometric properties at one point can be transferred to any other point. For example, as G has simple points, G is smooth.

Example 8.1.2 (i) The *additive group* $\mathbb{G}_a$ is the group $(k, +)$, i.e. the affine variety $\mathbb{A}^1$ under addition.

(ii) The *multiplicative group* $\mathbb{G}_m$ is the group $(k^\times, \times)$, i.e. the principal open subset $\mathbb{A}^1 \setminus \{0\}$ under multiplication.

(iii) The group $GL_n = GL_n(k)$ is the group of all invertible $n \times n$ matrices over k. As a variety, this is a principal open set in $M_n(k) = \mathbb{A}^{n^2}$ corresponding to the determinant. Since the formulas for matrix multiplication and inversion involve only polynomials in the matrix entries and $1/\det$, the group structure maps are morphisms of varieties.

Let V be an n-dimensional vector space over k. Then by fixing a basis we can define a structure of an algebraic group on $GL(V)$ which is independent of the choice of basis. Of course, $GL(V) \cong GL_n$.

(iv) The group $SL_n = SL_n(k)$ is the closed subgroup of GL_n defined by the zeros of $\det -1$.

(v) The group D_n of invertible diagonal matrices is a closed subgroup of GL_n (given be the zeros of which functions?) It is isomorphic to the direct product $\mathbb{G}_m \times \cdots \times \mathbb{G}_m$ (m copies).

(vi) The group U_n of upper unitriangular matrices is another closed subgroup of GL_n.

(vii) The *orthogonal* group $O_n = \{x \in GL_n \mid xx^t = 1\}$. We exclude the characteristic 2 when considering this example...

(viii) The *special orthogonal* group $SO_n = O_n \cap SL_n$ is a normal subgroup of O_n of index 2.

(ix) The symplectic group $Sp_{2n} = \{x \in GL_n \mid x^t J x = J\}$ where

$$\begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$$

is another closed subgroup.

Let G be an (affine) algebraic group with the identity element e, and put $A = k[G]$. The map

$$\varepsilon : A \to k,\ f \mapsto f(e)$$

is an algebra homomorphism (called *augmentation*). Consider also the dual morphisms

$$\Delta := \mu^* : A \to A \otimes A$$

(called *comultiplication*) and

$$\sigma := \iota^* : A \to A$$

(called *antipode*). In follows using group axioms that these define the structure of a *Hopf algebra* on $k[G]$. Conversely, a structure of the Hopf algebra on $k[G]$ defines a structure of an algebraic group on G. An easy corollary of Theorem 3.5.1 now is that the categories of (affine) algebraic groups and affine Hopf algebras are contravariantly equivalent.

Example 8.1.3 (i) $k[\mathbb{G}_a] = k[T]$ with $\varepsilon(T) = 0$, $\sigma(T) = -T$, and $\Delta(T) = T \otimes 1 + 1 \otimes T$.

(ii) $k[\mathbb{G}_m] = k[T, T^{-1}]$ with $\varepsilon(T) = 1$, $\sigma(T) = T^{-1}$, and $\Delta(T) = T \otimes T$.

(iii) $k[GL_n] = k[T_{i,j} \mid 1 \leq i,j \leq n]_{\det}$ with $\varepsilon(T_{ij}) = \delta_{ij}$, $\sigma(T_{ij}) = (-1)^{i+j} M_{j,i}/\det$ (where $M_{j,i}$ is the determinant of the (j,i)minor), and $\Delta(T_{i,j}) = \sum_{k=1}^{n} T_{ik} \otimes T_{kj}$.

A *rational representation* of G in a finite dimensional k-vector space V is a homomorphism of algebraic groups $\rho : G \to GL(V)$. The notion of a rational representation is equivalent to that of a rational G-module: V is called a *rational G-module* if it is a G-module in the usual sense and the corresponding representation is rational. From the point of view of Hopf algebras the notion of a G-module is equivalent to the notion of a comodule over the Hopf algebra $k[G]$ (read about this notion somewhere or better yet invent it yourself!)

8.2 First properties

Let G be an algebraic group. We note that only one irreducible component of G can pass through the identity element e. Indeed, if $X_1, \dots, X_m$ are the distinct irreducible components of G containing e. The image of the irreducible variety $X_1 \times \cdots \times X_m$ under the product morphism is an irreducible subset $X_1 \dots X_m$ of G, which again contains e. So $X_1 \dots X_m$ lies in some X_i. On the other hand each of the components $X_1, \dots, X_m$ clearly lies in $X_1 \dots X_m$. This forces $m = 1$. Denote by G° this unique irreducible component of G containing e, and call it the *identity component* of G.

Proposition 8.2.1 *Let G be an algebraic group.*

(i) *G° is a normal subgroup of finite index in G, whose cosets are the connected as well as irreducible components of G.*
(ii) *Each closed subgroup of finite index in G contain G°.*

Proof (i) We have $\iota(G^\circ)$ is an irreducible component of G containing e, so $\iota(G^\circ) = G^\circ$. It also follows from the argument preceding the theorem that $G^\circ G^\circ = G^\circ$, so G° is a (closed) subgroup of G.

For any $x \in G$, $xG^\circ x^{-1}$ is also an irreducible component of G containing e, so $xG^\circ x^{-1} = G^\circ$, i.e. G° is normal. Its cosets are translates of G°, hence must also be irreducible components of G. As there are only finitely many irreducible components, it follows that $[G : G^\circ] < \infty$. Since the cosets are disjoint, they are also connected components of G.

(ii) If H is a closed subgroup of a finite index in G, then H° is a closed subgroup of finite index in G°, and each of its finitely many left cosets in G° is also closed, and so the union of the cosets distinct from H° is closed. Hence H° is also open in G°. Since G° is irreducible it is connected, whence $H^\circ = G^\circ$. □

The algebraic group is called *connected* if $G^\circ = G$.

Lemma 8.2.2 *Let U and V be dense open subsets of G. Then $G = UV$.*

Proof Let $x \in G$. Then xV^{-1} and U are dense open subsets. So they have to meet, forcing $x \in UV$. □

Lemma 8.2.3 *Let $H < G$ be a subgroup of an algebraic group G. Then:*

(i) *$\bar{H}$ is a subgroup of G.*
(ii) *If H is constructible, then $H = \bar{H}$.*
(iii) *If H contains a dense open subset of $\bar{H}$, then $H = \bar{H}$.*

Proof (i) As ι is a homeomorphism, we have $\iota(\bar{H}) = \overline{\iota(H)} = \bar{H}$. Similarly, translation by x is a homeomorphism, so $\overline{xH} = x\bar{H}$, i.e. $H\bar{H} \subset \bar{H}$. Therefore, if $x \in \bar{H}$, we have $Hx \subset \bar{H}$, so $\bar{H}x = \overline{Hx} \subset \bar{H}$.

(ii),(iii) If H is constructible, it contains a dense open subset U of $\bar{H}$, see Problem 5.5.3. Then H is also open in $\bar{H}$, as H is a union of translates of U. By Lemma 8.2.2, $\bar{H} = HH = H$. □

Corollary 8.2.4 *Let A, B be closed subgroups of G. If B normalizes A, then AB is a closed subgroup of G.*

Proof It is clear that AB is a subgroup. Moreover, it the image of $A \times B$ under the product morphism, hence constructible by Theorem 5.3.3, hence closed by the lemma. □

Lemma 8.2.5 *Let $\varphi : G \to H$ be a morphism of algebraic groups. Then:*

(i) $\ker \varphi$ *is a closed subgroup of G.*
(ii) $\operatorname{im} \varphi$ *is a closed subgroup of H.*
(iii) $\varphi(G^\circ) = \varphi(G)^\circ$.
(iv) $\dim G = \dim \ker \varphi + \dim \operatorname{im} \varphi$.

Proof (i) follows from the continuity of φ and (ii) follows from Theorem 5.3.3 and Lemma 8.2.3(ii). Now, $\varphi(G^\circ)$ is closed by (ii) and irreducible, hence lies in $\varphi(G)^\circ$. Being of finite index in $\varphi(G)$, it must equal $\varphi(G)^\circ$, thanks to Proposition 8.2.1(ii). Finally, Theorem 5.3.1(ii) implies that $\dim G - \dim \varphi(G) = \dim \varphi^{-1}(x)$ for 'most' points $x \in \varphi(G)$. But all fibers $\varphi^{-1}(x)$ are isomorphic to $\ker \varphi$, so we have (iv). □

Proposition 8.2.6 *Let $(X_i, \varphi_i)_{i\in I}$ be a family of irreducible varieties and morphisms $\varphi_i : X_i \to G$ such that $e \in Y_i := \varphi_i(X_i)$ for all i. Let H be the smallest subgroup of G containing all Y_i. Then:*

(i) *H is closed and connected.*
(ii) *$H = Y_{a_1}^{\varepsilon_1} \dots Y_{a_n}^{\varepsilon_n}$ for some $a_1, \dots, a_n \in I$ and $\varepsilon_1, \dots, \varepsilon_n \in \{\pm 1\}$.*

Proof We may assume that the sets Y_i^{-1} occur among the Y_j. Note that for each $\underline{a} := (a_1, \dots, a_n) \in I^n$, $Y_{\underline{a}} := Y_{a_1} \dots Y_{a_n}$ is irreducible, hence $\bar{Y}_{\underline{a}}$ is irreducible, too. Obviously $Y_{\underline{a}} Y_{\underline{b}} = Y_{(\underline{a},\underline{b})}$.

Moreover, $\bar{Y}_{\underline{a}} \bar{Y}_{\underline{b}} \subset \overline{Y_{(\underline{a},\underline{b})}}$. Indeed, for $x \in Y_{\underline{b}}$, the homeomorphism (of G) $y \mapsto yx$ sends $Y_{\underline{b}}$ to $Y_{(\underline{a},\underline{b})}$, hence $\bar{Y}_{\underline{b}}$ into $\overline{Y_{(\underline{a},\underline{b})}}$, i.e $\bar{Y}_{\underline{a}} Y_{\underline{b}} \subset \overline{Y_{(\underline{a},\underline{b})}}$. Now $x \in \bar{Y}_{\underline{a}}$ sends $Y_{\underline{b}}$ into $\overline{Y_{(\underline{a},\underline{b})}}$, hence $\bar{Y}_{\underline{b}}$ as well.

Now choose the tuple $\underline{a}$ such that $\dim Y_{\underline{a}}$ is maximal. As $e \in Y_{\underline{a}}$, we have for any $\underline{b}$ that $\bar{Y}_{\underline{a}} \subset \bar{Y}_{\underline{a}} \bar{Y}_{\underline{b}} \subset \overline{Y_{(\underline{a},\underline{b})}}$. Equality holds by dimensions, so $\bar{Y}_{\underline{b}} \subset \bar{Y}_{\underline{a}}$ for every $\underline{b}$, and $\bar{Y}_{\underline{a}}$ is closed under multiplication. Choosing $\underline{b}$ such that $Y_{\underline{b}} = Y_{\underline{a}}^{-1}$, we also have $\bar{Y}_{\underline{a}}$ stable under inversion. So $\bar{Y}_{\underline{a}}$ is a group. Since Y_a is constructible, it contains a dense open subset of $\bar{Y}_{\underline{a}}$, whence $\bar{Y}_{\underline{a}} = Y_{\underline{a}} Y_{\underline{a}}$ in view of Lemma 8.2.2.

Finally, we claim that $H = \bar{Y}_{\underline{a}}$. It is clear that H is contained in $\bar{Y}_{\underline{a}}$, as we know that each $Y_{\underline{b}} \subset \bar{Y}_{\underline{a}}$. Since $H \supset Y_{\underline{a}}$, we have $\bar{H} = \bar{Y}_{\underline{a}}$. Finally, $H \supset Y_{\underline{a}}$ also implies that H contains a dense open subset of $\bar{H}$, so H is closed by Lemma 8.2.3(iii). □

Corollary 8.2.7 *Assume that $(G_i)_{i\in I}$ is a family of closed connected subgroups of G. Then the group H generated by them is closed and connected. Furthermore, $H = G_{a_1} \dots G_{a_n}$ for some $a_1, \dots, a_n \in I$.*

Example 8.2.8 It is easy to see that the groups $\mathbb{G}_m, \mathbb{G}_a, GL_n$ are connected. It is less obvious that SL_n, Sp_{2n}, and SO_n are connected. This can be deduced using Corollary 8.2.7 and some group theory. For example the group SL_n is known to be generated by transvections. It follows that the subgroups $G_{ij} = \{E + tE_{ij} \mid t \in k\}$ generate SL_n. This *transvection subgroups* are closed and isomorphic to $\mathbb{G}_a$, hence connected. For Sp_{2n}, let V be the $2n$-dimensional vector space on which Sp_{2n} acts, and $(\cdot, \cdot)$ be the non-degenerate symplectic bilinear form preserved by the group. For $v \in V \setminus \{0\}$ define the *symplectic transvection group* G_v to consist of all linear transformations of the form

$w \mapsto w + t(w, v)v$ $(t \in k)$. It remains to use the known fact that the G_v generate Sp_{2n}. A similar proof is available for SO_n.

As SO_n is of index 2 in O_n, it follows that it is the identity component of O_n.

Corollary 8.2.9 *Let H and K be closed subgroups of G with H conncted. Then the commutator group (H, K) generated by all commutators $[h, k]$ with $h \in H, k \in K$, is closed and connected.*

Proof Take the index set I in the proposition to be K and the maps $\varphi_k : H \to G$ to be the maps $h \mapsto hkh^{-1}k^{-1}$ $(k \in K)$. □

Example 8.2.10 Recall the definition of the derived series

$$G = G^{(0)} \geq G^{(1)} \geq \dots$$

of a group G: $G^{(0)} = G, G^{(i+1)} = (G^{(i)}, G^{(i)})$. The group G is the called *solvable* if $G^{(i)} = \{e\}$ for some i. In case G is a connected algebraic group, each of the derived subgroups are closed connected subgroup of G. So either $G^{(i+1)} = G^{(i)}$ or $\dim G^{(i+1)} < \dim G^{(i)}$. Thus we see that for algebraic groups the derived series stabilizes after finitely many steps. Similar remarks apply to nilpotent algebraic groups.

8.3 Actions of Algebraic Groups

Let G be an algebraic group and X be a variety (not necessarily affine). We say that G *acts* on X, or that X is a G-*variety*, if we are given a morphism

$$G \times X \to X, (g, x) \mapsto gx$$

of varieties that makes X into a G-set in the usual sense. If the G-action on X is transitive, X is called a *homogeneous space.*

Lemma 8.3.1 *Let G act on X. Let Y, Z be subsets of X with Z closed.*

(i) *The set $\{g \in G \mid gY \subset Z\}$ is closed; in particular $N_G(Z) := \{g \in G \mid gZ \subset Z\}$ is closed.*
(ii) *For each $x \in X$ the stabilizer G_x is a closed subgroup of G; in particular, $C_G(Y) := \{g \in G \mid gy = y \text{ for any } y \in Y\}$ is closed.*
(iii) *The fixed point set X^g of $g \in G$ is closed in X; in particular X^G is closed.*

Proof (i) For each $y \in X$ the orbit map $f_y : G \to X, g \mapsto gy$ is a morphism. So $f_y^{-1}(Z)$ is closed in G. Now note that

$$\{g \in G \mid gY \subset Z\} = \cap_{y \in Y} f_y^{-1}(Z).$$

(ii) Observe that $G_x = \{g \in G \mid g\{x\} \subset \{x\}\}$ and apply (i).

(iii) Consider the morphism $\psi : X \to X \times X,\ x \mapsto (x, gx)$. Then X^g is the inverse image under ψ of the diagonal, which is closed, since X is a variety. □

Remark 8.3.2 The lemma shows that things like centralizers of subsets, normalizers of closed subsets, fixed point sets , etc. are closed. However *orbits themselves are not closed in general.* In fact the structure of orbits of an algebraic group on a variety can be very interesting. Also, *connectedness* of centralizers and normalizers is not to be taken for granted.

Theorem 8.3.3 *Let G act on X. Then each orbit is smooth, locally closed subset subset of X, whose boundary $\overline{Gx} - Gx$ is a union of orbits of strictly smaller dimension. In particular, orbits of minimal dimension are closed (so closed orbits exist). If G is connected, the orbits are irreducible.*

Proof Let $\mathcal{O} = Gx$. As the image of G under the orbit map, $\mathcal{O}$ is constructible, hence contains an open dense subset U of $\bar{\mathcal{O}}$. (Also, $\mathcal{O}$ is irreducible if G is connected.) But G acts transitively on $\mathcal{O}$ (leaving $\bar{\mathcal{O}}$ stable), so $\mathcal{O} = \cup_{g \in G} gU$ is open in $\bar{\mathcal{O}}$, and $\mathcal{O}$ is smooth. Therefore $\bar{\mathcal{O}} - \mathcal{O}$ is closed and of strictly lower dimension than $\dim \bar{\mathcal{O}} = \dim \mathcal{O}$. Being G-stable, this boundary is the union of other G-orbits. □

Example 8.3.4 Let $G = GL_n = GL(V)$ where $V = k^n$ (viewed as an affine n-space). There are just two orbits of G on V: the ponit $\{0\}$ and the rest $V - \{0\}$, an open orbit of dimension n. What can you say about stabilizers in this action? More generally, if V is a rational G-module over an arbitrary algebraic group G, then $v \mapsto gv$ defines a structure of G-variety on $V \cong \mathbb{A}^{\dim V}$.

Example 8.3.5 Again take $G = GL_n = GL(V)$ and define the G-action on $\mathbb{P}(V)$ via $g\langle v\rangle = \langle gv\rangle$ (here $\langle v\rangle$ denote the line spanned by a non-zero vector $v \in V$). In other words this is just the natural action of GL_n on the lines of V, which is transitive by linear algebra. What can you say about stabilizers in this action?

In order to check that this is an action in the sense of algebraic groups, we need to check that the corresponding map $\rho : G \times \mathbb{P}(V) \to \mathbb{P}(V)$ is a morphism of varieties. For this we employ the Affine Criterion (Theorem 4.2.4) with the usual affine open subsets V_i of $\mathbb{P}(V)$ $(0 \leq i \leq n)$, and $U_i = \varphi^{-1}(V_i)$ (Here $\varphi : G \times \mathbb{P}^n \to \mathbb{P}^n$ is the action map.)

Let $V' = V - \{0\}$ be the non-trivial G-orbit from Example 8.3.4. it is easy to check using Affine Criterion that the map $V' \to \mathbb{P}(V), v \mapsto \langle v \rangle$ is a G-equivariant morphism of varieties.

Example 8.3.6 The natural actions of $G = GL_n = GL(V)$ on the Grassmann variety $G_d(V)$ and the flag variety $\mathcal{F}$ are transitive by linear algebra. These actions are morphic as they are just restrictions of the action of G on $\mathbb{P}(\Lambda^d(V))$ and $\mathbb{P}(\Lambda^1(V)) \times \cdots \times \mathbb{P}(\Lambda^{n-1}(V)) \times \mathbb{P}(\Lambda^n(V))$, respectively. What can you say about stabilizers in this actions?

Lemma 8.3.7 *Let G be a connected algebraic group and X, Y be homogeneous spaces over G. Suppose $\varphi : X \to Y$ is a G-equivariant morphism. Set $r = \dim X - \dim Y$. Then:*

(i) *φ is surjective and open.*

(ii) *for each closed irreducible subset $W \subset Y$ all irreducible components of $\varphi^{-1}(W)$ have dimension $r + \dim W$.*

Proof Surjectivity is clear. Now, it follows from (ii) and Theorem 5.4.1 that φ is open. It remains to prove (ii). By Theorem 5.3.1, there is an open set $U \subset Y$ such that for each irreducible closed subset $W \subset Y$ meeting U, the components of $\varphi^{-1}(W)$ meeting $\varphi^{-1}(U)$ have dimensions $\dim W + r$. Since G acts transitively on Y and X, the G-translates of U cover Y and the G-translates of $\varphi^{-1}(U)$ cover X. This implies (ii). $\square$

8.4 Linear Algebraic Groups

A *linear algeraic group* is a closed subgroup of some GL_n. The following theorem can be thought of as the analogue of the famous theorem that any finite group is a subgroup of some symmetric group S_n.

