Addendum *Under the conditions of (3.13), if furthermore k is algebraically closed, and A is an integral domain with field of fractions K then $y_1, \ldots, y_m \in A$ can be chosen as above so that (i) and (ii) hold, and in addition*

(iii) $k(y_1, \ldots, y_m) \subset K$ is a separable extension.

Proof If k is of characteristic 0, then every field extension is separable; suppose therefore that k has characteristic p. Since A is an integral domain, I is prime; hence if $I \neq 0$, it contains an irreducible element f. Now for each i, there is a dichotomy: either f is separable in X_i, or $f \in k[X_1, \ldots, X_i^p, \ldots, X_n]$.

Claim *If f is inseparable in each X_i, then $f = g^p$ for some g, contradicting the irreducibility of f.*

The assumption is that f is of the form:

$$f = F(X_1^p, \ldots, X_n^p), \quad \text{with} \quad F \in k[X_1, \ldots, X_n].$$

If this happens, let $g \in k[X_1, \ldots, X_n]$ be the polynomial obtained by taking the pth root of each coefficient of F; then making repeated use of the standard identity $(a+b)^p = a^p + b^p$ in characteristic p, it is easy to see that $f = g^p$.

It follows that any irreducible f is separable in at least one of the X_i, say in X_n. Then arguing exactly as above,

$$f(X_1' + \alpha_1 X_n, \ldots, X_{n-1}' + \alpha_{n-1} X_n, X_n)$$

provides a monic, separable relation for a_n over $A' = k[a_1', \ldots, a_{n-1}']$. The result then follows by the same induction argument, using this time the fact that a composite of separable field extensions is separable. Q.E.D.

3.17 Reduction to a hypersurface

Recall the following result from Galois theory:

Theorem (Primitive element theorem) *Let K be an infinite field, and $K \subset L$ a finite separable field extension; then there exists $x \in L$ such that $L = K(x)$. Moreover, if L is generated over K by elements $z_1, \ldots, z_k$, the element x can be chosen to be a linear combination $\sum_i \alpha_i z_i$.*

(This follows at once from the Fundamental Theorem of Galois theory: if $K \subset M$ is the normal closure of L over K then $K \subset M$ is a finite Galois field extension, so that by the Fundamental Theorem there only exist finitely many intermediate field extensions between K and M. The intermediate subfields between K and L form a finite collection $\{K_j\}$ of K-vector subspaces of L, so that I can choose $x \in L$ not belonging to any of these. If $z_1, \ldots, z_k$ are given, not all belonging to any K_i, then x can be chosen as a K-linear combination of the z_i. Then $K(x) = L$.)

Corollary *Under the hypotheses of the Noether normalisation lemma (3.13), there exist $y_1, \ldots, y_{m+1} \in A$ such that $y_1, \ldots, y_m$ satisfy the conclusion of (3.13), and in addition, the field of fractions K of A is generated over k by $y_1, \ldots, y_{m+1}$.*

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.