Proof According to (3.16), I can arrange that K is a separable extension of $k(y_1, \dots, y_m)$. If $A = k[x_1, \dots, x_n]$, then the x_i certainly generate K as a field extension of $k(y_1, \dots, y_m)$, so that a suitable linear combination y_{m+1} of the x_i with coefficients in $k(y_1, \dots, y_m)$ generates the field extension; clearing denominators, y_{m+1} can be taken as a linear combination of the x_i with coefficients in $k[y_1, \dots, y_m]$, hence as an element of A. Q.E.D.

Algebraically, what I have proved is that the field extension $k \subset K$, while not necessarily purely transcendental, can be generated as a composite of a purely transcendental extension $k \subset k(y_1, \dots, y_m) = K_0$ followed by a primitive algebraic extension $K_0 \subset K = K_0(y_{m+1})$. In other words, $K = k(y_1, \dots, y_{m+1})$, with only one algebraic dependence relation between the generators. The geometric significance of the result will become clear in (5.10).

Exercises to Chapter 3

3.1 An integral domain A is a *principal ideal domain* if every ideal I of A is principal, that is of the form $I = (a)$; show directly that the ideals in a PID satisfy the a.c.c.

3.2 Show that an integral domain A is a UFD if and only if every ascending chain of principal ideals terminates, and every irreducible element of A is prime.

3.3 (i) Prove Gauss's lemma: if A is a UFD and $f, g \in A[X]$ are polynomials with coefficients in A, then a prime element of A that is a common factor of the coefficients of the product fg is a common factor of the coefficients of f or g.

(ii) It is proved in undergraduate algebra that if K is a field then $K[X]$ is a UFD. Use induction on n to prove that $k[X_1, \dots, X_n]$ is a UFD; for this you will need to compare factorisations in $k[X_1, \dots, X_n]$ with factorisations in $k(X_1, \dots, X_{n-1})[X_n]$, using Gauss's lemma to clear denominators.

3.4 Prove Proposition 3.2, (ii): if A is an integral domain with field of fractions K, and if $0 \notin S \subset A$ is a subset, define

$$B = A[S^{-1}] = \left\{ \frac{a}{b} \in K \;\middle|\; \begin{array}{l} a \in A, \text{ and } b = 1 \text{ or a} \\ \text{product of elements of } S \end{array} \right\}.$$

prove that an ideal I of B is completely determined by its intersection with A, and deduce that A Noetherian $\implies$ B Noetherian.

3.5 Let $J = (XY, XZ, YZ) \subset k[X, Y, Z]$; find $V(J) \subset \mathbb{A}^3$; is it irreducible? Is it true that $J = I(V(J))$? Prove that J cannot be generated by 2 elements. Now let $J' = (XY, (X-Y)Z)$; find $V(J')$, and calculate $\operatorname{rad} J'$.

3.6 Let $J = (X^2 + Y^2 - 1, Y - 1)$; find $f \in I(V(J)) \setminus J$.

3.7 Let $J = (X^2 + Y^2 + Z^2, XY + XZ + YZ)$; identify $V(J)$ and $I(V(J))$.

3.8 Prove that the irreducible components of an algebraic set are unique (this was stated without proof in (3.7, b)). That is, given two decompositions $V = \bigcup_{i \in I} V_i = \bigcup_{j \in J} W_j$ of V as a union of irreducibles, assumed to be irredundant (that is, $V_i \not\subset V_{i'}$ for $i \neq i'$), prove that the V_i are just a renumbering of the W_j.

3.9 Let $f = X^2 - Y^2$ and $g = X^3 + XY^2 - Y^3 - X^2Y - X + Y$; find the irreducible components of $V(f, g) \subset \mathbb{A}^2_{\mathbb{C}}$.

3.10 If $J = (uw - v^2, w^3 - u^5)$, show that $V(J)$ has two irreducible components, one of which is the curve C of (3.11, b).

Prove that the same curve C can be defined by two equations, $uw = v^2$ and $u^5 - 2u^2vw + w^3 = 0$. The point here is that the second equation, restricted to the quadric cone $(uw = v^2)$, is trying to be a square.

3.11 Let $f = v^2 - uw$, $g = u^4 - vw$, $h = w^2 - u^3v$. Identify the variety $V(f, g, h) \subset \mathbb{A}^3$ in the spirit of (3.11, b). Find out whether $V(f, g), V(f, h)$ and $V(g, h)$ have any other interesting components.

3.12 (i) Prove that for any field k, an algebraic set in $\mathbb{A}^1_k$ is either finite or the whole of $\mathbb{A}^1_k$. Deduce that the Zariski topology is the cofinite topology.

(ii) Let k be any field, and $f, g \in k[X, Y]$ irreducible elements, not multiples of one another. Prove that $V(f, g)$ is finite. [Hint: Write $K = k(X)$; prove first that f, g have no common factors in the PID $K[Y]$. Deduce that there exist $p, q \in K[Y]$ such that $pf + qg = 1$; now by clearing denominators in p, q, show that there exists $h \in k[X]$ and $a, b \in k[X, Y]$ such that $h = af + bg$. Hence conclude that there are only finitely many possible values of the X-coordinate of points of $V(f, g)$.]

(iii) Prove that any algebraic set $V \subset \mathbb{A}^2_k$ is a finite union of points and curves.