Theorem 8.4.1 *Every (affine) algebraic group is linear.*

To prove the theorem we need to find a finite dimensional vector space on which G acts, and the only place we can look for it is inside the regular module $k[G]$. Given $g \in G$, the map $G \to G, h \mapsto hg$ is a morphism of varieties, whose dual map is $\rho_g : k[G] \to k[G]$, where

$$\rho_g(f)(h) = f(hg) \qquad (f \in k[G],\ h \in G).$$

This defines a representation ρ of G in the (usually infinite dimensional space) $k[G]$, called *(right) regular representation* or representation by *right translations* of functions. The *left regular representation* λ is defined similarly via

$$\lambda_g(f)(h) = f(g^{-1}h) \qquad (f \in k[G],\ h \in G).$$

The antipode map is actually an isomorphism of the left and right regular representations, so we will usually refer to it as the regular representation and use the right one if we need to write some formulas. The following lemma will help us to deal with the problem of infinite dimensionality of $k[G]$.

Lemma 8.4.2 *The regular representation is locally finite dimensional, i.e. every element of* $k[G]$ *is contained in a finite dimensional submodule.*

Proof Let us take a non-zero $f \in k[G]$. Let W be the subspace of $k[G]$ spanned by all right translations $\rho_g f$. We need to show that W is finite dimensional. Write $\Delta f = \sum_{i=1}^n f_i \otimes g_i$. Let X be the finite dimensional ubspace of $k[G]$ spanned by all f_i. Now consider $x \in G$. We have

$$(\rho_x f)(h) = f(hx) = (\Delta f)(h, x) = \sum_{i=1}^n f_i(h) g_i(x).$$

Hence $\rho_x f = \sum_{i=1}^n g_i(x) f_i \in X$. Hence $W \subset X$ and W is finite dimensional. $\square$

Proof of the theorem Choose linearly independent generators $f_1, \dots, f_n$ of the algebra $k[G]$. Applying the lemma, we may assume (adding finitely many more generators if necessary) that the span E of the f_i is invariant under all right translations. Now consider the restriction

$$\psi : G \to GL(E),\ x \mapsto \rho_x | E$$

of ρ.

Fix i and write $\Delta f_i = \sum_j g_j \otimes h_j$ with g_j linearly independent and $h_j \neq 0$. As in the proof of the lemma, $\rho_x f_i = \sum h_j(x) g_j$ for all $x \in G$, which implies $g_j \in E$, so we can write

$$\Delta f_i = \sum_j f_j \otimes h_{ij} \qquad (1 \leq i \leq n). \tag{8.1}$$

Then the coordinates of the matrix of $\psi(x)$ with respect to the basis $f_1, \dots, f_n$ are $h_{ij}(x)$. Hence ψ is a morphism of varieties.

Next notice that $f_i(x) = f_i(ex) = \sum_j f_j(e)h_{i,j}(x)$, so

$$f_i = \sum_j f_j(e)h_{i,j}. \tag{8.2}$$

If $\psi(x) = e$, then $h_{i,j}(x) = \delta_{i,j}$, so $f_i(x) = f_i(e)$ for all i, whence $x = e$, as f_i's generate $k[G]$.

By Lemma 8.2.5(ii), $G' := \operatorname{im}\psi$ is a closed subgroup of $GL(E)$. To complete the proof, we need only to show that $\psi : G \to G'$ is an isomorphism of varieties, i.e. $\psi^* : k[G'] \to k[G]$ is an isomorphism of algebras. As ψ is surjective, ψ^* is injective. On the other hand, let t_{ij} be coordinate functions on $GL(E)$ restricted to G'. Note that $\psi^*(t_{ij}) = h_{ij}$, and the h_{ij} generate $k[G]$ in view of (8.2), so ψ^* is surjective.

8.5 Problems

Problem 8.5.1 Let A be a finite dimensional k-algebra. Show that $\mathrm{Aut}(A)$ is a closed subgroup of $GL(A)$.

Solution. $\mathrm{Aut}(A)$ is the stabilizer of an element $t \in A^* \otimes A^* \otimes A$, see the proof of Corollary 9.5.2.

Problem 8.5.2 Describe $\mathrm{Aut}(\mathbb{G}_m)$, $\mathrm{Aut}(\mathbb{G}_a)$, and $\mathrm{End}\,(\mathbb{G}_m, \mathbb{G}_m)$.

Solution. Working with $k[G]$, we get $\mathrm{Aut}(\mathbb{G}_m) \cong \mathbb{Z}_2$, where the only nontrivial automorphism is $z \mapsto z^{-1}$. Moreover, $\mathrm{End}\,(\mathbb{G}_m) \cong \mathbb{Z}$ with $m \in \mathbb{Z}$ corresponding to the endomorphism $z \mapsto z^m$. Finally, $\mathrm{Aut}(\mathbb{G}_a) \cong k^\times$, with $a \in k^\times$ corresponding to the endomorphism $z \mapsto az$.

Problem 8.5.3 Closed subset of G containing e and closed under multiplication is a subgroup of G.

Solution. Let X be the subset and $x \in X$. Consider the morphism $\varphi : X \to X, y \mapsto yx$. It suffices to show that this morphism is surjective, as then e is in the image, and the result follows.

In order to prove that φ is surjective, let Z be an irreducible component of X of maximal dimension. Then $\varphi(X)$ is irreducible of the same dimension, as φ is the restriction to X of an autmorphism of G. So $\varphi(Z)$ must be an irreducible component of X. This proves that φ permutes irreducible components of X. As X is one-to-one, this argument can now be applied again to the irreducible components of the next largest dimension, etc.

Problem 8.5.4 Let $N < GL_n$ be the group of *monomial* matrices, i.e. matrices having precisely one non-zero entry in each column and each entry. Prove that N° is the subgroup of all diagonal matrices in GL_n.

Solution. Humphreys, problem 7 after section 7. The group D of diagonal matrices is connected, and $[N : D]$ is finite.

Problem 8.5.5 Show that the subgroup of $GL_2(\mathbb{C})$ geberated by $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ is not closed.

Solution. Let $X \cong \mathbb{A}^1 \subset GL_2(\mathbb{C})$ be the closed subset which consists of all upper unitrangular matrices. Note that our subgroup intersects X at the subset of all upper-unitrangular matrices with integer entries in the corner. This is not closed, as $\mathbb{Z} \subset \mathbb{A}^1$ is not closed.

Problem 8.5.6 Let G be a connected algebraic group. Prove that any finite normal subgroup H lies in the center of G.

Solution. If $h \in H$, then the image of the morphism $G \to G, x \mapsto xhx^{-1}$ is connected and contained in H, so the image is trivial.

Problem 8.5.7 True or false? Let $\varphi : G \to H$ be a morphism of algebraic groups which is an isomorphism of abstract groups. Then φ is an isomorphism of algebraic groups.

Solution. False: consider $\mathrm{Fr} : \mathbb{G}_m \to \mathbb{G}_m$ or Problem 8.5.8(iii).

Problem 8.5.8 We have $A := k[SL_2] = k[T_{11}, T_{12}, T_{21}, T_{22}]/(T_{11}T_{22} - T_{12}T_{21} - 1) = k[t_{11}, t_{12}, t_{21}, t_{22}]$ (t_{ij} denoting the image of T_{ij}). Let B be the subalgebra of A generated by all products $t_{ij}t_{kl}$.

(i) Show that B be is a Hopf subalgebra of A and deduce that that there is an algebraic group PSL_2 whose algebra is B. Show that the inclusion map $B \to A$ defines a surjective homomorphism of algebraic groups $SL_2 \to PSL_2$ with kernel of order at most 2.

(ii) If $\operatorname{char} k \neq 2$, then B is the algebra of functions $f \in A$ such that $f(-X) = f(X)$ for all $X \in SL_2$.

(iii) If $\operatorname{char} k = 2$, then the homomorphism of (i) defines an isomorphism of underlying abstract groups but is not an isomorphism of algebraic groups.

Solution. (i) That B is a Hopf subalgebra is easily checked using explicit formulas for coproduct and antipode. Also B is a reduced finitely generated k-algebra, so it corresponds to an algebraic group by general principles. Also, the inclusion map $\iota : B \to A$, being a Hopf algebra map, defines a surjective homomorphism $\iota_* : SL_2 \to PSL_2$.

Now B is generated by the elements

$$t_{11}^2, t_{11}t_{12}, t_{11}t_{21}, t_{11}t_{22}, t_{12}^2, t_{12}t_{22}, t_{21}^2, t_{21}t_{22}, t_{22}^2,$$

as $t_{11}t_{22} = t_{12}t_{21} + 1$. Now, using the counit, we see that the identity e in PSL_2 is defined by equations $t_{11}^2(e) = 1, t_{22}^2(e) = 1, t_{11}t_{22}(e) = 1$ and $t_{ij}t_{kl}(e) = 0$ for all other generators. So $A = (a_{ij})$ maps to e under ι_* if and only if $a_{11}^2 = 1, a_{22}^2 = 1, a_{11}a_{22} = 1$ and $a_{ij}a_{kl} = 0$ for all other pairs of indices corresponding to the generators. It follows that the kernel of ι_* is $\pm I$.

(ii) Direct check.

(iii) If $\operatorname{char} k = 2$, ι_* is bijective. Of course it is not an isomorphism since ι is not surjective.

Problem 8.5.9 Let X be a G-variety and $a : G \times X \to X$ is the action map. Define the left action of G on $k[X]$ via

$$(gf)(x) = f(g^{-1}x) \qquad (g \in G,\ x \in X,\ f \in k[X]).$$

Note that this yields a representation of abstract group G in $k[X]$.

(i) The representation is locally finite dimensional.

(ii) A finite dimensional subspace $V \subset k[X]$ is G-stable if and only if $a^*(V) \subset k[G] \otimes V$. If so, the action of G on V defines a rational representation of G.

(iii) There is a sequence of finite dimensional G-submodules $V_i \subset k[G]$ such that $V_1 \subset V_2 \subset \dots$ and $k[X] = \cup_i V_i$.

Solution. Take $f \in k[X]$. If $a^* : k[X] \to k[G] \otimes k[X]$ maps f to $\sum_i h_i \otimes f_i$, then $gf = \sum_i h_i(g^{-1})f_i$, which implies (i) and (ii). Now (ii) is a general fact on countably dimensional locally finite modules.

9

Lie algebra of an algebraic group

9.1 Definitions

Let G be an algebraic group and $A = k[G]$. We will consider the Lie algebra $\mathrm{Der}(A)$ of k-derivations $A \to A$ with respect to the bracket $[\delta_1, \delta_2] = \delta_1 \circ \delta_2 - \delta_2 \circ \delta_1$. A derivation $\delta \in \mathrm{Der}(A)$ is called *left-invariant* if it commutes with left translations, i.e. $\delta \circ \lambda_x = \lambda_x \circ \delta$ for all $x \in G$. The left invariant derivations of A form a Lie subalgebra of $\mathrm{Der}(A)$, called the *Lie algebra of* G and denoted $L(G)$. (Using right invariant derivations here would lead to an isomorphic object).

Let us denote by $\mathfrak{g}$ the tangent space T_eG. We claim that $\mathfrak{g}$ can be naturally identified with $L(G)$ as vector spaces. Recall that T_eG can be defined as the the derivations of A at e. Define a k-linear map $\theta : L(G) \to \mathfrak{g}$ by

$$(\theta\delta)(f) = (\delta f)(e) \qquad (\delta \in L(G),\ f \in A).$$

We claim that θ is an isomorphism of vector spaces. In order to prove this we construct the inverse map $\eta : \mathfrak{g} \to L(g)$ sending a tangent vector X to a derivation $*X$ called *right convolution by* X and defined by

$$(f * X)(x) = X(\lambda_{x^{-1}} f) \qquad (x \in G,\ f \in A).$$

It is a straightforward check that $*X$ is indeed a left invariant derivation of A and that η is k-linear. Finally, η is inverse to θ:

$$\begin{aligned} (f * \theta(\delta))(x) &= \theta(\delta)(\lambda_{x^{-1}} f) = \delta(\lambda_{x^{-1}} f)(e) = \lambda_{x^{-1}}(\delta f)(e) = (\delta f)(x), \\ \theta(*X)(f) &= (f * X)(e) = X(\lambda_{e^{-1}} f) = X(f) \end{aligned}$$

(for $X \in \mathfrak{g}, \delta \in L(G), f \in A, x \in G$).

From now on we are going to identify $L(G)$ with $\mathfrak{g}$ via the isomorphisms θ and η. For example, $\mathfrak{g}$ is a Lie algebra with respect to the bracket defined as follows:

$$[X,Y](f) = ((f * Y) * X - (f * X) * Y)(e) = X(f * Y) - Y(f * X).$$

We give another definition of $[X,Y]$ in terms of the coproduct Δ. Define

$$X \cdot Y : A \to k, \ f \mapsto (X \otimes Y) \circ \Delta(f).$$

If $\Delta(f) = \sum_i f_i \otimes f_i'$, then

$$f * X = \sum_i f_i X(f_i'),$$

whence it is easy to see that $(X \cdot Y)(f) = ((f * Y) * X))(e)$. So

$$[X,Y] = X \cdot Y - Y \cdot X.$$

This definition of the bracket makes the following easy to check:

Theorem 9.1.1 *If $\varphi : G \to G'$ is a homomorphism of algebraic groups, then $d\varphi : \mathfrak{g} \to \mathfrak{g}'$ is a homomorphism of Lie algebras.*

If H is a closed subgroup of an algebraic group G, the inclusion $\eta : H \to G$ is an isomorphism onto a closed subgroup, with $\eta^* : k[G] \to k[H] = k[G]/I$ being the natural projection. Therefore, $d\eta$ identifies $\mathfrak{h}$ with the Lie subalgebra of $\mathfrak{g}$ consisting of those $X \in \mathfrak{g}$ for which $X(I) = 0$. We will always identify $\mathfrak{h}$ with a Lie subalgebra of $\mathfrak{g}$ in this way. Now, let $\varphi : G \to G'$ be a morphism of algebraic groups, $H' < G'$ is a closed subgroup, and $\varphi(H) \subset H'$. Then $\varphi|H$ can be considered as a morphism $H \to H'$, so its differential $d(\varphi|H)$ is a Lie algebra homomorphism $\mathfrak{h} \to \mathfrak{h}'$. It follows from the definitions that

$$(d\varphi)|\mathfrak{h} : \mathfrak{h} \to \mathfrak{h}' = d(\varphi|H). \tag{9.1}$$

Lemma 9.1.2 *Let H be a closed subgroup of an algebraic group G and $I = I(H) \triangleleft k[G]$. Then $\mathfrak{h} = \{X \in \mathfrak{g} \mid I * X \subset I\}$.*

Proof If $f \in I$, $X \in \mathfrak{h}$, and $x \in H$, then $(f * X)(x) = X(\lambda_{x^{-1}} f) = 0$ since $\lambda_{x^{-1}} f \in I$. Conversely, if $I * X \subset I$ and $f \in I$, then $(f * X)(e) = X(\lambda_{e^{-1}} f) = X(f) = 0$, forcing $X \in \mathfrak{h}$. $\square$

Lemma 9.1.3 *Let $\rho : G \to GL(V)$ be a rational representation and $d\rho : \mathfrak{g} \to \mathfrak{g}l(V)$ be the corresponding Lie algebra representation. If $W \subset V$ is a G-invariant subspace then W is also $\mathfrak{g}$-invariant.*

Proof If we extend a basis of W to a basis of V, then the matrix of any $\rho(x)$ has the form $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$, and so the matrix of any $d\rho(X)$ has the same form. $\square$

9.2 Examples

Example 9.2.1 If $G = \mathbb{G}_a$, then $\mathfrak{g}$ is 1-dimensional, so its bracket is trivial.

Example 9.2.2 Let $G = GL_n$. Its tangent space at e has as a basis the set of partial derivatives $\frac{\partial}{\partial T_{ij}}|_e$ (evaluated at e). The coordinates x_{ij} with repsect to this basis can be arranged in a square matrix. So we can think of tangent vectors X as square matrices (x_{ij}), where $x_{ij} = X(T_{ij})$. With this convention $(X \cdot Y)(T_{ij}) = \sum_l x_{il} y_{lj}$. In other words, $X \cdot Y$ is the usual matrix product XY. Thus $\mathfrak{g} = \mathfrak{g}l_n(k)$.

Example 9.2.3 The Lie algebra $\mathfrak{s}l_n(k)$ of $SL_n < GL_n$ consists of all matrices in $\mathfrak{g}l_n(k)$ of trace 0. Indeed, let $X = (a_{ij}) = \sum a_{ij} \frac{\partial}{\partial T_{ij}}|_e$ be a tangent vector. Then $X \in \mathfrak{s}l_n(k)$ if and only if $X(\det) = 0$, which is equivalent to $\operatorname{tr} X = 0$.

Example 9.2.4 The group $Sp_{2n} < GL_{2n}$ is $Z(x^t Jx - x)$ ($4n^2$ polynomial equations written as one matrix equation). So the Lie algebra $\mathfrak{s}p_{2n}(k)$ consists of all matrices $X \in \mathfrak{g}l_{2n}(k)$ with $X(x^t Jx - x) = 0$. This is equivalent to $X^t J + JX = 0$ (compute!). Compute $\dim \mathfrak{s}p_{2n}(k)$.

Example 9.2.5 The group $O_n < GL_{2n}$ is $Z(xx^t - 1)$ (n^2 polynomial equations written as one matrix equation). So the Lie algebra $\mathfrak{s}o_n(k)$ consists of all matrices $X \in \mathfrak{g}l_n(k)$ with $X + X^t = 0$.

Example 9.2.6 The Lie algebra $\mathfrak{u}$ of the subgroup $U_n < GL_n$ of upper unitriangular matrices consists of all strictly upper triangular matrices in $\mathfrak{g}l_n(k)$.

Lemma 9.2.7 *Let G be an algebraic group with product $\mu : G \times G \to G$ and inverse $\iota : G \to G$. Then for all $X, Y \in \mathfrak{g}$:*

(i) $d\mu_{(e,e)}(X, Y) = X + Y$;
(ii) $d\iota_e(X) = -X$;

Proof Let $(X,Y) \in \mathfrak{g} \oplus \mathfrak{g} = T_{(e,e)} G \times G$, and $Z := d\mu_{(e,e)}(X,Y)$. If $f \in k[G]$ and $\Delta(f) = \sum_i f_i \otimes f_i'$, then $Z(f) = \sum_i (X(f_i) f_i'(e) + f_i(e) Y(f_i'))$, cf. the proof of Proposition 6.1.5. On the other hand, we have

$$f = \sum_i f_i(e) f_i' = \sum_i f_i'(e) f_i.$$

(you should have checked that when you checked the axioms of Hopf algebra for $k[G]$, but it's not too late now). So $Z(f) = (X+Y)(f)$, giving (i).

Consider the composite $G \to G \times G \to G,\ g \mapsto (g, \iota(g)) \mapsto g\iota(g) = e$. The composite is a constant function, so its differential is zero. But the differential of a composite is the composite of the differentials, so applying (i), we have $0 = d\,\mathrm{id}_e + d\iota_e = \mathrm{id} + d\iota_e$, whence (ii). $\square$

Lemma 9.2.8 *Let $E \subset k[G]$ be a finite dimensional subrepresentation of the (right) regular representation ρ of G, and $\psi : G \to GL(E)$ be the restriction of ρ to E. Then $d\psi(X)(f) = f * X$ for $f \in E$.*

Proof Pick a basis $\{f_1, \dots, f_n\}$ of E. Let $\Delta(f_i) = \sum_j f_j \otimes m_{ij}$, see (8.1). Then $\rho_x(f_i) = \sum_j m_{ij}(x) f_j$. So the matrix of $\psi(x)$ in our basis is $(m_{ij}(x))$. Note, moreover, that

$$\lambda_{x^{-1}} f_i = \sum_j f_j(x) m_{ij}. \tag{9.2}$$

Now, let $X \in \mathfrak{g}$. By definition, the (i,j)entry of the matrix $d\psi(X)$ is $X(\psi^*(T_{ij})) = X(m_{ij})$. On the other hand, using (9.2), we get

$$(f_i * X)(x) = X(\lambda_{x^{-1}} f_i) = \sum_j f_j(x) X(m_{ij}),$$

which completes the proof. $\square$

9.3 Ad and ad

Fix $x \in G$. Let $\operatorname{Int} x : G \to G, y \mapsto xyx^{-1}$. The differential $d(\operatorname{Int} x)_e$ is a Lie algebra automorphism denoted

$$\operatorname{Ad} x : \mathfrak{g} \to \mathfrak{g}.$$

The image of Ad is a (closed connected) subgroup of $GL(\mathfrak{g})$) denoted $\operatorname{Ad} G$.

