Proof (i) and (iii) are easy exercises (compare similar results for field extensions). For (ii), I use a rather nonobvious 'determinant trick' (I didn't think of it for myself): suppose $B = \sum Ab_i$; for each i, $xb_i \in B$, so there exist constants $a_{ij} \in A$ such that

$$xb_i = \sum_j a_{ij} b_j.$$

This can be written

$$\sum_j (x\delta_{ij} - a_{ij}) b_j = 0,$$

where δ_{ij} is the identity matrix. Now let M be the matrix with

$$M_{ij} = x\delta_{ij} - a_{ij},$$

and set $\Delta = \det M$. Then by standard linear algebra, (writing $\mathbf{b}$ for the column vector with entries $(b_1, \ldots, b_n)$ and M^{adj} for the adjoint matrix of M),

$$M\mathbf{b} = 0, \quad \text{hence} \quad 0 = (M^{\mathrm{adj}})M\mathbf{b} = \Delta\mathbf{b},$$

and therefore $\Delta b_i = 0$ for all i. However, $1_B \in B$ is a linear combination of the b_i, so that $\Delta = \Delta \cdot 1_B = 0$, and I've won my relation:

$$\det(x\delta_{ij} - a_{ij}) = 0.$$

This is obviously a monic relation for x with coefficients in A. Q.E.D.

3.13 Noether normalisation

Theorem (Noether normalisation lemma) *Let k be an infinite field, and $A = k[a_1, \ldots, a_n]$ a finitely generated k-algebra. Then there exist $m \leq n$ and $y_1, \ldots, y_m \in A$ such that*

(i) $y_1, \ldots, y_m$ are algebraically independent over k; and

(ii) A is a finite $k[y_1, \ldots, y_m]$-algebra.

((i) means as usual that there are no nonzero polynomial relations holding between the y_i; an algebraist's way of saying this is that the natural (surjective) map $k[Y_1, \ldots, Y_m] \to k[y_1, \ldots, y_m] \subset A$ is injective.)

It is being asserted that, as you might expect, the extension of rings can be built up by first throwing in algebraically independent elements, then 'making an algebraic extension'; however, the statement (ii) is far more precise than this, since it says that every element of A is not just algebraic over $k[y_1, \ldots, y_m]$, but satisfies a *monic* equation over it.

Proof Let I be the kernel of the natural surjection,

$$I = \ker\bigl\{k[X_1, \dots, X_n] \to k[a_1, \dots, a_n] = A\bigr\}.$$

Suppose that $0 \neq f \in I$; the idea of the proof is to replace $X_1, \dots, X_{n-1}$ by certain $X'_1, \dots, X'_{n-1}$ so that f becomes a monic equation for a_n over $A' = k[a'_1, \dots, a'_{n-1}]$. So write

$$\begin{aligned} a'_1 &= a_1 - \alpha_1 a_n \\ &\dots \\ a'_{n-1} &= a_{n-1} - \alpha_{n-1} a_n \end{aligned}$$

(where the $\alpha_i \in k$ are elements to be specified later). Then

$$0 = f(a'_1 + \alpha_1 a_n, \dots, a'_{n-1} + \alpha_{n-1} a_n, a_n).$$

Claim *For suitable choice of $\alpha_1, \dots, \alpha_{n-1} \in k$, the polynomial*

$$f(X'_1 + \alpha_1 X_n, \dots, X'_{n-1} + \alpha_{n-1} X_n, X_n)$$

is monic in X_n.

Using the claim, the theorem is proved by induction on n: if $I = 0$ then there's nothing to prove, since $a_1, \dots, a_n$ are algebraically independent. Otherwise, pick $0 \neq f \in I$, and let $\alpha_1, \dots, \alpha_{n-1}$ be as in the claim; then f gives a monic relation satisfied by a_n with coefficients in $A' = k[a'_1, \dots, a'_{n-1}] \subset A$. By the inductive assumption, there exist $y_1, \dots, y_m \in A'$ such that

(1) $y_1, \dots, y_m$ are algebraically independent over k;

(2) A' is a finite $k[y_1, \dots, y_m]$-algebra.

Then $A = A'[a_n]$ is finite over A' (by (3.12, iii)), so by (3.12, i), A is finite over $k[y_1, \dots, y_m]$, proving the theorem.

It only remains to prove the claim. Let $d = \deg f$, and write

$$f = F_d + G,$$

with F_d homogeneous of degree d, and $\deg G \leq d - 1$. Then

$$\begin{aligned} f(X_1, \dots, X_{n-1}, X_n) &= f(X'_1 + \alpha_1 X_n, \dots, X'_{n-1} + \alpha_{n-1} X_n, X_n) \\ &= F_d(\alpha_1, \dots, \alpha_{n-1}, 1) \cdot X_n^d \\ &\qquad + (\text{stuff involving } X_n \text{ to power} \leq d-1); \end{aligned}$$

I'm now home provided that $F_d(\alpha_1, \dots, \alpha_{n-1}, 1) \neq 0$. Since F_d is a nonzero polynomial, it's not hard to check that this is the case for 'almost all' values of $\alpha_1, \dots, \alpha_{n-1}$ (the proof of this is discussed in Ex. 3.13). Q.E.D.

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).