3.14 Remarks

(I) In fact, the proof of (3.13) shows that $y_1, \dots, y_m$ can be chosen to be m general linear forms in $a_1, \dots, a_n$. To understand the significance of (3.13), write $I = \ker\{k[X_1, \dots, X_n] \to k[a_1, \dots, a_n] = A\}$, and assume for simplicity that I is prime. Consider $V = V(I) \subset \mathbb{A}^n_k$; let $\pi\colon \mathbb{A}^n_k \to \mathbb{A}^m_k$ be the linear projection defined by $y_1, \dots, y_m$, and $p = \pi|V\colon V \to \mathbb{A}^m_k$. It can be seen that the conclusions (i) and (ii) of (3.13) imply that above every $P \in \mathbb{A}^m_k$, $p^{-1}(P)$ is a finite nonempty set (see Ex. 3.16).

(II) The proof of (3.13) has also a simple geometric interpretation: choosing $n-1$ linear forms in the n variables $X_1, \dots, X_n$ corresponds to making a linear projection $\pi\colon \mathbb{A}^n_k \to \mathbb{A}^{n-1}_k$; the fibres of π then form an $(n-1)$-dimensional family of parallel lines. Having chosen the polynomial $f \in I$, it is not hard to see that f gives rise to a monic relation in the final X_n if and only if none of the parallel lines are asymptotes of the variety $(f = 0)$; in terms of projective geometry, this means that the point at infinity $(0, \alpha_1, \dots, \alpha_{n-1}, 1) \in \mathbb{P}^{n-1}_k$ specifying the parallel projection does not belong to the projective closure of $(f = 0)$.

(III) The above proof of (3.13) does not work for a finite field (see Ex. 3.14). However, the theorem itself is true without any condition on k (see [Mumford, Introduction, p. 4] or [Atiyah and Macdonald, (7.9)]).

3.15 Proof of (3.8)

Let $A = k[a_1, \dots, a_n]$ be a finitely generated k-algebra and suppose that $y_1, \dots, y_m \in A$ are as in (3.13). Write $B = k[y_1, \dots, y_m]$. Then A is a finite B-algebra, and it is given that A is a field. If I knew that B is a field, it would follow at once that $m = 0$, so that A is a finite k-algebra, that is, a finite field extension of k, and (3.8) would be proved. Therefore it remains only to prove the following statement:

Lemma *If A is a field, and $B \subset A$ a subring such that A is a finite B-algebra, then B is a field.*

Proof For any $0 \neq b \in B$, the inverse $b^{-1} \in A$ exists in A. Now by (3.12, ii), the finiteness implies that b^{-1} satisfies a monic equation over B, that is, there exists a relation

$$b^{-n} + a_{n-1}b^{-(n-1)} + \dots + a_1 b^{-1} + a_0 = 0, \quad \text{with } a_i \in B;$$

then multiplying through by b^{n-1},

$$b^{-1} = -(a_{n-1} + a_{n-2}b + \dots + a_0 b^{n-1}) \in B.$$

Therefore B is a field. This proves (3.8) and completes the proof of NSS.

3.16 Separable addendum

For the purposes of arranging that everything goes through in characteristic p, it is useful to add a tiny precision. I'm only going to use this in one place in the sequel, so if you can't remember too much about separability from Galois theory, don't lose too much sleep over it (GOTO 3.17).

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 $y_1, \dots, y_m \in A$ can be chosen as above so that (i) and (ii) hold, and in addition*

(iii) $k(y_1, \dots, y_m) \subset K$ 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 $f \in k[X_1, \dots, X_i^p, \dots, X_n]$.

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:

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

If this happens, let $g \in k[X_1, \dots, X_n]$ 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,

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

provides a monic, separable relation for a_n over $A' = k[a_1', \dots, a_{n-1}']$. 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 $z_1, \dots, z_k$, 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 $z_1, \dots, z_k$ 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 $y_1, \dots, y_{m+1} \in A$ such that $y_1, \dots, y_m$ satisfy the conclusion of (3.13), and in addition, the field of fractions K of A is generated over k by $y_1, \dots, y_{m+1}$.*