Example 9.3.1 Let $G = GL_n$. Then $\mathrm{Ad}\, x(X) = xXx^{-1}$ (for $X \in \mathfrak{g} = \mathfrak{g}l_n(k)$). Hence for any closed subgroup $H < G$, its Lie algebra $\mathfrak{h}$, and $x \in H$, $\mathrm{Ad}\, x : \mathfrak{h} \to \mathfrak{h}$ is conjugation by x too.

For the proof, let us compute $(\mathrm{Int}\, x)^*(T_{ij})$:

$$(\mathrm{Int}\, x)^*(T_{ij})(g) = T_{ij}(xgx^{-1}) = \sum_{k,l} x_{ik} T_{kl}(g)(x^{-1})_{lj}.$$

Hence

$$(\mathrm{Int}\, x)^*(T_{ij}) = \sum_{k,l} x_{ik}(x^{-1})_{lj} T_{kl}.$$

Now, the ij-entry of $\mathrm{Ad}\, x(X)$ is

$$\mathrm{Ad}\, x(X)(T_{ij}) = X((\mathrm{Int}\, x)^*(T_{ij})) = \sum_{k,l} x_{ik}(x^{-1})_{lj} X(T_{kl}),$$

which is the ij-entry of xXx^{-1}.

Theorem 9.3.2 Ad *is a rational representation of* G *in (the vector space)* $\mathfrak{g}$ *(called the* adjoint representation *of* G*).*

Proof Embed G as a closed subgroup of some GL_n. Then by Example 9.3.1, $\mathrm{Ad}\, x$ is a conjugation by x, which implies that $\mathrm{Ad} : G \to GL(\mathfrak{g})$ is a morphism of varieties. □

Let $\mathrm{ad} : \mathfrak{g} \to \mathfrak{g}l(\mathfrak{g})$ be the *adjoint representation* of Lie algebra, i.e.

$$\mathrm{ad}\, X(Y) = [X, Y] \qquad (X, Y \in \mathfrak{g}).$$

Theorem 9.3.3 *The differential of* Ad *is* ad.

Proof Using embedding of G into some GL_n and (9.1), it suffices to check the result for $G = GL_n$. Note that $\mathrm{Ad}\, x$ is the image of x under the map

$$G \xrightarrow{(1,\iota)} G \times G \xrightarrow{\sigma \times \tau} GL(\mathfrak{g}) \times GL(\mathfrak{g}) \xrightarrow{\mu} GL(\mathfrak{g}),$$

where $\sigma(x)$ (resp. $\tau(x)$) is the left (resp. right) multiplication by x in $\mathfrak{g}$. Since the entries of $\sigma(x)$ and $\tau(x)$ are linear polynomials in the entries of x, it follows that $d\sigma(X)$ (resp. $d\tau(X)$) is a left (resp. right) multiplication by X. Now the result follows from Lemma 9.2.7. □

9.4 Properties of subgroups and subalgebras

Lemma 9.4.1 *If H is a closed normal subgroup of an algebraic group G, then $\mathfrak{h}$ is an ideal $\mathfrak{g}$.*

Proof We have $\mathrm{Int}\, x$ stabilizes H for all $x \in G$. Hence $\mathrm{Ad}\, x$ stabilizes $\mathfrak{h}$ for all $x \in G$. If we extend a basis of $\mathfrak{h}$ to a basis of $\mathfrak{g}$, then the matrix of $\mathrm{Ad}\, x$ therefore has the form $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ $(x \in G)$, and so the matrix of $d(\mathrm{Ad})(X) = \mathrm{ad}\, X$ has the same form $(X \in \mathfrak{g})$. □

Lemma 9.4.2 *If H is a closed subgroup of an algebraic group G and $N = N_G(H)$, then $\mathfrak{n} \subset \mathfrak{n}_{\mathfrak{g}}(\mathfrak{h})$.*

Proof Note that N is closed in view of Lemma 8.3.1(i). Applying Lemma 9.4.1 to the normal subgroup H of N, we see that $\mathfrak{h}$ is an ideal of $\mathfrak{n}$, i.e. $\mathfrak{n}$ normalizes $\mathfrak{h}$. □

For $x \in G$ denote

$$\gamma_x : G \to G, y \mapsto yxy^{-1}x^{-1}.$$

Lemma 9.4.3 *$(d\gamma_x)_e(X) = X - \mathrm{Ad}\, x(X)$.*

Proof Consider first the morphism $\psi : G \to G, y \mapsto xy^{-1}x^{-1}$. As $\psi = \mathrm{Int}\, x \circ \iota$, we have

$$d\psi_e(X) = d(\mathrm{Int}\, x) \circ d\iota_e(X) = \mathrm{Ad}\, x(-X) = -\mathrm{Ad}(X).$$

Now γ_x can be realizete as the composite

$$G \xrightarrow{(1,\psi)} G \times G \xrightarrow{\mu} G.$$

So $(d\gamma_x)_e(X) = d\mu_{(e,e)}(X, d\psi_e(X)) = X - \mathrm{Ad}\, x(X)$. □

Lemma 9.4.4 *Let $x \in G$. Then $L(C_G(x)) \subset \mathfrak{c}_{\mathfrak{g}}(x) := \{X \in \mathfrak{g} \mid \mathrm{Ad}\, x(X) = X\}$. If $G = GL_n$, then equality holds.*

Proof Note that the Lie algebra $L(C_G(x))$ of the fiber $\gamma_x^{-1}(e) = C_G(x)$ maps to zero under the map $(d\gamma_x)_e$. Now use Lemma 9.4.3.

In case of GL_n the fixed points of $\mathrm{Ad}\, x$ in $\mathfrak{g}$ are just the matrices commuting with x, so $C_G(x)$ is a principal open set in $\mathfrak{c}_{\mathfrak{g}}(x)$, containing e, which implies the result. □

Lemma 9.4.5 *Let $\rho : G \to GL(V)$ be a rational representation, and $d\rho : \mathfrak{g} \to \mathfrak{g}l(V)$ be the corresponding representation of the Lie algebra. If $v \in V$, let $C_G(v) = \{x \in G \mid xv = v\}$ and $\mathfrak{c}_{\mathfrak{g}}(v) := \{X \in \mathfrak{g} \mid Xv = 0\}$. Then $L(C_G(v)) \subset \mathfrak{c}_{\mathfrak{g}}(v)$.*

Proof Note that $x \mapsto xv$ is a morphism $G \to V$ constant on $C_G(v)$, so $d\rho_e$ is zero on the Lie algebra $L(C_G(v))$. □

Lemma 9.4.6 *Let A and B be closed subgroups of G, and let C be the closure of the subgroup $C = (A, B)$ generated by the commutators. The its Lie algebra $\mathfrak{c}$ contains all elements of the form $[X, Y]$, $Y - \operatorname{Ad} x(Y)$, $X - \operatorname{Ad} y(X)$ $(x \in A, X \in \mathfrak{a}, y \in B, Y \in \mathfrak{b})$. In particular, if H is the closure of (G, G), then $\mathfrak{h} \supset [\mathfrak{g}, \mathfrak{g}]$.*

Proof For $x \in A$, γ_x maps A to C, so the differential $1 - \operatorname{Ad} x$ maps $\mathfrak{b}$ to $\mathfrak{c}$. This yields all elements of the second type listed, and similarly for the third type. Next for $X \in \mathfrak{a}$ consider the morphism $\varphi : B \to \mathfrak{c}$ defined by $\varphi(y) = X - \operatorname{Ad} y(X)$. Since φ maps e to 0, we have $d\varphi_e(Y) = -\operatorname{ad} Y(X) = -[Y, X] = [X, Y]$. □

Remark 9.4.7 Inclusions in Lemmas 9.4.2, 9.4.4, 9.4.5, and 9.4.6 can be proper in positive characteristic and are equalities in characteristic 0.

9.5 Automorphisms and derivations

Lemma 9.5.1 *Let V and W be rational G-modules. Then*

(i) *$\mathfrak{g}$ acts on V^* by the rule $Xf(v) = -f(Xv)$ for $f \in V^*, v \in V, X \in \mathfrak{g}$.*
(ii) *$\mathfrak{g}$ acts on $V \otimes W$ by the rule $X(v \otimes w) = (Xv) \otimes W + v \otimes (Xw)$ for $v \in V, w \in W, X \in \mathfrak{g}$.*

Proof (i) We fix a basis of V and write the action of $x \in G$ as a matrix. Then the matrix of x acting on the dual basis of V^* is the transpose inverse matrix. We know that the differential of $x \mapsto x^{-1}$ is $X \mapsto -X$, while the map $x \mapsto x^t$ of GL_n has the differential $X \mapsto X^t$ on $\mathfrak{g}l_n$. This implies the result.

(ii) Fix bases $\{v_1, \dots, v_n\}$ of V and $\{w_1, \dots, w_m\}$ of W, and let $\rho_1 : G \to GL_n$, $\rho_2 : G \to GL_m$ be the corresponding matrix representations.

If $\rho_1(x) = (a_{ij})$ and $\rho_2(x) = (b_{rs})$, then the matrix $(\rho_1 \otimes \rho_2)(x)$ has entry $a_{ir}b_{js}$ in the (i,j)row and (r,s)column. So the representation $G \to GL_{mn}$ factors as the composite of two morphisms

$$G \stackrel{(\rho_1,\rho_2)}{\longrightarrow} GL_n \times GL_m \to GL_{mn},$$

where the second map is given in coordinates via $Z_{ij,rs} = X_{ir}Y_{js}$. It is easy to compute the differential (at (e,e)) of the second morphism—it maps a pair of matrices $((c_{ij}),(d_{rs})) \in \mathfrak{g}l_n \oplus \mathfrak{g}l_m$ to the matrix whose entry in row (i,j) and column (r,s) is $\delta_{js}c_{ir} + \delta_{ir}d_{js}$. This implies the rule asserted in (ii). □

Corollary 9.5.2 *Let $\mathcal{B}$ be a finite dimensional k-algebra (not necessarily associative), and let G be a closed subgroup of $GL(\mathcal{B})$, consisting of algebra automorphisms. Then $\mathfrak{g}$ consists of derivations of $\mathcal{B}$.*

Proof Let $t \in \mathcal{B}^* \otimes \mathcal{B}^* \otimes \mathcal{B} = \mathrm{Hom}_k(\mathcal{B} \otimes \mathcal{B}, \mathcal{B})$ be the multiplication on $\mathcal{B}$. Note that $x \in GL(\mathcal{B})$ is an automorphism of $\mathcal{B}$ if and only if t is an invariant of x. So t is an invariant of G, whence it is an invariant of $\mathfrak{g}$, see Lemma 9.4.5. This is equivalent to the fact that $\mathfrak{g}$ consists of derivations of $\mathcal{B}$. □

9.6 Problems

Problem 9.6.1 Let H be a closed subgroup of $G = GL(V)$, $\mathfrak{h} \subset \mathfrak{g}l(V)$ be its Lie algebra, $v \in V$, and $W \subset V$ be a vector subspace.

(i) If H leaves W stable, then so does $\mathfrak{h}$. Is the converse true?
(ii) If H leaves v stable, then $\mathfrak{h}$ kills v. Is the converse true?
(iii) Set $G_W := \{x \in G \mid x(W) \subset W\}$, $\mathfrak{g}_W := \{X \in g \mid X(W) \subset W\}$. Then $L(G_W) = \mathfrak{g}_W$. (*Hint:* $L(G_W) \subset \mathfrak{g}_W$ by (i). Now, use explicit descriptions of G_W and $\mathfrak{g}_W$ using matrices and dimensions).
(iv) Set $G_v := \{x \in G \mid xv = v\}$, $\mathfrak{g}_v := \{X \in g \mid Xv = 0\}$. Then $L(G_v) = \mathfrak{g}_v$.

Problem 9.6.2 Prove that $Z(G) \subset \ker \mathrm{Ad}$.

Problem 9.6.3 Let $\mathrm{char}\, k = p > 0$ and $G \subset GL_3$ consist of all matrices of the form $\begin{pmatrix} a & 0 & 0 \\ 0 & a^p & b \\ 0 & 0 & 1 \end{pmatrix}$ with $a \neq 0$. Observe that $\mathfrak{g}$ consists of all matrices $\begin{pmatrix} a & 0 & 0 \\ 0 & 0 & b \\ 0 & 0 & 0 \end{pmatrix}$ and is commutative. Moreover, $\{e\} = Z(G) \subsetneq \ker \operatorname{Ad} \subsetneq G$.

Problem 9.6.4 Let $\operatorname{char} k = 2$, $G = SL_2$, and B the group of all upper triangular matrices in G. Then $N_G(B) = B$, whereas $\mathfrak{n}_{\mathfrak{g}}(\mathfrak{b}) = \mathfrak{g}$.

Problem 9.6.5 Let $H < G$ be a closed subgroup and $x \in G$. Then $\operatorname{Ad} x(\mathfrak{h}) = L(\operatorname{Int} x(H))$.

Problem 9.6.6 Define $PGL_n := \operatorname{Ad} GL_n$ and $PSL_n := \operatorname{Ad} SL_n$. The centers of GL_n and SL_n consist of all scalar matrices contained in these groups. As abstract groups $PGL_n \cong GL_n/Z(GL_n)$ and $PSL_n \cong SL_n/Z(SL_n)$. If the characteristic p of k divides n, then $Z(SL_n) = \{1\}$, but SL_n is not isomorphic to PSL_n as algebraic groups!!!!

Problem 9.6.7 If $\operatorname{char} k = p > 0$ and X is a left invariant derivation of $k[G]$, then X^p is also a left invariant derivation of $k[G]$. This gives an extra operation on $\mathfrak{g}$, called *pth power operation*, which makes $\mathfrak{g}$ into a *restricted Lie algebra*. (One needs to check a number of axioms here, but never mind...) Compute the pth power operation for $G = \mathbb{G}_a$ and $G = GL_n$.

10

Quotients

The main problem addressed in this chapter is as follows: given an algebraic group G and a closed subgroup H, how to endow the quotient G/H with a 'reasonable' structure of algebraic variety?

10.1 Construction

We start with a linear algebra lemma.

Lemma 10.1.1 *Let M be a d-dimensional subspace of a vector space W, $x \in GL(W)$, $X \in \mathfrak{gl}(W)$. Then $L := \Lambda^d M$ can be considered as a line in $\Lambda^d W$.*

(i) *$xL = L$ if and only if $xM = M$.*
(ii) *$XL \subset L$ if and only if $XM \subset M$.*

Proof Exercise or read it in *Humpreys*. □

Theorem 10.1.2 (Chevalley) *Let G be an algebraic group, $H < G$ a closed subgroup. Then there is a rational representation $\varphi : G \to GL(V)$ and a 1-dimensional subspace L of V such that $H = \{x \in G \mid \varphi(x)L = L\}$ and $\mathfrak{h} = \{X \in \mathfrak{g} \mid d\varphi(X)L \subset L\}$.*

Proof Let $I = I(H) \triangleleft k[G]$. Let $W \subset k[G]$ be a finite dimensional subspace invariant with respect to all ρ_x and containing a (finite) generating set for I, see Lemma 8.4.2. Let $M = W \cap I$ (so M generates I). Note that $H = \{x \in G \mid \rho_x I = I\}$, so M is stable under all ρ_y for $y \in H$. It follows from Lemmas 9.2.8 and 9.1.3 that M is stable under all $*Y$ for $Y \in \mathfrak{h}$.

We claim that $H = \{x \in G \mid \rho_x M = M\}$ and $\mathfrak{h} = \{X \in \mathfrak{g} \mid M * X \subset M\}$. Indeed, if $\rho_x M = M$, then we have

$$\rho_x I = \rho_x(MA) = \rho_x(M)\rho_x(A) = MA = I,$$

forcing $x \in H$. If $M * X \subset M$ then the product rule implies

$$I * X = (MA) * X \subset (M * X)A + M(A * X) \subset MA = I,$$

forcing $X \in \mathfrak{h}$ by Lemma 9.1.2.

Finally, pass to $\Lambda^d W$ where $d = \dim M$, take φ to be the dth exterior power of the representation constructed above, and use Lemma 10.1.1. □

Corollary 10.1.3 *Let H be a closed subgroup of a connected algebraic group G. Then there exists a quasi-projective variety X that G acts transitively on and a point $x \in X$ such that*

(i) $G_x = H$;
(ii) *the orbit map $\psi : G \to X,\ g \mapsto gx$ is separable;*
(iii) *the fibers of ψ are the cosets gH of H in G.*

Proof Let V and $L = \langle v \rangle \subset V$ be as in the theorem. Take X to be the G-orbit $G\langle v \rangle$ in $\mathbb{P}(V)$ and $x = \langle v \rangle$. This is open in its closure, hence it is a quasi-projective variety. By the theorem, $H = G_x$, and now (iii) is also clear.

Finally note that the tangent space to $\mathbb{P}(V)$ at x can be canonically identified with $V/\langle v \rangle$, and the tangent space to X at x is a subspace of $V/\langle v \rangle$. The differential $d\psi_e$ maps $Y \in \mathfrak{g}$ to $Yv + \langle v \rangle$. Now, by the theorem, the kernel of the differential is $\mathfrak{h}$. So

$$\dim \ker d\psi_e = \dim \mathfrak{h} = \dim H = \dim G - \dim X.$$

Hence $d\psi_e$ is onto by dimension, and ψ is separable in view of Theorem 6.7.1. □

10.2 Quotients

In this section we will assume that G is a connected algebraic group and $H < G$ a closed subgroup. (The assumption that G is connected is not essential, but we do not want to deal with necessary modifications needed in the non-connected case).

A *Chevalley quotient* of G by H is a variety X together with a surjective separable morphism $\pi : G \to X$ such that the fibers of π are exactly cosets of H in G. By Corollary 10.1.3 Chevalley quotients exist, but it is not clear if they are unique up to isomorphism.

A *categorical quotient* of G by H is a variety X together with a morphism $\pi : G \to X$ that is constant on all cosets of H in G with the following universal property: given any other variety Y and a morphism $\varphi : G \to X$ that is constant on all cosets of H in G there is a unique morphism $\bar{\varphi} : X \to Y$ such that $\varphi = \bar{\varphi} \circ \pi$. Now, it is clear that categorical quotients are unique up to unique isomorphism, but it is not clear if they exist.

Our goal is to prove that Chevalley quotients are categorical quotients. This will prove that categorical quotients exist and that Chevalley quotients are unique. So we need to take a Chevalley quotient (X, π) and check that it has the right universal property. Given a morphism $\varphi : G \to Y$ constant on cosets, there is a unique map of *sets* $X \to Y$ such that $\varphi = \bar{\varphi} \circ \pi$, since fibers of π are exactly the cosets. But it is very difficult to prove from this point of view that φ is a morphism of varieties. So we proceed rather differently.

Theorem 10.2.1 *Chevalley quotients are categorical quotients.*

Proof Step 1. Let us try to construct a categorical quotient not in the category of varieties but in the more general category of geometric spaces. Define G/H to be the set of cosets of H in G. Let $\pi : G \to G/H$ be the map $x \mapsto xH$. Give G/H the structure of topological space by declaring $U \subset G/H$ to be open if and only if $\pi^{-1}(U)$ is open. Next define a sheaf $\mathcal{O}$ of functions on G/H: if $U \subset G/H$ is open, let $\mathcal{O}(U)$ consist of all functions f on U such that $f \circ \pi \in \mathcal{O}_G(\pi^{-1}(U))$. (Check the sheaf axioms!)

