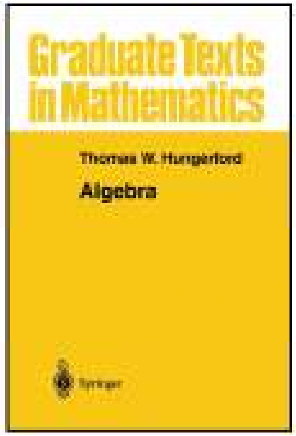
Modern Algebra

Chapter V. Fields and Galois Theory
V.6. Separability—Proofs of Theorems



Theorem V.6.2

Theorem V.6.2. Let F be an extension field of K. then $u \in F$ is both separable and purely inseparable over K if and only if $u \in K$.

Proof. The element $u \in F$ is purely inseparable over K if (and only if) its irreducible polynomial is of the form $(x-u)^m$. u is separable if (an only if) $(x-u)^m$ has m distinct roots in some splitting field. But this occurs if and only if $m = 1$, which occurs if and only if $x - u \in K[x]$, which in turn occurs if and only if $u \in K[x]$. □

Lemma V.6.3

Lemma V.6.3. Let F be an extension field of K with $\mathrm{char}(K) = p \neq 0$. If $u \in F$ is algebraic over K, then u^{p^n} is separable over K for some $n \geq 0$.

Proof. If $\deg(u) = 1$ over K, then u is separable and the result holds with $n = 0$. If u is separable over K, then the result holds with $n = 0$. So let u be nonseparable with irreducible polynomial f of degree greater than one. We proceed by induction on the degree of u over K and assume the result holds for elements of K of degree less than the degree of u. Since u is nonseparable, then u is a root of f of multiplicity greater than 1 and so by Theorem III.6.10(iii), $f'(u) = 0$. By Exercise III.6.3, f is a polynomial in x^p and $f(x) = a_0 + a_1x^p + a_2x^{2p} + \cdots + a_jx^{jp}$, say, and the degree of u over K is jp. But then u^p is of degree $\leq j$ and so by the induction hypothesis, the result holds for u^p and so $(u^p)^{p^m} = u^{p^{m+1}}$ is separable over K for some $m \geq 0$. □

Theorem V.6.4

Theorem V.6.4. If F is an algebraic extension field of a field K of characteristic $p \neq 0$ then the following statements are equivalent:

(i) F is purely inseparable over K;
(ii) the irreducible polynomial of any $u \in F$ is of the form $x^{p^n} - a \in K[x]$;
(iii) if $u \in F$, then $u^{p^n} \in K$ for some $n \geq 0$;
(iv) the only elements of F which are separable over K are the elements of K itself;
(v) F is generated over K by a set of purely inseparable elements.

Proof. (i)⇒(ii) Let $(x-u)^m \in K[x]$ be the irreducible polynomial of $u \in F$ and let $m = np^r$ with $\gcd(n,p) = (n,p) = 1$. Then $(x-u)^m = (x-u)^{p^r n} = (x^{p^r} - u^{p^r})^n$ by Exercise III.1.11. Since $(x-u)^m \in K[x]$ then the coefficient $x^{p^r(n-1)}$, namely $\pm nu^{p^r}$ by the Binomial Theorem (Theorem III.1.6) must lie in K.

Theorem V.6.4 (continued 1)

Theorem V.6.4. If F is an algebraic extension field of a field K of characteristic $p \neq 0$ then the following statements are equivalent:

(i) F is purely inseparable over K;

(ii) the irreducible polynomial of any $u \in F$ is of the form $x^{p^n} - a \in K[x]$.