3.13 (a) Let k be an infinite field and $f \in k[X_1, \ldots, X_n]$; suppose that f is nonconstant, that is, $f \notin k$. Prove that $V(f) \neq \mathbb{A}^n_k$. [Hint: suppose that f involves X_n, and consider $f = \sum a_i(X_1, \ldots, X_{n-1})X_n^i$; now use induction on n.]

(b) Now suppose that k is algebraically closed, and let f be as in (a). Suppose that f has degree m in X_n, and that its leading term is $a_m(X_1, \ldots, X_{n-1})X_n^m$; show that wherever $a_m \neq 0$, there is a finite nonempty set of points of $V(f)$ corresponding to every value of $(X_1, \ldots, X_{n-1})$. Deduce in particular that if $n \geq 2$ then $V(f)$ is infinite.

(c) Put together the results of (b) and of Ex. 3.12, (iii) to deduce that if the field k is algebraically closed, then distinct irreducible polynomials $f \in k[X, Y]$ define distinct hypersurfaces of $\mathbb{A}^2_k$ (compare (3.11, a)).

(d) Generalise the result of (c) to $\mathbb{A}^n_k$.

3.14 Give an example to show that the proof of Noether normalisation given in (3.13) fails over a finite field k. [Hint: find a polynomial $f(X, Y)$ for which $F_d(\alpha, 1) = \alpha^q - \alpha$, so that $F_d(\alpha, 1) = 0$ for all $\alpha \in k$.]

3.15 Let A be a ring and $A \subset B$ a finite A-algebra. Prove that if m is a maximal ideal of A then $mB \neq B$. [Hint: by contradiction, suppose $B = mB$; if $B = \sum Ab_i$ then for each i, $b_i = \sum a_{ij}b_j$ with $a_{ij} \in m$. Now prove that

$$\Delta = \det(\delta_{ij} - a_{ij}) = 0,$$

and conclude that $1_B \in m$, a contradiction. See also [Atiyah and Macdonald, Prop. 2.4 and Cor. 2.5].]

3.16 Let $A = k[a_1, \ldots, a_n]$ be as in the statement of Noether normalisation (3.13), write $I = \ker\{k[X_1, \ldots, X_n] \to k[a_1, \ldots, a_n] = A\}$, and consider $V = V(I)$ in $\mathbb{A}^n_k$; assume for simplicity that I is prime.

Let $Y_1, \ldots, Y_m$ be general linear forms in $X_1, \ldots, X_m$, and write $\pi\colon \mathbb{A}^n_k \to \mathbb{A}^m_k$ for the linear projection defined by $Y_1, \ldots, Y_m$; set $p = \pi|V\colon V \to \mathbb{A}^m_k$. Prove that (i) and (ii) of (3.13) imply that above every $P \in \mathbb{A}^m_k$, $p^{-1}(P)$ is a finite set, and nonempty if k is algebraically closed. [Hint: I contains a monic relation for each X_i over $k[Y_1, \ldots, Y_m]$; the finiteness comes easily from this. For the nonemptiness, use Ex. 3.15 to show that for any $P = (b_1, \ldots, b_m) \in \mathbb{A}^m_k$, the ideal $J_P = I + (Y_1 - b_1, \ldots, Y_m - b_m) \neq k[X_1, \ldots, X_m]$. Then apply the nonemptiness assertion of the Nullstellensatz.]

Chapter 4

Functions on varieties

In this section I work over a fixed field k; from (4.8, II) onwards, k will be assumed to be algebraically closed. The reader who assumes throughout that $k = \mathbb{C}$ will not lose much, and may gain a psychological crutch. I sometimes omit mention of the field k to simplify notation.

4.1 Polynomial functions

Let $V \subset \mathbb{A}^n_k$ be an algebraic set, and $I(V)$ its ideal. Then the quotient ring $k[V] = k[X_1, \dots, X_n]/I(V)$ is in a natural way a ring of functions on V. In more detail, define a *polynomial function* on V to be a map $f\colon V \to k$ of the form $P \mapsto F(P)$, with $F \in k[X_1, \dots, X_n]$; this just means that f is the restriction of a map $F\colon \mathbb{A}^n \to k$ defined by a polynomial. By definition of $I(V)$, two elements $F, G \in k[X_1, \dots, X_n]$ define the same function on V if and only if

$$F(P) - G(P) = 0 \text{ for all } P \in V,$$

that is, if and only if $F - G \in I(V)$. Thus I define the *coordinate ring* $k[V]$ by

$$\begin{aligned} k[V] &= \big\{ f\colon V \to k \;\big|\; f \text{ is a polynomial function} \big\} \\ &\cong k[X_1, \dots, X_n]/I(V). \end{aligned}$$

This is the smallest ring of functions on V containing the coordinate functions X_i (together with k), so for once the traditional terminology is not too obscure.

4.2 $k[V]$ and algebraic subsets of V

An algebraic set $X \subset \mathbb{A}^n$ is contained in V if and only if $I(X) \supset I(V)$. On the other hand, ideals of $k[X_1, \dots, X_n]$ containing $I(V)$ are in obvious bijection with ideals of $k[X_1, \dots, X_n]/I(V)$. (Think about this if it's not obvious to you: the ideal J with $I(V) \subset J \subset k[X_1, \dots, X_n]$ corresponds to $J/I(V)$; and conversely, an ideal J_0 of $k[X_1, \dots, X_n]/I(V)$ corresponds to its inverse image in $k[X_1, \dots, X_n]$.)