In order to check the universal property, let $\psi : G \to Y$ be a morphism of geometric spaces constant on the cosets of H in G. We get the induced map of sets $\bar{\psi} : G/H \to Y,\ xH \mapsto \psi(x)$. We claim that ψ is a morphism of geometric spaces. For continuity, take an open subset $V \subset Y$, and note that $U := \bar{\psi}^{-1}(V)$ is open in G/H, as $\pi^{-1}(\bar{\psi}^{-1}(V)) = \psi^{-1}(V)$ is open in G. Finally, take $f \in \mathcal{O}_Y(V)$ and show that $\bar{\psi}^*(f) \in \mathcal{O}_{G/H}(U)$. By definition, we just need to check that $\pi^*(\bar{\psi}^*(f)) \in \mathcal{O}_G(\psi^{-1}(V))$. But $\pi^*(\bar{\psi}^*(f)) = \psi^* f \in \mathcal{O}_G(\psi^{-1}(V))$, as ψ is a morphism of geometric spaces.

Step 2. Now, let $(G/H, \pi)$ be as in step 1, and let (X, ψ) be a Chevalley quotient. Using the universal property established above, we get a unique G-equivariant morphism $\bar{\psi} : G/H \to X$ such that $\psi = \bar{\psi} \circ \pi$, i.e. $\bar{\psi}(xH) = \psi(x)$. We will prove that $\bar{\psi}$ is an isomorphism of geometric spaces, which will imply that G/H is a variety and that X is a categorical quotient.

First of all, it is clear that $\bar{\psi}$ is bijective. Moreover, by Lemma 8.3.7, the map ψ is open (and continuous), which implies that $\bar{\psi}$ is a homeomorphism. In order to finish the proof, take an open subset $U \subset X$, a function $f \in \mathcal{O}_G(\psi^{-1}(U))$ constant on the cosets, and prove that $f = \psi^*(g)$ for some $g \in \mathcal{O}_X(U)$. For simplicity we consider the case $U = X$ when $\psi^{-1}(U) = G$. The argument for the general case is similar.

We show first that there exists a *rational* function g with the required property, i.e. $f = \psi^*(g)$ in $k(G)$. Consider the morphisms

$$G \xrightarrow{\varphi} X \times \mathbb{A}^1 \xrightarrow{\pi_1} X,$$

where $\varphi = (\psi, f)$. The composite is just ψ. If Y is the closure in $X \times \mathbb{A}^1$ of $\varphi(G)$, then Y is irreducible, and π_1 induces a surjective morphism $\eta : Y \to X$. Since ψ is separable, so is η (use $\psi^* = \varphi^* \circ \eta^*$).

Now, $\varphi(G)$ contains a dense open subset of Y, see Problem 5.5.3. Since f is constant on fibers of ψ, the restriction of η to this open set is injective, as well as dominant and separable. By Theorem 5.4.3, η^* maps $k(X)$ isomorphically onto $k(Y)$. But $\pi_2 : X \times \mathbb{A}^1 \to \mathbb{A}^1$ induces on Y a morphism $g : Y \to \mathbb{A}^1$, i.e. a regular function, in particular a rational function. So there exists $h \in k(X)$ for which $g = \eta^* h$. Finally, notice that $\varphi^* g = \varphi^* \eta^* h = \psi^* h$ agrees everywhere on G with f. So $f = \psi^* h$, as desired.

Next we want to show that the rational function $h \in k(X)$ just constructed is actually a regular function on Y. Since all points of X are simple, Theorem 6.3.2 shows that unless h is everywhere defined on X, $1/h$ is defined and is equal to 0 at some point. But then $\psi^*(1/h) = 1/f$ must also take the value zero, which is absurd since $f \in k[G]$. $\square$

We will denote by G/H the categorical quotient of G by the closed subgroup H. We now know that the categorical quotient exists and is unique up to a unique isomorphism. We also know that G/H is a quasi-projective variety and $\pi : G \to G/H$ is separable. Also note that

$$T_{eH}(G/H) \cong \mathfrak{g}/\mathfrak{h}.$$

Indeed, the separability of π implies that $d\pi_{eH}$ is surjective, and it contains $\mathfrak{h}$ in its kernel. Now use dimensions.

Example 10.2.2 Let $G = GL(V)$, $\{v_1, \dots, v_n\}$ be a basis of G, and $G = G_{\langle v_1 \rangle}$. Then $X = G\langle v_1 \rangle = \mathbb{P}(V)$ is a Chevalley quotient of G by H, see the proof of Corollary 10.1.3. So $G/H \cong \mathbb{P}(V)$. Similarly, let $P = G_{\langle v_1, \dots, v_d \rangle}$. Then $G/P \cong G_d(V)$. Finally, $G/B \cong \mathcal{F}$, where B is the stabilizer of a standard flag.

In the examples above quotients are projective varieties. Let $K := G_{v_1}$. Then $G/K \cong \mathbb{A}^n \setminus \{0\}$. This is neither affine nor projective (unless $n = 1$).

Example 10.2.3 Let $G = GL_n$ and $H = O_n = \{g \in GL_n \mid g^t g = I\}$ (assuming $\operatorname{char} k \neq 2$). Let S be the set of all $n \times n$ symmetric matrices, and affine variety of dimension $n(n+1)/2$. Let $S^\times$ be the invertible matrices in S, a principal open subset of S, hence also affine of dimension $n(n+1)/2$.

Let G act on S by $g \cdot x = g^t x g$. Then $G_I = O_n$, and the action is transitive, as by linear algebra all non-degenerate symmetric bilinear forms are equivalent. To prove that $GL_n/O_n \cong S^\times$, we just need to prove that the orbit map $G \to S^\times,\ g \mapsto g^t g$ is separable. Its differential is the map $X \mapsto X^t + X$. The tangent space to $S^\times$ at I can be identified with S. Clearly any symmetric matrix can be written in the form $X^t + X$ (characteristic is not 2!).

Thus $GL_n/O_n \cong S^\times$, which is an affine variety.

10.3 Normal subgroups

Let G be an algebraic group. A *character* of G is a homomorphism $\chi : G \to \mathbb{G}_m$ of algebraic groups. We write $X(G)$ for the set of all characters of G. It has a natural structure of an abelian group:

$$(\chi + \psi)(g) = \chi(g)\psi(g).$$

Let V be a rational G-module. For $\chi \in X(G)$, let

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

It is easy to see that $\sum_{\chi \in X(G)} V_\chi = \oplus_{\chi \in X(G)} V_\chi$, see Problem 10.4.5. On the other hand, it is usually not true that $V = \sum_{\chi \in X(G)} V_\chi$. But there is one important case when it is the case. This is when $G = D_n \cong (\mathbb{G}_m)^n$, the group of all diagonal matrices in GL_n. This will be established later.

Now, let N be a closed normal subgroup of G, and V be a rational G-module. If $\chi \in X(N)$, then for any $g \in G$ we have $gV_\chi \subset V_{\chi'}$ for

$\chi' = g\chi \in X(N)$. Here $g\chi(h) := \chi(g^{-1}hg)$. Indeed, let $v \in V_\chi$ and $h \in N$. Then $hgv = gg^{-1}hgv = \chi(g^{-1}hg)gv$.

Theorem 10.3.1 *Let G be an algebraic group and $N \subset G$ be a closed normal subgroup. Then the variety G/N is affine, and $G/N \times G/N \to G/N, (g_1N, g_2N) \mapsto g_1g_2N$, $G/N \to G/N, gN \mapsto g^{-1}N$ are morphisms of varieties.*

Proof Let us show first that $(g_1N, g_2N) \mapsto g_1g_2N$ is a morphism. The map $G \times G \to G/N$, $(g_1, g_2) \mapsto g_1g_2N$ is a morphism that is constant on cosets of $N \times N$. Hence by the universal property of the quotients, we get induced a unique morphism $G/N \times G/N \cong (G \times G)/(N \times N) \to G/N$, see Problem 10.4.1. The proof that $gN \mapsto g^{-1}N$ is a morphism is similar (but easier).

By Chevalley's theorem, we can find a rational representation $\rho : G \to GL(V)$ and $v \in V$ such that $H = G_{\langle v \rangle}$, and $\mathfrak{h}$ is the stabilizer of $\langle v \rangle$ in $\mathfrak{g}$. Let $V' = \oplus_{\chi \in X(N)} V_\chi$. Note that $v \in V'$ and V' is G-invariant, so we may assume that $V = V'$.

Now, let $W = \{f \in \mathrm{End}\,(V) \mid f(V_\chi) \subset V_\chi \text{ for all } \chi \in X(H)\}$. Define a morphism of algebraic groups $\psi : G \to GL(W)$, where

$$\psi(g)f = \rho(g)f\rho(g)^{-1} \qquad (g \in G,\ f \in W).$$

Let us compute the kernel of ψ: if $\psi(g) = \mathrm{id}$, then $\rho(g)$ stabilizes each V_χ and commutes with $\mathrm{End}\,(V_\chi)$, hence by Schur's lemma $\rho(g)$ acts as scalars on each V_χ. Hence g stabilizes $\langle v \rangle$, so $g \in H$. Conversely, if H acts as a scalar on each V_χ, then $H \subset \ker \psi$.

Note that the image of ψ is a closed—hence affine—subgroup of $GL(W)$. To show that this is a Chevalley quotient we just need to prove that ψ is separable. For this we show that $d\psi$ is onto, or equivalently by dimensions that $\ker d\psi \subset \mathfrak{h}$. Let $X \in \ker d\psi$. Then $d\psi(X)(f) = d\rho(X)f - fd\rho(X) = 0$, so $d\rho(X)$ commutes with all $f \in W$. This implies that $d\rho(X)$ acts as a scalar on all V_χ's, in particular, it stabilizes $\langle v \rangle$, hence $X \in \mathfrak{h}$. □

Corollary 10.3.2 *Suppose that $\varphi : G \to H$ be a separable surjective morphism of algebraic groups and $N = \ker \varphi$. Then φ induces an isomorphism $G/N \cong H$.*

Note in characteristic 0 the separability is automatic. On the other hand, let $G = H = GL_n$, and let φ be the Frobenius homomorphism given by raising matrix entries to the pth power. This is a morphism of algebraic groups and an isomorphism of abstract groups, but the differential $d\varphi$ is the zero map. So φ is definitely not an isomorphism of algebraic groups.

10.4 Problems

Problem 10.4.1 Let $H_1 < G_1, H_2 < G_2$ be closed subgroups of connected algebraic groups. Prove that $(G_1 \times G_2)/(H_1 \times H_2) \cong G_1/H_1 \times G_2/H_2$.

Problem 10.4.2 Prove that GL_{2n}/Sp_{2n} is isomorphic to the affine variety of all invertible $2n \times 2n$-skew symmetric matrices. (In characteristic 2 a skew symmetric matrix means a symmetric matrix with zeros on the main diagonal).

Problem 10.4.3 Prove that $X(SL_n) = \{0\}$, $X(\mathbb{G}_a) = \{0\}$, $X(\mathbb{G}_m) \cong \mathbb{Z}$, $X(GL_n) = \mathbb{Z}$.

Problem 10.4.4 Prove that $X(G \times H) \cong X(G) \oplus X(H)$.

Problem 10.4.5 Prove that $\sum_{\chi \in X(G)} V_\chi = \oplus_{\chi \in X(G)} V_\chi$

Problem 10.4.6 Let $A, B \subset G$ be closed subgroups. Prove that $\mathfrak{a} \cap \mathfrak{b} = L(A \cap B)$ if and only if the restriction to A of the canonical morphism $\pi : G \to G/B$ is again separable. (*Hint:* consult Theorem 12.1.1.)

Problem 10.4.7 Let H be a closed subgroup of a connected algebraic group G. Then H acts naturally on $k(G)$ as a group of automorphisms, and $k(G/H) \cong k(G)^H$.

Problem 10.4.8 Compute the dimension of the flag variety.

11

Semisimple and unipotent elements

11.1 Jordan-Chevalley decomposition

The following result about the *additive Jordan decomposition* is well known:

Lemma 11.1.1 *Let V be a finite dimensional k-vector space and $X \in \operatorname{End} V$.*

(i) *There exist unique $X_s, X_n \in \operatorname{End}(V)$ satisfying the conditions $X = X_s + X_n$, X_s is semisimple, X_n is nilpotent, and $X_s X_n = X_n X_s$.*

(ii) *There exist polynomials $p(T), q(T)$ without constant term such that $X_s = p(X), X_n = q(X)$. In particular X_s, X_n commute with any endomorphism of V which commutes with X.*

(iii) *If $A \subset B \subset V$ are subspaces and X maps B to A, then so do X_s and X_n.*

(iv) *If $XY = YX$ for $Y \in \operatorname{End} V$ then $(X+Y)_s = X_s + Y_s$ and $(X+Y)_n = X_n + Y_n$.*

(v) *If $\varphi : V \to W$ is a linear map and $Y \in \operatorname{End} W$ such that $Y \circ \varphi = \varphi \circ X$, then $Y_s \circ \varphi = \varphi \circ X_s$ and $Y_n \circ \varphi = \varphi \circ X_n$.*

An element $x \in \operatorname{End} V$ is called *unipotent* if it is the sum of id_V and a nilpotent element, or, equivalently, if the only eigenvalue of x is 1. In characteristic p an element $x \in \operatorname{End} V$ is unipotent if and only if $x^{p^N} = 0$ for some N. The additive Jordan decomposition implies the *multiplicative Jordan decomposition*:

Lemma 11.1.2 *Let V be a finite dimensional k-vector space and $x \in GL(V)$.*

(i) *There exist unique* $x_s, x_u \in \mathrm{End}\,(V)$ *satisfying the conditions* $x = x_s x_u$, x_s *is semisimple,* x_u *is unipotent, and* $x_s x_u = x_u x_s$.

(ii) x_s, x_u *commute with any endomorphism of* V *which commutes with* x.

(iii) *If* $A \subset V$ *is a subspaces stable under* x*, then* A *is stable under* x_s *and* x_u.

(iv) *If* $xy = yx$ *for* $y \in GL(V)$ *then* $(xy)_s = x_s y_s$ *and* $(xy)_u = x_u y_u$.

(v) *If* $\varphi : V \to W$ *is a linear map and* $y \in \mathrm{End}\,W$ *such that* $y \circ \varphi = \varphi \circ x$*, then* $y_s \circ \varphi = \varphi \circ x_s$ *and* $y_u \circ \varphi = \varphi \circ x_u$.

We leave the following as an exercise:

Lemma 11.1.3 *Let* $x = x_s x_u$ *and* $y = y_s y_u$ *be Jordan decompositions of* $x \in GL(V)$ *and* $y \in GL(W)$*. Then* $x \oplus y = (x_s \oplus y_s)(x_u \oplus y_u)$ *and* $x \otimes y = (x_s \otimes y_s)(x_u \otimes y_u)$ *are Jordan decompositions of* $x \oplus y \in GL(V \oplus W)$ *and* $x \otimes y \in GL(V \otimes W)$.

Theory of Jordan decompositions generalize to infinite dimensional vector spaces V providing we restrict our attention to *locally finite* endomorphisms x, i.e. endomorphisms such that any $v \in V$ belongs to a finite dimensional x-invariant subspace. A locally finite endomorphism x of V is *semisimple* if its restriction to every finite dimensional x-invariant subspace of V is semisimple. Nilpotent and unipotent are defined similarly. For a general locally finite $x \in \mathrm{End}\,V$ we have its Jordan decompositions $x = x_s + x_n$ and $x = x_s x_u$, with all the properties of the finite dimensional case holding. To define x_s, take $v \in V$, find a finite dimensional x-invariant subspace W containing v and define $x_s(v) = (x|W)_s(v)$. The fact that this is well-defined follows from the uniqueness statement in the finite dimensional Jordan decomposition. The elements x_n and x_u are defined similarly.

Theorem 11.1.4 *For any* $x \in G$*, there are unique elements* $x_s, x_u \in G$ *such that* $(\rho_x)_s = \rho_{x_s}$, $(\rho_x)_u = \rho_{x_u}$*, and* $x = x_s x_u = x_u x_s$*. Moreover, if* $\varphi : G \to H$ *is a morphism of algebraic groups, then* $\varphi(x_s) = \varphi(x)_s$ *and* $\varphi(x_u) = \varphi(x)_u$.

Proof Let $m : k[G] \otimes k[G] \to k[G]$ be the algebra multiplication. We have

$$m \circ (\rho_x \otimes \rho_x) = \rho_x \circ m.$$

Hence by Lemmas 11.1.2(v) and 11.1.3,

$$m \circ ((\rho_x)_s \otimes (\rho_x)_s) = (\rho_x)_s \circ m,$$

i.e. $(\rho_x)_s$ respects the multiplication on $k[G]$. Also $\rho_x(1) = 1$ implies $(\rho_x)_s(1) = 1$ by the properties of Jordan decomposition. Thus $(\rho_x)_s$ is an automorphism of $k[G]$. Hence $\xi : f \mapsto ((\rho_x)_s f)(e)$ is an algebra homomorphism $k[G] \to k$. So there is a point $x_s \in G$ with $\xi(f) = f(x_s)$.

To prove that $(\rho_x)_s$ and ρ_{x_s} are the same note that λ_y and ρ_x commute for all y, so λ_y and $(\rho_x)_s$ commute too. Now,

$$\begin{aligned} ((\rho_x)_s f)(y) &= (\lambda_{y^{-1}}(\rho_x)_s f)(e) = ((\rho_x)_s \lambda_{y^{-1}} f)(e) \\ &= (\lambda_{y^{-1}} f)(x_s) = f(yx_s) = (\rho_{x_s} f)(y). \end{aligned}$$

Similarly we find x_u such that $(\rho_x)_u = \rho_{x_u}$. But the right regular representation is faithful, so $\rho_x = \rho_{x_s}\rho_{x_u} = \rho_{x_u}\rho_{x_s}$ implies $x = x_s x_u = x_u x_s$.

Now, let $x \in G$ and $y = \varphi(x)$. It is easy to check that $\varphi^* \circ \rho_y = \rho_x \circ \varphi^*$. Hence $\varphi^* \circ (\rho_y)_s = (\rho_x)_s \circ \varphi^*$. So $\varphi^* \circ \rho_{y_s} = \rho_{x_s} \circ \varphi^*$. For any $f \in k[H]$,

$$(\varphi^*(\rho_{y_s}(f)))(e) = (\rho_{y_s}(f))(\varphi(e)) = (\rho_{y_s}(f))(e) = f(y_s).$$

This equals

$$(\rho_{x_s} \circ \varphi^*)(f)(e) = (\varphi^* f)(x_s) = f(\varphi(x_s)).$$

We conclude that $\varphi(x_s) = y_s$. The argument for the unipotent parts is similar. $\square$

Remark 11.1.5 One can also prove the infinitesimal analogue of this result: for any $X \in \mathfrak{g}$, there are unique elements $X_s, X_n \in \mathfrak{g}$ such that $(*X)_s = *X_s$, $(*X)_u = *X_n$, $[X_s, X_n] = 0$, and $X = X_s + X_n$; moreover, if $\varphi : G \to H$ is a morphism of algebraic groups, then $d\varphi(X_s) = d\varphi(X)_s$ and $d\varphi(X_n) = d\varphi(X)_n$. See *Humphreys* for details.

Decompositions $x = x_s x_u$ and $X = X_s + X_n$ coming from the theorem and the remark are refereed to as the *abstract Jordan decompositions* or *Jordan-Chevalley decompositions*. If $x = x_s$, we call x *semisimple*, and of $x = x_u$ we call u *unipotent*. The set of all semisimple (resp. unipotent) elements of G is denoted G_s (resp. G_u).

Example 11.1.6 If $x \in G = GL_n$, then x_s is just the semisimple part of x considered as an endomorphism of $V = k^m$, and x_u is the unipotent part. To see this, let $f \in V^*$ be a non-zero functional. For $v \in V$ define

$\tilde{f}(v) \in k[G]$ by $\tilde{f}(v)(x) = f(xv)$. This gives an injective linear map $\tilde{f} : V \to k[G]$ which satisfies $\tilde{f}(xv) = \rho_x \tilde{f}(v)$. Hence

$$\tilde{f}(x_s v) = (\rho_x)_s \tilde{f}(v) = \rho_{x_s} \tilde{f}(v) = \tilde{f}(x_s v),$$

where the first x_s is the semisimple part of x in the old sense of linear algebra, and the other two x_s's refer to the semisimple part of x in the abstract Jordan decomposition. This implies that the two are the same. The argument for the unipotent parts and Lie algebras is similar.

For an arbitrary G, we can embed it as a closed subgroup of some $GL(V)$. Then again, the abstract Jordan decompositions $x = x_s x_u$ of x as an element of G and as an endomorphism of V coincide.

11.2 Unipotent algebraic groups

An algebraic group is called *unipotent* if all of its elements are unipotent.

Theorem 11.2.1 *Let G be a unipotent closed subgroup of GL_n. Then there is $g \in GL_n$ such that $gGg^{-1} < U_n$.*

Proof Let $V = k^n$. It suffices to show that G fixes some flag in V. Using induction on n we may assume that G does not stabilize any subspace of V, i.e. G acts irreducibly on G. Then by Wedderburn theorem the elements of G span the vector space $\operatorname{End} V$. Since G is unipotent, all elements of G have trace n. Hence $0 = \operatorname{tr}(h - gh) = \operatorname{tr}(1 - g)h$ for all $g, h \in G$, hence for all $g \in G$ and all $h \in \operatorname{End} V$. Taking h to be various matrix units, you now get that $1 - g = 0$, i.e. $G = \{e\}$. □

Corollary 11.2.2 *Unipotent algebraic groups are nilpotent.*

Theorem 11.2.3 (Rosenlicht) *Let G be an unipotent algebraic group acting on an algebraic variety X. Then all orbits of G on X are closed.*

Proof Let $\mathcal{O}$ be an orbit. Replacing X by $\bar{\mathcal{O}}$, we may assume that $\mathcal{O}$ is open dense in X. Let Y be its complement. Consider the action of G on $k[X]$ by translation of functions. This action is locally finite, see Problem 8.5.9. Moreover, G stabilizes Y, so it leaves $I(Y)$ invariant. By Theorem 11.2.1, there is a non-zero function $f \in I(Y)$ fixed by G. But then f is constant on $\mathcal{O}$. So, since $\mathcal{O}$ is dense, f is constant on X. This shows that f is a non-zero scalar, hence $I(Y) = k[X]$ and $Y = \varnothing$. □

Now let G be an arbitrary connected algebraic group. Suppose that X, Y are two closed connected normal solvable subgroups of G. Then XY is again a closed connected normal solvable subgroup of G. It follows that G contains a unique maximal closed connected normal solvable subgroup. This is called the *radical* of G and denoted $R(G)$. Similarly one defines the *unipotent radical* $R_u(G)$ as the unique maximal closed connected normal unipotent subgroup.

A connected algebraic group is called *semisimple* if $R(G) = \{e\}$ and *reductive* if $R_u(G) = \{e\}$. Unipotent groups are nilpotent, so semisimple groups are reductive. There is a beautiful structure theory and classification of reductive groups.

Lemma 11.2.4 *If $M \subset M_n(k)$ is a commuting set of matrices, then M is triagonalizable. If M consists of the diagonalizable matrices, then M is diagonalizable.*

Proof Linear algebra. See *Humpreys*, 15.4. □

Theorem 11.2.5 *Let G be a commutative algebraic group. Then G_s and G_u are closed subgroups of G, connected if G is, and the product map $\varphi : G_s \times G_u \to G$ is an isomorphism of algebraic groups.*

Proof That G_s, G_u are subgroups follows from Lemma 11.1.2(iv). That G_u is closed is Problem 11.3.1. Moreover, Theorem 11.1.4 implies that φ is an isomorphism of abstract groups. Now embed G into some GL_n. Lemma 11.2.4 allows us to assume that G is a group of upper triangular matrices and that G_s is a group of diagonal matrices. This implies that G_s is also closed.

It has to be shown that the inverse map is a morphism or that the maps $x \mapsto x_s$ and $x \mapsto x_u$ are morphisms. The second is if the first is, as $x_u = x_s^{-1}x$. Now x_s is just the diagonal part of the matrix x (why?), so $x \mapsto x_s$ is a morphism. Now the connectedness of G also implies that of G_s and G_u. □

11.3 Problems

Problem 11.3.1 The set of all unipotent elements of G is closed.

Problem 11.3.2 Let $\mathcal{B}$ be a finite dimensional k-algebra. If $x \in \mathrm{Aut}\mathcal{B}$, then $x_s, x_u \in \mathrm{Aut}\mathcal{B}$.

Problem 11.3.3 Let $\mathrm{char}\, k = 0$. An element of GL_n having finite order must be semisimple.

Problem 11.3.4 Let G be a connected algebraic group of positive dimension. Prove that $R(G) = \{e\}$ if and only if G has no closed connected commutative normal subgroup. (*Hint:* see Example 8.2.10).

Problem 11.3.5 If $\mathrm{char}\, k = 0$, then every unipotent subgroup of GL_n is connected.

Problem 11.3.6 If $\mathrm{char}\, k = 0$ then 1-dimensional unipotent group is isomorphic to G_a.

12
Characteristic 0 theory

Throughout this chapter we assume $\operatorname{char} k = 0$.

12.1 Correspondence between groups and Lie algebras

Theorem 12.1.1

(i) *If* $\varphi : G \to G'$ *is a morphism of algebraic groups then* $\ker d\varphi = L(\ker\varphi)$.
(ii) *If* $A, B < G$ *are closed subgroups then* $\mathfrak{a} \cap \mathfrak{b} = L(A \cap B)$.

Proof (i) We may assume that φ is surjective. Of course, $L(\ker\varphi) \subset \ker d\varphi$. Since φ is separable, $d\varphi$ is surjective, and the result follows by dimensions.

(ii) Let $\pi : G \to G/B$ be the canonical morphism, so $\ker d\pi_e = \mathfrak{b}$. Let $\pi' : A \to \pi(A)$ be the restriction of π. The fibers of π' are the cosets of $A \cap B$ in A, and π' is separable. (Also $\pi(A)$ is a variety because it is an A-orbit in G/B). Therefore $\pi(A) \cong A/(A \cap B)$, and now as in (i) we deduce that $\ker d\pi'_e = L(A \cap B)$. On the other hand, $\ker d\pi'_e = \mathfrak{a} \cap \ker d\pi_e = \mathfrak{a} \cap \mathfrak{b}$. □

Lemma 12.1.2 *Let G be connected, $\rho : G \to GL(V)$ be a rational representation and $d\rho : \mathfrak{g} \to \mathfrak{gl}(V)$ be the corresponding representation of $\mathfrak{g}$. Then G and $\mathfrak{g}$ leave the same subspaces (resp. vectors) invariant.*

Proof In view of Theorem 12.1.1(i), we may assume that $G < GL(V)$. By Problem 9.6.1, $L(GL(V)_W) = \mathfrak{gl}(V)_W$, and $G_W = G \cap GL(V)_W$, $\mathfrak{g}_W = \mathfrak{g} \cap \mathfrak{gl}(V)_W$. By Theorem 12.1.1(ii), $L(G_W) = \mathfrak{g}_W$. Finally, G

stabilizes W if and only if $G_W = G$ and $\mathfrak{g}$ stabilizes W if and only if $\mathfrak{g}_W = \mathfrak{g}$. □

Corollary 12.1.3 *Let $\mathcal{B}$ be a finite dimensional k-algebra. Then*

$$L(\mathrm{Aut}\mathcal{B}) \cong \mathrm{Der}\,\mathcal{B}.$$

Proof The proof of Corollary 9.5.2 shows that $x \in GL(\mathcal{B})$ is an automorphism if and only if it fixes certain tensor $t \in \mathcal{B}^*\otimes\mathcal{B}^*\otimes\mathcal{B}$, while $X \in \mathfrak{g}l(\mathcal{B})$ is a derivation if and only if it kills t. Now apply Lemma 12.1.2. □

Definition 12.1.4 Let $\mathfrak{g} = L(G)$. A Lie subalgebra $\mathfrak{h}$ of $\mathfrak{g}$ is called *algebraic* if $\mathfrak{h} = L(H)$ for a closed connected subgroup $H < G$.

Even in characteristic 0 not all subalgebras are algebraic.

Theorem 12.1.5 *Assume that G is connected. Then the map $H \mapsto \mathfrak{h}$ is a one-to-one inclusion preserving correspondence between the closed connected subgroups of G and the algebraic Lie subalgebras. Moreover, normal subgroups correspond to ideals.*

Proof Suppose $L(H) = L(K)$. Using Theorem 12.1.1(ii), we have $L(H\cap K) = L(H)\cap L(K) = L(H)$. So $\dim H\cap K = \dim H$, whence $H\cap K = H$. Similarly, $H \cap K = K$. It follows that $H = K$.

We already know that $\mathfrak{h}$ is an ideal if H is normal, see Lemma 9.4.1. Conversely, suppose $\mathfrak{h} \subset \mathfrak{g}$ is an ideal. Then $\mathfrak{g}$ stabilizes $\mathfrak{h}$ via ad, hence G stabilizes $\mathfrak{h}$ via Ad, see Lemma 12.1.2. But for $x \in G$, $\mathrm{Ad}\,x : \mathfrak{h} \to \mathfrak{g}$ is the differential of $\mathrm{Int}\,x : H \to G$. By separability, $\mathfrak{h} = \mathrm{Ad}\,x(\mathfrak{h}) = L(\mathrm{Int}\,x(H)) = L(xHx^{-1})$. Now, by the previous paragraph, $H = xHx^{-1}$, as they have the same Lie algebra. □

Theorem 12.1.6 *Let G be a connected algebraic group.*

(i) *If $x \in G$, then $L(C_G(x)) = \mathfrak{c}_{\mathfrak{g}}(x)$.*
(ii) $\ker \mathrm{Ad} = Z(G)$*, and* $L(Z(G)) = \mathfrak{z}(\mathfrak{g})$.

Proof (i) Lemma 9.4.4 shows that this is true when $G = GL_n$. In general, embed G as a closed subgroup of some GL_n and use Theorem 12.1.1(ii).

(ii) By Theorem 12.1.1, $L(\ker \mathrm{Ad}) = \ker \mathrm{ad} = \mathfrak{z}(\mathfrak{g})$. As $\mathrm{Ad} = d\,\mathrm{Int}$, $Z(G) \subset \ker \mathrm{Ad}$. Conversely, if $x \in \ker \mathrm{Ad}$, then $\mathfrak{g} = \mathfrak{c}_{\mathfrak{g}}(x) = L(C_G(x))$, whence $C_G(x) = G$ since they have the same Lie algebras. Thus $x \in Z(G)$. □

Corollary 12.1.7 *A connected algebraic group is commutative if and only if its Lie algebra is abelian.*

12.2 Semisimple groups and Lie algebras

A Lie algebra (of positive dimension) is *semisimple* if it does not have non-trivial solvable ideals. This is equivalent to the requirement that the Lie algebra does not have non-zero commutative ideals. Similarly, a connected algebraic group of positive dimension is *semisimple* if and only if it has no closed connected commutative normal subgroup except $\{e\}$, see Problem 11.3.4.

Theorem 12.2.1 *A connected algebraic group is semisimple if and only if its Lie algebra is semisimple.*

Proof If $N < G$ is a closed connected commutative normal subgroup then $\mathfrak{n}$ is a commutative ideal of $\mathfrak{g}$, so $\mathfrak{n} = 0$ forcing $N = \{e\}$. Conversely, let $\mathfrak{n} \subset \mathfrak{g}$ be a commutative ideal. Define $H := C_G(\mathfrak{n})^\circ$. Then $\mathfrak{h} = \mathfrak{c}_\mathfrak{g}(\mathfrak{n})$ by Lemma 12.1.2. Since $\mathfrak{n}$ is an ideal, so is $\mathfrak{c}_\mathfrak{g}(\mathfrak{n})$. Hence H is normal in G. Hence $Z := Z(H)^\circ$ is also normal in G. By Theorem 12.1.6(ii), $\mathfrak{z}$ is the center of $\mathfrak{h}$, and therefore includes $\mathfrak{n}$. But G is semisimple, so $Z = \{e\}$, $\mathfrak{z} = 0$. This forces $\mathfrak{n} = 0$. □

Remark 12.2.2 When G is semisimple, $\mathfrak{g}$ is semisimple, so $\mathfrak{z}(\mathfrak{g}) = 0$, whence $Z(G)$ is finite, see Theorem 12.1.6.

Corollary 12.2.3 *Rational representations of semisimple algebraic groups are completely reducible.*

Proof This follows from the similar fact about Lie algebras (known as Weyl's complete reducibility theorem) together with Theorem 12.2.1 and Lemma 12.1.2. □

Theorem 12.2.4 *Let G be semisimple. Then* $\mathrm{Ad}\, G = (\mathrm{Aut}\mathfrak{g})^\circ$ *and* $\mathrm{ad}\,\mathfrak{g} = \mathrm{Der}\,\mathfrak{g}$.

Proof That $\operatorname{ad}\mathfrak{g} = \operatorname{Der}\mathfrak{g}$ is a well-known result in Lie algebras that all derivations of a semisimple Lie algebra are inner. On the other hand, $\operatorname{Ad} G \subseteq \operatorname{Aut}(\mathfrak{g})^\circ$, so it suffices to observe that their dimensions coincide. Well, this follows from $\dim \operatorname{Ad} G = \dim G$, and $\dim \mathfrak{g} = \dim \operatorname{Der}(\mathfrak{g}) = \dim \operatorname{Aut}(G)^\circ$, see Corollary 12.1.3. $\square$

The theorem shows that a semisimple group can be recovered from its Lie algebra "up to a finite center", and goes a long way towards the classification of semisimple algebraic groups in characteristic 0.

12.3 Problems

Recall that $\operatorname{char} k = 0$ in this capter.

Problem 12.3.1 Let G be a connected algebraic group, $H < G$ closed connected subgroup. Prove that $L(N_G(H)) = \mathfrak{n}_{\mathfrak{g}}(\mathfrak{h})$ and $L(C_G(H)) = \mathfrak{c}_{\mathfrak{g}}(\mathfrak{h})$.

Problem 12.3.2 Let G be a connected algebraic group, $\mathfrak{h}$ a subalgebra of $\mathfrak{g}$. Prove that $L(C_G(\mathfrak{h})) = \mathfrak{c}_{\mathfrak{g}}(\mathfrak{h})$.

Problem 12.3.3 Prove that SL_2 is semisimple.

13
Semisimple Lie algebras

We saw that in characteristic 0 a connected algebraic group is semisimple if and only its Lie algebra is semisimple. Semisimple Lie algebras can be classified, and this gives us a first approximation to the classification of semisimple algebraic groups in characteristic 0. It turns out that the semisimple algebraic group in characteristic 0 is determined up to finite central subgroup by its Lie algebra (and it is easy to keep the finite group under control). It turns out that the classification of semisimple groups is essentially the same in arbitrary characteristic, although this is much more difficult to prove. In this chapter we are going to review semisimple Lie algebras and explain how to a semisimple Lie algebra we can associate an algebraic group in arbitrary characteristic. This is going to be roughly half of the classification.

13.1 Root systems

We want to review classification of the finite dimensional semisimple Lie algebras over $\mathbb{C}$. The first step is to introduce the abstract notion of a root system.

Definition 13.1.1 A *root system* is a pair (E, Φ) where E is a (real) Euclidean space and Φ is a finite set of non-zero vectors, called *roots*, in E such that

(i) Φ spans E.
(ii) $\alpha, c\alpha \in \Phi$ implies $c = \pm 1$.
(iii) For any root α, Φ is invariant under the reflection s_α in the hyperplane orthogonal to α, i.e. the automorphism

$$\beta \mapsto \beta - (\beta, \alpha^\vee)\alpha,$$

where $\alpha^\vee := 2\alpha/(\alpha,\alpha)$.

(iv) $(\alpha,\beta^\vee) \in \mathbb{Z}$ for all $\alpha,\beta \in \mathbb{Z}$.

Given a root system, the *Weyl group* W is the subgroup of $GL(E)$ generated by the s_α for $\alpha \in \Phi$. It is a finite group, since it acts faithfully on the finite set Φ.

We let $H_\alpha = \{\beta \in E \mid (\alpha,\beta) = 0\}$ be the hyperplane orthogonal to α. The connected components of

$$E \setminus \bigcup_{\alpha\in\Phi} H_\alpha$$

are called the *Weyl chambers*. Fix a chamber C, which we will call the *fundamental chamber*. Then one can show that the map

$$w \mapsto wC$$

is a bijection between W and the set of chambers.

The choice of C fixes several other things. We let Φ^+ be the set of all $\alpha \in \Phi$ which are in the same half space as C (by this we mean that $(\gamma,\alpha) > 0$ for any $\gamma \in C$). Then, $\Phi = \Phi^+ \sqcup (-\Phi^+)$. Elements of Φ^+ are called *positive roots*. Next, let

$$\Pi = \{\alpha \in \Phi^+ \mid H_\alpha \text{ is one of the walls of } C\}.$$

This is called a *base* for the root system. One can show that Π is actually a basis for the vector space E, and moreover every element of Φ^+ is a non-negative integer linear combination of Π. Elements of Π are called *simple roots*.

The Weyl group W is actually generated by the s_α for $\alpha \in \Pi$, i.e. by the reflections in the walls of the fundamental chamber. This leads to the idea of the *length* $\ell(w)$ of $w \in W$, which is defined as the minimal length of an expression $w = s_{\alpha_1} \dots s_{\alpha_r}$ where $\alpha_1, \dots, \alpha_r$ are simple roots. Geometrically, $\ell(w)$ is the number of hyperplanes separating wC from C.

Let $\Pi = \{\alpha_1, \dots, \alpha_\ell\}$. Here $\ell = \dim E$ is the *rank* of the root system. The *Cartan matrix* $A = (a_{i,j})_{1\le i,j\le \ell}$ is the matrix with

$$a_{i,j} = (\alpha_i, \alpha_j^\vee).$$

Since all the Weyl chambers are conjugate under the action of W, the Cartan matrix is an invariant of the root system (up to simultaneous permutation of rows/columns). Here are some basic properties about this matrix:

(C1) $a_{i,i} = 2$.
(C2) For $i \neq j$, $a_{i,j} \in \{0, -1, -2, -3\}$.
(C3) $a_{i,j} \neq 0$ if and only if $a_{j,i} \neq 0$.

Note (C2) is not obvious. It follows because $E' = \langle \alpha_i, \alpha_j \rangle$ together with $\Phi' := \Phi \cap E'$ is a root system of rank 2. Rank 2 root systems are easy (and fun) to classify. Their Cartan matrices are exactly the following:

$$A_1 \times A_1 : \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \quad A_2 : \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix},$$
$$B_2 : \begin{pmatrix} 2 & -2 \\ -1 & 2 \end{pmatrix}, \quad G_2 : \begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix}.$$

Note if $a_{i,j} \neq 0$, then

$$(\alpha_i, \alpha_i)/(\alpha_j, \alpha_j) = a_{i,j}/a_{j,i} \in \{1, 2, 3\},$$

so in this case you can work out the ratio of the lengths of the roots α_i, α_j to each other from the Cartan matrix.

A root system is called *indecomposable* if it cannot be partitioned $E = E_1 \perp E_2, \Phi = \Phi_1 \sqcup \Phi_2$ where (E_i, Φ_i) are root systems. An equivalent property is that we cannot order roots in such a way that the corresponding Cartan matrix has block-diagonal form. Thus, for an indecomposable root system, one can work out the ratio of lengths of any pair of roots to each other from the Cartan matrix, hence one completely recovers the form $(.,.)$ on E *up to a scalar* from the Cartan matrix. One also recovers Φ, since the Cartan matrix contains enough information to compute the reflection s_{α_i} for each $i = 1, \dots, \ell$, and $\Phi = W\Pi$. So (with the correct definition of an isomorphism—give it!) *an indecomposable root system is completely determined up to isomorphism by its Cartan matrix.*

A convenient shorthand for Cartan matrices is given by the *Dynkin diagram.* This is a graph with vertices labelled by $\alpha_1, \dots, \alpha_\ell$. There are $a_{i,j}a_{j,i}$ edges joining vertices α_i and α_j, with an arrow pointing towards α_i if $(\alpha_i, \alpha_i) < (\alpha_j, \alpha_j)$ Clearly you can recover the Cartan matrix from the Dynkin diagram given properties (C1)–(C3) above.

Now I can state the classification of root systems:

Theorem 13.1.2 *The Dynkin diagrams of the indecomposable root systems are as given in Figure 13.1.*

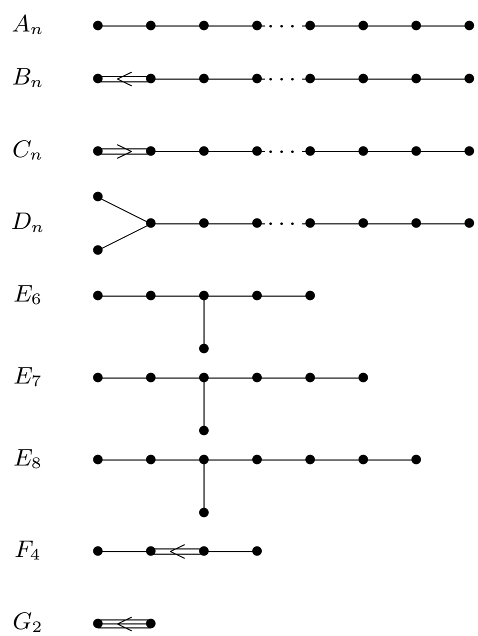

Fig. 13.1. Dynkin diagrams of semisimple Lie algebras

13.2 Semisimple Lie algebras

Now we sketch how the semisimple Lie algebras are classified by the root systems. We need to start with a semisimple Lie algebra and build a root system out of it, and vice versa.

So we begin with a finite dimensional semisimple Lie algebra $\mathfrak{g}$ over $\mathbb{C}$. Then $\mathfrak{g}$ possesses a *non-degenerate invariant* symmetric bilinear form $(.,.)$, where invariant here means $([X,Y],Z) = (X,[Y,Z])$ (in fact, the converse is also true). Moreover, if $\mathfrak{g}$ is simple, there is a unique such form up to a scalar. There is a "canonical" choice of non-degenerate form, the Killing form, but we don't need that here.

Example 13.2.1 Let us consider $\mathfrak{sl}_n$. The bilinear form $(X,Y) = \mathrm{tr}(XY)$ is non-degenerate and invariant. Let $e_{i,j}$ be the ij-matrix unit and let $\mathfrak{h}$ be the diagonal, trace zero matrices. We can decompose

$$\mathfrak{sl}_n = \mathfrak{h} \oplus \bigoplus_{i \neq j} \mathbb{C} e_{i,j}.$$

A basis for $\mathfrak{h}$ is given by $h_1, \ldots, h_{n-1}$ where $h_i = e_{i,i} - e_{i+1,i+1}$. Let

$\varepsilon_i \in \mathfrak{h}^*$ be the map sending a diagonal matrix to its ith diagonal entry. Note $\varepsilon_1 + \cdots + \varepsilon_n = 0$, i.e. the ε_i's are not independent. Then for any $H \in \mathfrak{h}$ we have

$$[H, e_{i,j}] = (\varepsilon_i - \varepsilon_j)(H)e_{i,j},$$

i.e. $e_{i,j}$ is a simultaneous eigenvector for $\mathfrak{h}$. We use the word *weight* in place of eigenvalue, so $e_{i,j}$ is a vector of *weight* $\varepsilon_i - \varepsilon_j$. Now you recall that the root system of type A_{n-1} can be defined as the real vector subspace of $\mathfrak{h}^*$ spanned by $\varepsilon_1, \ldots, \varepsilon_n$, and the roots are

$$\Phi := \{\varepsilon_i - \varepsilon_j \mid i \neq j\}.$$

A base for Φ is given by by $\alpha_1, \ldots, \alpha_{n-1}$ where $\alpha_i = \varepsilon_i - \varepsilon_{i+1}$. Let us finally write $\mathfrak{g}_\alpha := \mathbb{C}e_{i,j}$ if $\alpha = \varepsilon_i - \varepsilon_j$, i.e. the weight space of $\mathfrak{g}$ of weight $\varepsilon_i - \varepsilon_j$. Then

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{g}_\alpha.$$

In other words, you "see" the root system of type A_{n-1} when you decompose $\mathfrak{g}$ into weight spaces with respect to the diagonal matrices. Final note: the inner product giving the Euclidean space structure is induced by the non-degenerate form defined to start with. Indeed if you compute the matrix (h_i, h_j) you get back the Cartan matrix of type A_{n-1}.

This example is more or less how things go in general, when you start with an arbitrary semisimple Lie algebra $\mathfrak{g}$, with a non-degenerate invariant form $(.,.)$. The first step is to develop in $\mathfrak{g}$ a theory of Jordan decompositions. This parallels the Jordan decomposition we proved for algebraic groups. You call an element X of $\mathfrak{g}$ *semisimple* if the linear map $\operatorname{ad} X : \mathfrak{g} \to \mathfrak{g}$ is diagonalizable, and *nilpotent* if $\operatorname{ad} X$ is nilpotent. The *abstract Jordan decomposition* shows that any $X \in \mathfrak{g}$ decomposes uniquely as $X = X_s + X_n$ where $X_s \in \mathfrak{g}$ is semisimple and $X_n \in \mathfrak{g}$ is nilpotent, and $[X_s, X_n] = 0$.

What is more, if you have a *representation of* $\mathfrak{g}$, i.e. a Lie algebra homomorphism $\rho : \mathfrak{g} \to \mathfrak{gl}_n$, it is true that $\rho(X_s) = \rho(X)_s$ and $\rho(X_n) = \rho(X)_n$, where the semisimple and nilpotent parts on the right hand side are taken just as $n \times n$ matrices in $\mathfrak{gl}_n$. Thus, the abstract Jordan decomposition is consistent with all other Jordan decompositions arising from all other representations. In particular, semisimple elements of $\mathfrak{g}$ map to diagonalizable matrices under any matrix representation of $\mathfrak{g}$. For $\mathfrak{sl}_n$, $e_{i,j}$ is nilpotent for $i \neq j$, and $e_{i,i} - e_{i,j}$ is semisimple.

Now you introduce the notion of a *maximal toral subalgebra* or *Cartan* *subalgebra* $\mathfrak{h}$ of $\mathfrak{g}$ (in general maximal toral subalgebra and Cartan subalgebra are different notions but they agree for semisimple algebras). This is a maximal abelian subalgebra all of whose elements are semisimple. It turns out that in a semisimple Lie algebra, maximal toral subalgebras are non-zero, and they are all conjugate under automorphisms of $\mathfrak{g}$. Now fix one – it doesn't really matter which, since they are all conjugate. Importantly, the restriction of the invariant form $(.,.)$ on $\mathfrak{g}$ to $\mathfrak{h}$ is still non-degenerate. So we can define a map

$$\mathfrak{h}^* \to \mathfrak{h}$$

mapping $\alpha \in \mathfrak{h}^*$ to $t_\alpha \in \mathfrak{h}$, where t_α is the unique element satisfying $(t_\alpha, h) = \alpha(h)$ for all $h \in \mathfrak{h}$. Now we can lift the non-degenerate form on $\mathfrak{h}$ to $\mathfrak{h}^*$ by defining $(\alpha, \beta) = (t_\alpha, t_\beta)$. Thus, $\mathfrak{h}^*$ now has a non-degenerate symmetric bilinear form on it too.

For $\alpha \in \mathfrak{h}^*$, define

$$\mathfrak{g}_\alpha = \{X \in \mathfrak{g} \mid [H, X] = \alpha(H)X \text{ for all } H \in \mathfrak{g}\}.$$

Clearly, $\mathfrak{g} = \bigoplus_{\alpha \in \mathfrak{h}^*} \mathfrak{g}_\alpha$. Set $\Phi = \{0 \neq \alpha \in \mathfrak{h}^* \mid \mathfrak{g}_\alpha \neq 0\}$. Then you get *Cartan decomposition of* $\mathfrak{g}$:

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{g}_\alpha$$

(it is not obvious that the right hand side is everything...). It turns out with some work that each of the $\mathfrak{g}_\alpha$ spaces are *one-dimensional*.

Now you can build a root system out of $\mathfrak{g}$: we've already constructed the set Φ. Let E be the real vector subspace of $\mathfrak{h}^*$ spanned by Φ. The restriction of the form on $\mathfrak{h}^*$ to E turns out to be real valued only, and makes E into a Euclidean space. Now:

Theorem 13.2.2 *The pair (E, Φ) just built out of $\mathfrak{g}$ (starting from a choice of $\mathfrak{h}$) is a root system. Moreover, the resulting map from semisimple Lie algebras to Dynkin diagrams gives a bijection between isomorphism classes of semisimple Lie algebras and Dynkin diagrams. The decomposition of a semisimple Lie algebra as a direct sum of simples corresponds to the decomposition of the Dynkin diagram into indecomposable components.*

For example, $\mathfrak{sl}_n$ is the *simple* Lie algebra corresponding to the Dynkin diagram A_{n-1}.

13.3 Construction of simple Lie algebras

We now explain how to construct the simply-laced simple Lie algebras. So let (E, Φ) be a root system of type A_ℓ, D_ℓ or E_ℓ, $\pi = \{\alpha_1, \ldots, \alpha_\ell\}$ be a base and Φ^+ the corresponding set of positive roots. We may assume that $(\alpha, \alpha) = 2$ for all $\alpha \in \Phi$, as all roots have the same length. Let $Q = \mathbb{Z}\Phi \subset E$ be the *root lattice*, the free abelian group on basis Π.

We construct an asymmetry function

$$\varepsilon : Q \times Q \to \{\pm 1\}$$

such that

(1) ε is bilinear, i.e. $\varepsilon(\alpha + \alpha', \beta) = \varepsilon(\alpha, \beta)\varepsilon(\alpha', \beta)$ and $\varepsilon(\alpha, \beta + \beta') = \varepsilon(\alpha, \beta)\varepsilon(\alpha, \beta')$ for all $\alpha, \alpha', \beta, \beta' \in Q$.
(2) $\varepsilon(\alpha, \alpha) = (-1)^{(\alpha,\alpha)/2}$ for all $\alpha \in Q$.

Note (2) implies

(3) $\varepsilon(\alpha, \beta)\varepsilon(\beta, \alpha) = (-1)^{(\alpha,\beta)}$ for all $\alpha, \beta \in Q$.

To construct such an ε, it suffices by bilinearity to define it on elements of Π. Choose an orientation of the Dynkin diagram. Then define

$$\varepsilon(\alpha_i, \alpha_j) = \begin{cases} 1 & \text{if } \alpha_i \text{ and } \alpha_j \text{ are not connected,} \\ 1 & \text{if } \alpha_i \to \alpha_j, \\ -1 & \text{if } \alpha_i \leftarrow \alpha_j, \\ -1 & \text{if } \alpha_i = \alpha_j. \end{cases}$$

Now we can construct $\mathfrak{g}$. Let $\mathfrak{h}^* = \mathbb{C} \otimes_{\mathbb{Z}} Q = \mathbb{C} \otimes_{\mathbb{R}} E$. Let $\mathfrak{h}$ be the dual space, and let $H_\alpha \in \mathfrak{h}$ be the element such that $\beta(H_\alpha) = (\beta, \alpha)$ for all $\beta \in \mathfrak{h}^*$. Then, $H_1, \ldots, H_\ell$ gives a basis for $\mathfrak{h}$, where $H_i = H_{\alpha_i}$.

Now let

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in \Phi} \mathbb{C} E_\alpha$$

as a vector space. Define a multiplication by the formulae

$$\begin{aligned} [H_i, H_j] &= 0, \\ [H_i, E_\alpha] &= \alpha(H_i)E_\alpha = (\alpha_i, \alpha)E_\alpha, \\ [E_\alpha, E_{-\alpha}] &= -H_\alpha, \\ [E_\alpha, E_\beta] &= 0 \text{ if } \alpha + \beta \notin \varphi \cup \{0\}, \\ [E_\alpha, E_\beta] &= \varepsilon(\alpha, \beta)E_{\alpha+\beta} \text{ if } \alpha + \beta \in \Phi. \end{aligned}$$

Theorem 13.3.1 *$\mathfrak{g}$ is the simple Lie algebra of type Φ, with maximal toral subalgebra $\mathfrak{h}$.*

Proof You of course have to check that $\mathfrak{g}$ is a Lie algebra, which boils down to checking that the Jacobi identity is satisfied. This is a case analysis.

Having done that, we define a bilinear form on $\mathfrak{g}$ by

$$(H_i, H_j) = (\alpha_i, \alpha_j), (H_i, E_\alpha) = 0, (E_\alpha, E_\beta) = -\delta_{\alpha,-\beta}.$$

You check that this is a non-degenerate invariant bilinear form. Moreover, $\mathfrak{h}$ is a toral subalgebra of $\mathfrak{g}$, and since the 0-weight space of $\mathfrak{h}$ on $\mathfrak{g}$ is just $\mathfrak{h}$ itself, it must be maximal. Finally, it is automatic that the corresponding root system is of type Φ. Hence, $\mathfrak{g}$ is simple of type Φ with maximal toral subalgebra $\mathfrak{h}$. $\square$

Definition 13.3.2 Let $\mathfrak{g}$ be an arbitrary semisimple Lie algebra (not necessarily simply-laced). Let Φ be a root system corresponding to a choice of maximal toral subalgebra $\mathfrak{h}$, and let $\Pi = \{\alpha_1, \ldots, \alpha_\ell\}$ be a base for Φ. For $\alpha, \beta \in \Phi$, the *α-string through β* is the sequence

$$\beta - r\alpha, \ldots, \beta, \ldots, \beta + q\alpha$$

where r and s are the maximal integers such that all the vectors in the string belong to Φ. It turns out that r and q are equal to $0, 1$, 2 or 3 in all cases, and 2 and 3 don't arise if the root system is simply-laced.

Denote $H_\alpha := 2t_\alpha/(\alpha, \alpha)$ and $H_i := H_{\alpha_i}$. A *Chevalley basis* for $\mathfrak{g}$ means a basis

$$\{H_1, \ldots, H_\ell\} \cup \{X_\alpha \mid \alpha \in \Phi\}$$

such that

(a) $[H_i, H_j] = 0$,
(b) $[H_i, X_\alpha] = (\alpha, \alpha_i^\vee)X_\alpha$,
(c) $[X_\alpha, X_{-\alpha}] = H_\alpha$, and this is a $\mathbb{Z}$-linear combination of $H_1, \ldots, H_\ell$,
(d) If $\alpha, \beta, \alpha + \beta \in \Phi$ and $\beta - r\alpha, \ldots, \beta + q\alpha$ is the α-string through β, then $[X_\alpha, X_\beta] = N_{\alpha,\beta}X_{\alpha+\beta} = \pm(r + 1)X_{\alpha+\beta}$.

The key thing is that all the structure constants in a Chevalley basis are *integers*!

Theorem 13.3.3 (Chevalley) *Chevalley bases exist.*

Proof If Φ is simply-laced, this is easy from the above construction: take $X_\alpha = E_\alpha$ if $\alpha \in \Phi^+$ and $-E_\alpha$ is $\alpha \in \Phi^-$. Now you easily check this satisfies the properties. If Φ is not simply-laced, we need some other construction. For classical Lie algebras that is not too hard: you can write them down just as explicitly as $\mathfrak{sl}_n$. Problem 13.6.4 gives an example of how you do this. Another way is to realize all the non-simply-laced root systems as fixed points of automorphisms of simple-laced ones. $\square$

13.4 Kostant $\mathbb{Z}$-form

Informally speaking, Chevalley group is constructed from a semisimple Lie algebra $\mathfrak{g}$ as the group generated by the 'exponents' of the form $\exp(tX_\alpha)$ where X_α is a root element of the Lie algebra and t is a scalar. But there are some problems here. Consider, for example

$$\exp(X_\alpha) = 1 + X_\alpha + X_\alpha^2/2! + X_\alpha^3/3! + \dots$$

What does that mean? We don't have a toplogy to speak of convergence, so we need to make sure that the sum is finite. Well, this will be achieved if X_α is nilpotent in a certain sense. Further, what does X_α^3 mean? We can't multiply in a Lie algebra! However we can consider this as an element of the universal enveloping algebra. There is a further problem however. If characteristic is 2 or 3, we can't make sense of the division by 3!. The solution to this is very clever—we will first divide by 3! and then pass to characteristic p!! More formally, we will consider a $\mathbb{Z}$-form $U_\mathbb{Z}$ of the universal enveloping algebra U of $\mathfrak{g}$ which contains all $X_\alpha^n/n!$ and then pass to the algebra $U = U_k := U_\mathbb{Z} \otimes_\mathbb{Z} k$, called the *hyperalgebra*.

First, recall the universal enveloping algebra $U(\mathfrak{g})$ associated to a Lie algebra $\mathfrak{g}$. It is defined by a universal property, but there is also an explicit construction. The all-important PBW theorem shows that we can identify $\mathfrak{g}$ with a Lie subalgebra of $U(\mathfrak{g})$, and moreover if $X_1, \dots, X_N$ is a basis for $\mathfrak{g}$, then the monomials

$$X_1^{r_1} \dots X_N^{r_n}$$

give a basis for $U(\mathfrak{g})$.

One reason $U(\mathfrak{g})$ is important is because it allows you to view representations, i.e. Lie algebra homomorphisms $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$, as $U(\mathfrak{g})$-modules:

Lemma 13.4.1 *The categories of representations of $\mathfrak{g}$ and of $U(\mathfrak{g})$-modules are isomorphic.*

Proof Let $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$ be a representation. Viewing $\mathfrak{gl}(V)$ as $\operatorname{End}(V)$, we get induced a unique associative algebra homomorphism $\hat{\rho} : U(\mathfrak{g}) \to \operatorname{End}(V)$. Using this, we make V into a $U(\mathfrak{g})$-module by $u.v = \hat{\rho}(u)(v)$. If you think about it, this gives a functor $\{$representations of $\mathfrak{g}\} \to \{U(\mathfrak{g})$-modules$\}$. Conversely, given a $U(\mathfrak{g})$-module, define $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$ by $\rho(X)(v) := Xv$. This defines an inverse functor. $\square$

Now we state the main result about the Kostant $\mathbb{Z}$-form.

Theorem 13.4.2 *Let $\mathfrak{g}$ be a semisimple Lie algebra over $\mathbb{C}$, with Chevalley basis $\{H_1, \ldots, H_\ell\} \cup \{X_\alpha \mid \alpha \in \Phi\}$. Let $U_{\mathbb{Z}}$ be the $\mathbb{Z}$-subalgebra of $U(\mathfrak{g})$ generated by the $X_\alpha^r/r!$ for all $\alpha \in \Pi, r \geq 1$. Then, $U_{\mathbb{Z}}$ is free as a $\mathbb{Z}$-module with basis given by all monomials in the*

$$X_\alpha^{r_\alpha}/|r_\alpha! \ (\alpha \in \Phi), \qquad \binom{H_i}{m_i} \ (i = 1, \ldots, \ell)$$

in some fixed order, where $m_i, r_\alpha \geq 0$.

Proof (1) Observe all the "Kostant monomials" form a $\mathbb{C}$-basis for $U(\mathfrak{g})$ by the PBW theorem, so they are linearly independent.

(2) Observe all $X_\alpha^{(r)}$ and all $\binom{H_i}{m_i}$ belong to $U_{\mathbb{Z}}$ – by constructing them as various commutators of the generators of $U_{\mathbb{Z}}$. Hence all Kostant monomials belong to $U_{\mathbb{Z}}$.

(3) Prove that the product of two Kostant monomials can be expanded as a $\mathbb{Z}$-linear combination of other Kostant monomials. Hence they span $U_{\mathbb{Z}}$. This is done by proving various commutation relations. $\square$

13.5 Weights and representations

Let $Q = \mathbb{Z}\Phi \subset \mathfrak{h}^*$ be the root lattice. Let P be the *weight lattice*, defined as

$$P = \{\lambda \in \mathfrak{h}^* \mid \lambda(H_i) \in \mathbb{Z} \text{ for all } i = 1, \ldots, \ell\}.$$

Thus P is the lattice dual to the lattice $\mathbb{Z}H_1 + \cdots + \mathbb{Z}H_\ell$ in $\mathfrak{h}$. Obviously, $Q \subseteq P$. Moreover, since P and Q are both lattices in $\mathfrak{h}^*$, i.e. they are both finitely generated abelian groups that span $\mathfrak{h}^*$ over $\mathbb{C}$, the quotient

P/Q is a finitely generated, torsion abelian group. But that implies P/Q is a finite abelian group. It is called the *fundamental group*.

To get a basis for P (as a free abelian group), one can take the *fundamental weights* $\omega_1, \dots, \omega_\ell$ defined by

$$\omega_i(H_j) = \delta_{i,j},$$

i.e. the dual basis to $H_1, \dots, H_\ell$. We claim that

$$\alpha_i = \sum_{j=1}^{\ell} a_{i,j}\omega_j$$

where $a_{i,j} = (\alpha_i, \alpha_j^\vee) = \alpha_i(H_j)$ is the Cartan integer. To see this, just evaluate both sides on H_j – you get the same thing. Thus, P/Q is the abelian group on generators $\bar{\omega}_1, \dots, \bar{\omega}_j$ subject to relations

$$\sum_{j=1}^{\ell} a_{i,j}\bar{\omega}_j = 0.$$

Considering elementary divisors, you get that

$$|P/Q| = \det A,$$

indeed, you get an explicit description of P/Q as an abelian group. These are the orders:

$$\begin{aligned} A_\ell &: \ell + 1 \\ B_\ell, C_\ell, E_7 &: 2 \\ D_\ell &: 4 \\ E_6 &: 3 \\ E_8, F_4, G_2 &: 1 \end{aligned}$$

In fact the fundamental group is cyclic in all cases except for D_ℓ with ℓ even, when it is $\mathbb{Z}/2 \times \mathbb{Z}/2$. This is going to be very important: we now know exactly all possible lattices lying between Q and P.

The last important ingredient that we need to construct the Chevalley groups is a little representation theory of semisimple Lie algebras. We are interested here just in the *finite dimensional* representations of $\mathfrak{g}$. A fundamental theorem of Weyl (mentioned before) shows that any finite dimensional representation of $\mathfrak{g}$ decomposes as a direct sum of irrducible representations, i.e. ones with no proper invariant submodules. So we really only need to discuss the finite dimensional irreducible representations.

Now, if V is a finite dimensional $U(\mathfrak{g})$-module, we can decompose

$$V = \bigoplus_{\lambda \in \mathfrak{h}^*} V_\lambda$$

where

$$V_\lambda = \{v \in V \mid Hv = \lambda(H)v \text{ for all } H \in \mathfrak{h}\}.$$

This is the *weight space decomposition* of V. For example, the Cartan decomposition of $\mathfrak{g}$ itself is the weight space decomposition of the adjoint representation. We will say that $v \in V$ is a *high weight vector* of *high weight* λ if $0 \neq v \in V_\lambda$ and $X_\alpha v = 0$ for all $\alpha \in \Phi^+$. It is obvious that any non-zero finite dimensional V possesses such a vector – because $X_\alpha V_\lambda \subseteq V_{\lambda+\alpha}$ and there are only finitely many non-zero weight spaces in total.

It turns out that the high weight vector of an irreducible representation of $\mathfrak{g}$ is unique up to a scalar and its weight belongs to the set

$$P^+ = \{\lambda \in P \mid \lambda(H_i) \geq 0 \text{ for each } i = 1, \ldots, \ell\}.$$

Conversely, for any element of P^+, there is a unique up to isomorphism irreducible representation of that highest weight.

Relation to $\mathbb{Z}$-forms is as follows:

Theorem 13.5.1 *Let $\lambda \in P^+$ and V be the corresponding irreducible highest weight representation. Then, there exists a lattice $V_\mathbb{Z}$ in V invariant under the action of the Kostant $\mathbb{Z}$-form $U_\mathbb{Z}$, such that*

$$V_\mathbb{Z} = \sum_{\mu \in \mathfrak{h}^*} V_{\mu,\mathbb{Z}}$$

where $V_{\mu,\mathbb{Z}} = V_\mu \cap V_\mathbb{Z}$.

Given any finite dimensional representation V, we consider its lattice $L(V)$, which is defined to be the subgroup of P generated by all λ such that $V_\lambda \neq 0$. If V is faithful, then $Q \subseteq L(V) \subseteq P$. In fact you can get any intermediate lattice arising for suitable choice of V, and the possible lattices are parametrized by the subgroups of the fundamental group.

13.6 Problems

Problem 13.6.1 Write down the explicit construction of the root systems of type A_ℓ, B_ℓ, C_ℓ and D_ℓ, and show that the length of the longest element w_0 of the Weyl group was $\ell(\ell+1)/2$. (*Hint:* You need to look it up! There are many good sources, e.g. Humphreys' "Introduction to Lie algebras and representation theory", Bourbaki "Groupes et Algebres de Lie", Kac "Infinite dimensional Lie algebras", Carter "Finite groups of Lie type", Helgason "Differential geometry and symmetric spaces"...)

Problem 13.6.2 Look up or work out the dimensions of the simple Lie algebras of types A_ℓ, B_ℓ, C_ℓ and D_ℓ. In particular, check that $\dim C_\ell$ is the same as the dimension of the algebraic group $Sp_{2\ell}$.

Problem 13.6.3 In the proof of Theorem 13.3.1, go through the details needed to verify that the bilinear form defined is *invariant*.

Problem 13.6.4 Let V be a $(2\ell+1)$-dimensional complex vector space with an ordered basis $e_1, \ldots, e_\ell, e_0, e_{-\ell}, \ldots, e_{-1}$. Define a symmetric bilinear form on V by declaring $(e_i, e_j) = 0$ $(i \neq -j)$, $(e_i, e_{-i}) = 1$ $(i \neq 0)$ and $(e_0, e_0) = 2$. Let J be the matrix of this bilinear form in the basis, ordering rows and columns as $e_1, \ldots, e_\ell, e_0, e_{-\ell}, \ldots, e_{-1}$.

(i) Compute the matrix J explicitly.

(ii) Let $\mathfrak{g} = \{X \in \mathfrak{gl}(V) \mid X^T J + JX = 0\}$ be the Lie algebra $\mathfrak{so}(V) = \mathfrak{so}(2\ell+1)$. Viewing elements of $\mathfrak{g}$ as block matrices in our ordered basis, we can write

$$X = \left(\begin{array}{c|c|c} A & v & B \\ \hline r & x & s \\ \hline C & w & D \end{array}\right).$$

Compute explicitly the conditions that the $\ell \times \ell$ matrices A, B, C, D, the column vectors v, w, the row vectors r, s and the scalar x must satisfy for X to belong to $\mathfrak{g}$.

(iii) Let $\mathfrak{h}$ be the set of all diagonal matrices in $\mathfrak{g}$. This is a toral subalgebra of $\mathfrak{g}$. Let $\epsilon_i \in \mathfrak{h}^*$ be the function

$$diag(t_1, \ldots, t_\ell, 0, -t_\ell, \ldots, -t_1) \mapsto t_i,$$

so that $\varepsilon_1, \ldots, \varepsilon_\ell$ form a basis for $\mathfrak{h}^*$. Let

$$\Phi = \{\pm\varepsilon_i \pm \varepsilon_j, \pm\varepsilon_k \mid 1 \leq i < j \leq \ell, 1 \leq k \leq \ell\},$$

the root system of type B_ℓ. Let $E_{i,j} : V \to V$ denote the linear map with $E_{i,j}.v_k = \delta_{jk} v_i$ for all $-\ell \leq i, j, k \leq \ell$. For $\alpha \in \Phi$, define

α	$\epsilon_i - \epsilon_j (i < j)$	$\epsilon_i + \epsilon_j (i < j)$	ϵ_i
X_α	$E_{i,j} - E_{-j,-i}$	$E_{j,-i} - E_{i,-j}$	$2E_{i,0} - E_{0,-i}$
$X_{-\alpha}$	$E_{j,i} - E_{-i,-j}$	$E_{-i,j} - E_{-j,i}$	$E_{0,i} - 2E_{-i,0}$

Verify that

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in \Phi} \mathbb{C} X_\alpha$$

is the Cartan decomposition of $\mathfrak{g}$.

(v) Defining $H_1, \ldots, H_\ell$ appropriately, check that $\{H_1, \ldots, H_\ell\} \cup \{X_\alpha | \alpha \in \Phi\}$ is a Chevalley basis for $\mathfrak{g}$.

14
The Chevalley construction

To motivate the construction, let's stick to working over $\mathbb{C}$ for a bit. Let $\mathfrak{g}$ be a semisimple Lie algebra, and let V be a finite dimensional faithful representation. So the lattice $L(V)$ is some intermediate lattice between Q and P (e.g. if V is the adjoint representation, $L(V) = Q$).

Let $\{H_i\} \cup \{X_\alpha\}$ be a Chevalley basis. Since V has only finitely many weight spaces and the X_α map V_μ into $V_{\mu+\alpha}$, each X_α acts on V nilpotently. Thus, we can consider the formal series

$$\exp(cX_\alpha) = 1 + cX_\alpha + c^2 X_\alpha^2/2! + \dots$$

for any scalar $c \in \mathbb{C}$ as a well-defined endomorphism of V (the infinite sum terminates...).

By familiar properties of exponential series,

$$\exp(cX_\alpha)\exp(dX_\alpha) = \exp((c+d)X_\alpha).$$

In particular, $\exp(cX_\alpha)$ is *invertible* with inverse $\exp(-cX_\alpha)$. Now let G be the subgroup of $GL(V)$ generated by all $\exp(cX_\alpha)$ for all $c \in \mathbb{C}$ and $\alpha \in \Phi$. This is the *Chevalley group* corresponding to $\mathfrak{g}$ in the representation V. It turns out that (up to isomorphism) G is determined by $\mathfrak{g}$ and the lattice $L(V)$.

Using $\mathbb{Z}$-forms we can imitate this construction over an arbitrary field k. In the case that k is an algebraically closed field, G is always a *semisimple algebraic group*, and in fact all semisimple algebraic groups arise out of this contstruction for some choice of Φ and $L(V)$.

In order to study the structure of G in detail, we construct closed subgroups U, T, B, N of G with explicitly named generators, and prove various relations between these generators. We will show that $B = U \rtimes T$ (semidirect product), that $T \lhd N$, and identify the quotient group N/T with the original Weyl group W.

Finally, we will prove the Bruhat decomposition:

$$G = \bigcup_{w \in W} BwB.$$

Here $w \in W$ needs to be interpreted as a fixed coset representative in N. Thus, the (B, B)-double cosets in G are parametrized by the Weyl group W.

14.1 Definition and first properties

To every field, every root system Φ and every lattice L such that $Q \subseteq L \subseteq P$ we associate the *Chevalley group* $G = G(k, \Phi, L)$ defined as follows. Let $U_{\mathbb{Z}}$ be the Kostant $\mathbb{Z}$-form of the universal enveloping algebra $U(\mathfrak{g})$ of the semisimple Lie algebra $\mathfrak{g}$ of type Φ, and $V_{\mathbb{C}}$ be a representation of $\mathfrak{g}$ with $L = L(V)$. Pick a $U_{\mathbb{Z}}$-invariant lattice $V_{\mathbb{Z}}$ in V as in Theorem 13.5.1. Let $V = V_{\mathbb{Z}} \otimes_{\mathbb{Z}} k$. Then for any $t \in k$ and $\alpha \in \Phi$,

$$x_\alpha(t) := \exp(tX_\alpha) = 1 + X_\alpha \otimes t + (X_\alpha^2/2!) \otimes t^2 + \ldots$$

can be considered as an invertible endomorphism of V. By definition, G is the group generated by all $x_\alpha(t)$ for $t \in k$ and $\alpha \in \Phi$.

The proof that the group only depends on L and not on the choice of $V_{\mathbb{C}}$ and $V_{\mathbb{Z}} \subset V_{\mathbb{C}}$ will be skipped.

For fixed $\alpha \in \Phi$, let $\mathcal{X}_\alpha$ be the subgroup of $GL(V)$ generated by all $x_\alpha(t)$ for all $t \in k$.

From now on we assume as usual that k is algebraically closed.

Theorem 14.1.1 *The group G is a closed connected subgroup of $GL(V)$.*

Proof Note that the map $\mathbb{G}_a \to GL(V),\ t \mapsto x_\alpha(t)$ is a morphism of algebraic groups, as the exponent stops after finitely many steps and so is "polynomial" in t. So each $\mathcal{X}_\alpha$ is a closed connected subgroup of $GL(V)$. Now use Corollary 8.2.7. □

The main goal of this course is to prove that: (a) G is a semisimple algebraic group and (b) every semisimple algebraic group is obtained in this way. You have probably already figured out that we are not going to get there by the end of the term but we will try to get as far as possible...

Concerning (a), it is a well known fact (often proved even in the 600 algebra courses) that $PSL_n(k)$ is simple as an abstract group (all you need for this is the assumption that k has more than 3 elements if $n = 2$, but remember that for us k is algebraically closed, so infinite). So if G is of type A, any of its solvable normal subgroups is contained in the center of G, which is finite. As the radical is connected, this proves that the radical of G is trivial. The proof for other types uses elements $x_\alpha(t)$ instead of transvections in the usual proof for PSL_n, and we will not reproduce it here.

15

Borel subgroups and flag varieties

In the previous chapter, we sketched the *construction* of the semisimple algebraic groups. It is very explicit and case-free. We will now go back to algebraic geometry and sketch the proof of the Classification Theorem. We will see that algebraic geometry, in particular the variety structure on quotient varieties G/H which we haven't really used yet in a deep way, is a fundamental tool to studying group theory.

15.1 Complete varieties and Borel's fixed point theorem

Recall the notion of the *complete* variety from chapter 7. We need the following:

Lemma 15.1.1 *Let G be an algebraic group acting transitively on varieties X, Y. Let $\varphi : X \to Y$ be a bijective, G-equivariant morphism. If Y is complete, then X is complete.*

Proof By Remark 7.1.3(ii), we need to show that $\pi_2 : X \times Z \to Z$ is closed for all affine varieties Z. Since Y is complete, it suffices to prove that $\varphi \times \mathrm{id} : X \times Z \to Y \times Z$ is closed. By Proposition 5.3.2, there are open subsets $U \subset X$ and $V \subset Y$ such that $\varphi(U) = V$ and $\varphi|U : U \to V$ is a finite morphism. Let R, S, T be the respective affine algebras of U, V, Z. Since R is integral over S, $R \otimes T$ is integral over $S \otimes T$. Therefore $\varphi \times \mathrm{id} : U \times Z \to V \times Z$ is also a finite morphism. In particular, it is a closed map, see Corollary 5.2.4. Because G acts transitively on X, Y and φ is G-equivariant, X (resp. Y) is covered by finitely many translates of the form xU (resp. xV) for some $x \in G$. It follows that $\varphi \times \mathrm{id} : X \times Z \to Y \times Z$ is closed. $\square$

Now we can prove the important

Theorem 15.1.2 (Borel's fixed point theorem) *Let G be a connected solvable algebraic group, and X be a non-empty complete G-variety. Then G has a fixed point on X.*

Proof Proceed by induction on $\dim G$, the case $G = \{1\}$ being trivial. Suppose then that $\dim G > 0$ and let $H = G'$, which is connected solvable of strictly smaller dimension. By induction,

$$Y = \{x \in X \mid Hx = x\}$$

is non-empty. By Lemma 8.3.1(iii), Y is closed, hence complete, and G stabilizes Y as $H \lhd G$. So we may as well replace X by Y to assume that $H \subseteq G_x$ for all $x \in X$. Since G/H is abelian, this implies that each $G_x \trianglelefteq G$.

Now choose x so that the orbit $G \cdot x$ is of minimal dimension. Then, $G \cdot x$ is closed hence complete. The map $G/G_x \to G.x$ is bijective, so we deduce that G/G_x is complete by the preceeding lemma. But G/G_x is affine as $G_x \trianglelefteq G$. So in fact G/G_x is a point, i.e. $G = G_x$ and x is a fixed point. □

Corollary 15.1.3 (Lie-Kolchin theorem) *Let G be a connected solvable subgroup of $GL(V)$. Then G fixes a flag in V.*

Proof Let G act on the flag variety $\mathcal{F}(V)$. This is projective, so G has a fixed point. □

15.2 Borel subgroups

Let G be a connected algebraic group.

Definition 15.2.1 A Borel subgroup B of G is a *maximal* closed connected solvable subgroup of G.

Example 15.2.2 (i) If G is a Chevalley group, the subgroup $B = TU$ is a Borel subgroup of G. Any conjugate of B in G will give another such subgroup.

(ii) If $G = GL_n$, the subgroup B of all upper triangular matrices is a maximal closed connected solvable subgroup by the Lie-Kolchin theorem. Hence, it is a Borel subgroup. Any conjugate of this will give another. Note in this case that the quotient variety G/B is the flag variety, so it is a projective variety in particular.

Theorem 15.2.3 *For any connected algebraic group G, let B be a Borel subgroup. Then, G/B is a projective variety, and all other Borel subgroups of G are conjugate to B.*

Proof Let S be a a Borel subgroup of maximal dimension. Apply Chevalley's theorem to construct a representation $\rho : G \to GL(V)$ and a 1-space $L \subset V$ such that $S = \mathrm{Stab}_G(L)$. By the Lie-Kolchin theorem, S fixes a flag in V/L. Hence S fixes a flag $F = (L = L_1 \subset L_2 \subset \cdots \subset L_n = V)$ in the flag variety $\mathcal{F}(V)$. Recall this is a projective variety, hence it is complete.

By the choice of L, $S = \mathrm{Stab}_G(F)$. Hence the orbit map induces a bijective morphism $G/S \to G \cdot F \subset \mathcal{F}(V)$. Take any other flag $F' \in \mathcal{F}(V)$. Then $\mathrm{Stab}_G(F')$ is upper triangular in some basis, hence it is solvable, hence its dimension is $\leq \dim S$. This shows that $\dim G \cdot F' = \dim G - \dim \mathrm{Stab}_G(F') \geq \dim G \cdot F$. Therefore, $G \cdot F$ is a G-orbit in $\mathcal{F}(V)$ of minimal dimension, hence it is closed. This shows that $G \cdot F$ is also complete, so G/S is complete too. Now G/S is complete and its quasi-projective, hence it is projective.

Finally, let B be another Borel subgroup of G. Then B acts on G/S, so by Borel's fixed point theorem, B has a fixed point gS on G/S. Therefore $BgS = gS$, i.e. $g^{-1}Bg \subseteq S$. By maximality, we get that $g^{-1}Bg = S$ and this completes the proof. □

Definition 15.2.4 A *parabolic subgroup* P of G is any closed subgroup of G such that G/P is a projective (equivalently, complete) variety.

Theorem 15.2.5 *Let P be a closed subgroup of G. Then, P is parabolic if and only if it contains a Borel subgroup. In particular, P is a Borel subgroup if and only if P is connected solvable and G/P is a projective variety.*

Proof Suppose G/P is projective. Let B be a Borel subgroup of G. It acts on G/P with a fixed point, say $BgP = gP$. This implies that $g^{-1}Bg \subseteq P$, i.e. P contains a Borel subgroup.

Conversely, suppose P contains a Borel subgroup B. The map $G/B \to G/P$ is surjective and G/B is complete. Hence, G/P is complete too. But it is quasi-projective too, so in fact G/P is projective. □

Example 15.2.6 (i) Let $G = GL_n$. The subgroups of G containing B (upper triangular matrices) are exactly the "step" subgroups, one for each way of writing $n = n_1 + \cdots + n_s$ as a sum of positive integers $n_1, \ldots, n_s$. There are 2^{n-1} such subgroups.

(ii) Let G be an arbitrary Chevalley group. Let S be a subset of the simple roots Π, so there are 2^ℓ possibilities for S. Let P be the subgroup of G generated by B and all s_α for $\alpha \in S$. (Equivalently, P is the subgroup generated by T and the $\mathcal{X}_\alpha$'s for $\alpha \in \Phi^+ \cup (-S)$.) Then, P contains B so it is a parabolic subgroup by the theorem, and G/P is a projective variety. In fact, these P's give *all* the parabolic subgroups of G containing the fixed choice of Borel subgroup B. By the theorem, all other parabolic subgroups of G are conjugate to one of these. There are exactly 2^ℓ different conjugacy classes of parabolic subgroup in the Chevalley group G.

15.3 The Bruhat order

Let G be a Chevalley group, with all the subgroups $U, T, X_\alpha, B, N, W = N/T, \ldots$. Recall also that W is generated by the simple reflections $\{s_\alpha \mid \alpha \in \Pi\}$. For any $w \in W$, we can write w as a product of simple reflections. The *length* of w was the length of a shortest such expression, called a *reduced expression* for W.

Let me define a partial order on W as follows. Take $w, w' \in W$. Let $w = s_1 \ldots s_r$ be a reduced expression for w. Declare that $w' \leq w$ if and only if $w' = s_{i_1} \ldots s_{i_j}$ for some $1 \leq i_1 < \cdots < i_j \leq r$, i.e. if w' is a "subexpression" of w. How do you prove this really is a partial order? How do you even show that it is well-defined, i.e. independent of the choice of the reduced expression of w? One of the ways is to use algebraic geometry!

By the Bruhat decomposition, the B-orbits on G/B are parametrized by the Weyl group W, i.e. the orbits are the BwB/B's. Now, the closure of an orbit is a union of orbits, the ones in the boundary being of strictly smaller dimension. So there is obviously a partial ordering $\leq$ on the orbits of B on G/B defined by $\mathcal{O} \leq \mathcal{O}'$ if and only if $\mathcal{O} \subseteq \overline{\mathcal{O}'}$. What we are going to prove is that this is exactly the partial ordering defined in the previous paragraph! In other words, the ordering in the previous paragraph IS well-defined because there is a geometrically defined partial ordering that amounts to the combinatorics there.

Let's proceed with some lemmas.

Lemma 15.3.1 *Let G be an algebraic group, X a G-variety, $H \leq G$ a closed subgroup and $Y \subseteq X$ a closed H-stable subvariety of X. If G/H is a complete variety (i.e. if H is a parabolic subgroup of G) then $G \cdot Y$ is closed in X.*

Proof Let $A = \{(g, x) \in G \times X \mid g^{-1}x \in Y\}$, which is closed in $G \times X$. Let

$$\pi : G \times X \to G/H \times X$$

be the quotient map. Recall this is an open map. If $(g, x) \in A$ then $(gh, x) \in A$ for all $h \in H$, since H stabilizes Y. Hence,

$$\pi(A) = G/H \times X - \pi(G \times X - A),$$

so $\pi(A)$ is closed in $G/H \times X$. Since G/H is complete, the projection $pr_X(\pi(A)) \subseteq X$ is also closed. This is exactly $G \cdot Y$. □

Lemma 15.3.2 *Any product of parabolic subgroups of G containing B is closed in G.*

Proof Let $P_1, \ldots, P_r$ be parabolic subgroups of G containing B. By induction, $P_2 \ldots P_r$ is closed in G and B-stable. Note $P_2 \ldots P_r.B = P_1 \ldots P_{r-1}$ is closed and B-stable. Since P_1/B is complete, we get by the lemma that $P_1 P_2 \ldots P_r$ is closed too. □

Theorem 15.3.3 (Chevalley) *Let G be a Chevalley group. Fix $w \in W$ and a reduced expression $w = s_1 \ldots s_r$ for w as a product of simple reflections. Then,*

$$\overline{BwB} = \bigcup_{w'} Bw'B$$

where w' runs over all subexpressions $s_{i_1} \ldots s_{i_j}$ of $s_1 \ldots s_r$.

Proof Let $w = s_1 \ldots s_r$ be the fixed reduced expression for w, Let

$$P_i = \langle B, s_i \rangle = B \cup Bs_iB,$$

where the last equality comes from the work on Chevalley groups in the previous chapter. We show by induction on r that

$$P_1 \ldots P_r = \bigcup_{w'} Bw'B$$

where the union is taken over all subexpressions w' of the reduced expression $s_1 \dots s_r$. The case $r = 1$ is already done!

Now suppose $r > 1$. Then by induction,

$$P_1 \dots P_r = \bigcup_{w''} Bw''B.(B \cup B_{s_r} B)$$

where w'' runs over all subexpressions of $s_1 \dots s_{r-1}$. But that equals

$$\bigcup_{w'} B_{w'} B$$

as required, since $Bw''s_rB \subseteq Bw''BB_{s_r}B \subseteq Bw''B \cup Bw''s_rB$ by the previous chapter.

By the preceeding lemma, $P_1 \dots P_r$ is closed, hence

$$\bigcup_{w'} Bw'B,$$

union over all subexpressions w' of $s_1 \dots s_r$, is closed. So it certainly contains the closure $\overline{BwB}$. Finally, we know $\dim BwB$ is equal to $\dim B+$ the number of positive roots sent to negative roots by w. So in fact we must have that

$$\bigcup_{w'} Bw'B = \overline{BwB}$$

by dimension. □

Now since $\overline{BwB}$ is defined intrinsically independent of any choice of reduced expression of w, the relation $w' \leq w$ iff w' is a subexpression of some fixed reduced expression for w is well-defined independent of the choice. Moreover, it is a partial ordering on W called the *Bruhat ordering*.

For $w \in W$, the *Schubert variety*

$$X_w := \overline{BwB}/B$$

is a closed subvariety of the flag variety G/B. Note X_w is no longer an orbit of an algebraic group, so it needn't be smooth. Schubert varieties are extremely interesting projective varieties with many wonderful properties. The Schubert variety X_{w_0} is the flag variety itself, the Schubert variety X_1 is a point. We have shown above that in general, the lattice of containments of Schubert varieties is isomorphic to the Bruhat order on W.

16
The classification of reductive algebraic groups

16.1 Maximal tori and the root system

Now we sketch the procedure to build a root system starting from an arbitrary reductive algebraic group. This is the first step in proving the classiciation of reductive algebraic groups.

Let us start by talking about *tori*. Recall an n-dimensional torus is an algebraic group isomorphic to $\mathbb{G}_m \times \cdots \times \mathbb{G}_m$. For example, the subgroup D_n of GL_n consisting of all diagonal matrices is an n dimensional torus. Let T be an n-dimensional torus. The character group

$$X(T) = \mathrm{Hom}(T, \mathbb{G}_m) \cong \mathrm{Hom}(\mathbb{G}_m, \mathbb{G}_m)^{\oplus n} \cong \mathbb{Z}^n.$$

An important point is that, given any two tori T and T',

$$\mathrm{Hom}(T, T') \cong \mathrm{Hom}(X(T'), X(T)).$$

So any homomorphism $f : X(T') \to X(T)$ of abelian groups induces a unique morphism $T \to T'$ of algebraic groups, and vice versa. In fact, you can view $X(?)$ as a contravariant equivalence of categories between the category of tori and the category of finitely generated free abelian groups.

All elements of a torus T are semisimple. So if V is any finite dimensional representation of T, every element of T is diagonalizable in its action on V by the Jordan decomposition. Moreover, they commute, hence we can actually diagonalize

$$V = \bigoplus_{\lambda \in X(T)} V_\lambda$$

where

$$V_\lambda = \{v \in V \mid tv = \lambda(t)v \text{ for all } t \in T\}.$$

As before, the V_λ's are called the *weight spaces* of V with respect to the torus T.

Now let G be an arbitrary connected algebraic group. A *maximal torus* of G is what you'd think: a closed subgroup T that is maximal subject to being a torus. Let me state some theorems about maximal tori in connected solvable groups. These are proved by induction, though it is often quite difficult...

Theorem 16.1.1 *Let G be a connected solvable group. Then, the set G_u of all unipotent elements of G is a closed connected normal subgroup of G. All the maximal tori of G are conjugate, and if T is any one of them, then G is the semi-direct product of T acting on G_u.*

As a consequence, you show that in an arbitrary connected group G, all its maximal tori are conjugate. Indeed, any maximal torus T of G is contained in a Borel subgroup B. If T' is another maximal torus, contained in a Borel B', we can conjugate B' to B to assume that T' is also contained in B. But then T and T' are conjugate in B by the theorem.

Now start to assume that G is a reductive algebraic group. Let T be a maximal torus. Let $\mathfrak{g}$ be the Lie algebra of G. We can view $\mathfrak{g}$ as a representation of T via the adjoint action. It turns out moreover – using for the first time that G is reductive – that the zero weight space of $\mathfrak{g}$ with respect to T is exactly the Lie algebra $\mathfrak{t}$ of T itself. So we can decompose

$$\mathfrak{g} = \mathfrak{t} \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{g}_\alpha$$

where Φ is the set of all $0 \neq \alpha \in X(T)$ such that the T-weight space $\mathfrak{g}_\alpha \neq 0$. You can already see the root system emerging... The difference now however is that the set Φ of roots is a subset of the free abelian group $X(T)$. Now using the assumption that G is reductive again, you show:

(1) Each $\mathfrak{g}_\alpha$ is one dimensional, and $\alpha \in \Phi$ iff $-\alpha \in \Phi$.
(2) The group $W = N_G(T)/T$ is a finite group that acts naturally on $X(T)$ and permutes the subset $\Phi \subseteq X(T)$.
(3) Let Q be the *root lattice*, the subgroup of $X(T)$ generated by Φ, and let $E = \mathbb{R} \otimes_{\mathbb{Z}} Q$. Fix a positive definite inner product on E that is invariant under the action of W. Then, (E, Φ) is an abstract root system.

(4) If we embed T into a Borel subgroup B, we get a choice Φ^+ of positive roots defined by $\alpha \in \Phi^+$ iff $\mathfrak{g}_\alpha \subset \mathfrak{b}$. Conversely, any choice Φ^+ of positive roots determines a unique Borel subgroup of G containing T.

We've now built out of G a root system (E, Φ), and realized the Weyl group W explicitly as the quotient group $N_G(T)/T$. Moreover, Φ is a subset of the character group $X(T)$ of T.

If G is semisimple, then G is determined up to isomorphism by its root system (E, Φ) together with the extra information given by the fundamental group $X(T)/Q$. In the next section, we will see a more natural setup which classifies the *reductive*, not just semisimple, groups. This is harder, since $X(T)$ will in general be of bigger rank than Q, and so there is much more freedom not captured by the fundamental group alone. For GL_n, $X(T)$ is a free abelian group of rank n, whereas Q is of rank $(n-1)$.

16.2 Sketch of the classification

Finally let's prepare the way to state the classification of reductive algebraic groups in general. Let G be a reductive algebraic group, and let T be a maximal torus. Let $\Phi \subset X(T)$ be the root system of G, defined from the decomposition

$$\mathfrak{g} = \mathfrak{t} \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{g}_\alpha.$$

Let

$$X(T) = \mathrm{Hom}(T, \mathbb{G}_m)$$

be the *character group* of T, and let

$$Y(T) = \mathrm{Hom}(\mathbb{G}_m, T)$$

be the *cocharacter group*. This is also a free abelian group of rank $\dim T$. Moreover, there is a pairing

$$X(T) \times Y(T) \to \mathbb{Z}$$

defined as follows. Given $\lambda \in X(T)$ and $\varphi \in Y(T)$, the composite $\lambda \circ \varphi$ is a map $\mathbb{G}_m \to \mathbb{G}_m$. So since $\mathrm{Aut}(\mathbb{G}_m) = \mathbb{Z}$,

$$(\lambda \circ \varphi)(x) = x^{\langle \lambda, \varphi \rangle}$$

for a unique $\langle \lambda, \varphi \rangle \in \mathbb{Z}$.

For each $\alpha \in \Phi$, you prove that there is a (unique up to scalars) homomorphism

$$x_\alpha : \mathbb{G}_a \to G$$

such that

$$t x_\alpha(c) t^{-1} = x_\alpha(\alpha(t)c)$$

for all $c \in \mathbb{G}_a, t \in T$, such that the tangent map

$$dx_\alpha : L(\mathbb{G}_a) \to \mathfrak{g}_\alpha$$

is an isomorphism. Moreover, the x_α's can be normalized so that there is a homomorphism

$$\varphi_\alpha : SL_2 \to G$$

such that

$$\varphi_\alpha \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} = x_\alpha(c), \varphi_\alpha \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} = x_{-\alpha}(c).$$

Define

$$\alpha^\vee : \mathbb{G}_m \to T, \alpha^\vee(c) = \varphi_\alpha \begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix}.$$

So $\alpha^\vee \in Y(T)$. This is called the *coroot* associated to the root $\alpha \in \Phi$.

Now we have built a datum $(X(T), \Phi, Y(T), \Phi^\vee)$, where $\Phi^\vee$ is the set of all coroots. This is the *root datum* of G with respect to the torus T. (Actually, since all maximal tori in G are conjugate, it doesn't depend up to isomorphism on the choice of T.) The notion of root datum is the appropriate generalization of root system to take care of arbitrary reductive algebraic groups, not just the semisimple ones.

Here is an axiomatic formulation of the notion of root datum: a root datum is a quadruple $(X, \Phi, Y, \Phi^\vee)$ where

(a) X ("characters") and Y ("cocharacters") are free abelian groups of finite rank, in duality by a pairing $\langle .,. \rangle : X \times Y \to \mathbb{Z}$;
(b) $\Phi \subset X$ ("roots") and $\Phi^\vee \subset Y$ ("coroots") are finite subsets, and there is a given bijection $\alpha \mapsto \alpha^\vee$ from Φ to $\Phi^\vee$.

To record the additional axioms, define for $\alpha \in \Phi$ the endomorphisms $s_\alpha, s_\alpha^\vee$ of X, Y respectively by

$$s_\alpha(x) = x - \langle x, \alpha^\vee \rangle \alpha, s_\alpha^\vee(y) = y - \langle \alpha, y \rangle \alpha^\vee.$$

Then we have the axioms:

(RD1) For $\alpha \in \Phi$, $\langle \alpha, \alpha^\vee \rangle = 2$.
(RD2) For $\alpha \in \Phi$, $s_\alpha \Phi = \Phi$, $s_\alpha^\vee \Phi^\vee = \Phi^\vee$.

The datum $(X(T), \Phi, Y(T), \Phi^\vee)$ built from our algebraic group G earlier is such a gadget.

There is a notion of morphism of root datum

$$(X, \Phi, Y, \Phi^\vee) \to (X', \Phi', Y', (\Phi')^\vee) :$$

a map $f : X' \to X$ that maps Φ' bijectively onto Φ and such that the dual map $f^\vee : Y \to Y'$ maps $f(\alpha)^\vee$ to $\alpha^\vee$ for all $\alpha \in \Phi'$. Hence there is a notion of isomorphism of root datums.

Now suppose that G, G' are reductive algebraic groups with maximal tori T, T' respectively and corresponding root data $(X(T), \Phi, Y(T), \Phi^\vee)$ and the primed version. Let $f : (X(T), \dots) \to (X'(T), \dots)$ be a morphism of root data. It induces a dual map $f : T \to T'$ of tori. The step is to show that f can be extended to a homomorphism $\bar{f} : G \to G'$.

Using it you prove in particular the *isomorphism theorem*:

Theorem 16.2.1 *Two reductive algebraic groups G, G' are isomorphic if and only if their root datums (relative to some maximal tori) are isomorphic.*

There is also an *existence theorem*:

Theorem 16.2.2 *For every root datum, there exists a corresponding reductive algebraic group G.*

Finally, one intriguing thing: given a root datum $(X, \Phi, Y, \Phi^\vee)$ there is the *dual* root datum $(Y, \Phi^\vee, X, \Phi)$. If G is a reductive algebraic group with root datum $(X, \Phi, Y, \Phi^\vee)$ you see there is a *dual group* $G^\vee$ with the corresponding dual root datum. Note the process of going from G to $G^\vee$ is very clumsy: I don't think there is any direct way of constructing the dual group out of the original.

Example 16.2.3 Suppose that G is a semisimple algebraic group. Let $Q = \mathbb{Z}\Phi \subset X(T)$. Here, Q and $X(T)$ have the same rank, so Q is a lattice in $X(T)$, and $X(T)/Q$ is a finite group, the fundamental group. Let P be the dual lattice to Q. Fixing a positive definite W-invariant inner product on $E = \mathbb{R} \otimes_{\mathbb{Z}} Q$, we can identify P with the weight lattice of the root system of G, and then everything is determined by the relationship between $Q \subseteq X(T) \subseteq P$. You can formulate the classification just of the *semisimple* algebraic groups in these terms.

Example 16.2.4 Let G be a semisimple algebraic group, and suppose that $Q \subseteq X(T) \subseteq P$ are as in the previous example. If $X(T) = P$, then G is called the *simply-connected* group of type Φ. If $X(T) = Q$, then G is called the *adjoint* group of this type. Now let G_{sc} be the simply-connected one, G_{ad} be the adjoint one. Let G be any other semisimple group of type Φ. Then, there is an inclusion $X(T) \hookrightarrow P = X(T_{sc})$. This induces a map $G_{sc} \twoheadrightarrow G$. Similarly, there is always a map $G \twoheadrightarrow G_{ad}$.

Example 16.2.5

(1) Consider the root datum of GL_2. Here, $X(T)$ has basis $\varepsilon_1, \varepsilon_2$, these being the characters picking out the diagonal entries. Moreover, the positive root is $\alpha = \varepsilon_1 - \varepsilon_2$. Also $Y(T)$ has basis $\varepsilon_1^\vee, \varepsilon_2^\vee$, the dual basis, mapping $\mathbb{G}_m$ into each of the diagonal slots. The coroot is $\alpha^\vee = \varepsilon_1^\vee - \varepsilon_2^\vee$.
(2) GL_2 is its own dual group.
(3) Consider the root datum of $SL_2 \times \mathbb{G}_m$. Here, $X(T)$ has basis $\alpha/2, \varepsilon$, $Y(T)$ has the dual basis $\alpha^\vee, \varepsilon^\vee$ (here α is the usual positive root of SL_2).
(4) Consider the root datum of $PSL_2 \times \mathbb{G}_m$. Here, $X(T)$ has basis α, ε, $Y(T)$ has the dual basis $\alpha^\vee/2, \varepsilon$. So $PSL_2 \times \mathbb{G}_m$ is the dual group to $SL_2 \times \mathbb{G}_m$.
(5) As an exercise in applying the classification, you can show that (1),(3) and (4) plus one more, the 4 dimensional torus, are *all* the reductive algebraic groups of dimension 4.

Example 16.2.6 Here are some more examples of dual groups (I think!). The dual group to SL_n is PSL_n. The dual group to Sp_{2n} is SO_{2n+1}. The dual group to PSp_{2n} is $Spin_{2n+1}$. The dual group to SO_{2n} is SO_{2n}. The dual group to $Spin_{2n}$ is PSO_{2n}.

For more explicit constructions of root datums, see Springer, 7.4.7.

Bibliography

[Br] J. Brundan, *Lecture Notes on Algebraic Groups.*
[Hu] J. Humphreys, *Linear Algebraic Groups.*
[Ma] H. Matsumura, *Commutative Algebra.*
[Sh] I.R. Shafarevich, *Basic Algebraic Geometry.*
[Sp] T.A. Springer, *Linear Algebraic Groups.*
[St] R. Steinberg, *Lectures on Chevalley Groups.*