Proof (continued). (i)⇒(ii) [Exercise V.6.1 states: Let $\text{char}(K) = p \neq 0$ and let $n \geq 1$ be an integer such that $\gcd(p, n) = (p, n) = 1$. If $v \in F$ and $nv \in K$, then $v \in K$.] Since $\gcd(n, p) = (n, p) = 1$ and $nu^{p^r} \in K$ and $u^{p^r} \in F$ (because $u \in F$) then by Exercise V.6.1 (with $v = u^{p^r}$) we have $u^{p^r} \in K$. Since $(x-u)^m = (x^{p^r} - u^{p^r})^n$ is irreducible in $K[x]$, we must have $n = 1$ (or else it factors into a product of $(x^{p^r} - u^{p^r})$ terms since $u^{p^r} \in K$). So $(x-u)^m = x^{p^r} - a$ where $a = u^{p^r} \in K$. That is, the irreducible polynomial for $u \in F$ is of the form $x^{p^n} - a \in K[x]$. Hence, (i)⇒(ii).

Theorem V.6.4 (continued 2)

Theorem V.6.4. If F is an algebraic extension field of a field K of characteristic $p \neq 0$ then the following statements are equivalent:

(ii) the irreducible polynomial of any $u \in F$ is of the form $x^{p^n} - a \in K[x]$;

(iii) if $u \in F$, then $u^{p^n} \in K$ for some $n \geq 0$.

Proof (continued). (ii)⇒(iii) Since (ii) gives that $x^{p^n} - a \in K[x]$ is the irreducible polynomial of u and so $f(u) = u^{p^n} - a = 0$ then $a = u^{p^n} \in K$.

Theorem V.6.4 (continued 3)

Theorem V.6.4. If F is an algebraic extension field of a field K of characteristic $p \neq 0$ then the following statements are equivalent:

(i) F is purely inseparable over K;

(iii) if $u \in F$, then $u^{p^n} \in K$ for some $n \geq 0$;

(v) F is generated over K by a set of purely inseparable elements.

Proof. (i)⇒(v) By definition, each element of F is purely inseparable over K and hence F is generated over K by the set F itself, say.

(iii)⇒(i) This follows from The Freshman's Dream (Exercise III.1.11) as follows: $u \in F$ implies $u^{p^n} \in K$ and so $s^{p^n} - u^{p^n} = (x-u)^{p^n}$ is the irreducible polynomial for $u \in F$ and so u is purely inseparable over K.

Theorem V.6.4 (continued 4)

Theorem V.6.4. If F is an algebraic extension field of a field K of characteristic $p \neq 0$ then the following statements are equivalent:

(i) F is purely inseparable over K;

(iv) the only elements of F which are separable over K are the elements of K itself.

Proof. (i)⇒(iv) Let F be purely inseparable over K and let $u \in F$ be separable over K. Then u is both separable and purely inseparable over K and so by Theorem V.6.2, $u \in K$. Conversely, if $u \in F$ and $u \notin K$ then by Theorem V.6.2, u is not both separable and purely separable (it is not separable, in fact, since F is hypothesized to be purely inseparable over K). So under the hypothesis (i), the only elements of F separable over K are elements of K itself, and (iv) holds.

Theorem V.6.4 (continued 5)

Theorem V.6.4. If F is an algebraic extension field of a field K of characteristic $p \neq 0$ then the following statements are equivalent:

(iii) if $u \in F$, then $u^{p^n} \in K$ for some $n \geq 0$;

(iv) the only elements of F which are separable over K are the elements of K itself.

Proof. (iv)⇒(iii) Suppose the only elements of F which are separable over K are the elements of K itself. Then for $u \in F$, by Lemma V.6.3, u^{p^n} is separable over K and hence by hypothesis $u^{p^n} \in K$ and (iii) follows.

Theorem V.6.4 (continued 6)

Theorem V.6.4. If F is an algebraic extension field of a field K of characteristic $p \neq 0$ then the following statements are equivalent:

(iii) if $u \in F$, then $u^{p^n} \in K$ for some $n \geq 0$;

(v) F is generated over K by a set of purely inseparable elements.

Proof. (v)⇒(iii) Suppose F is generated over K by a set of purely inseparable elements. Now *if* u is purely inseparable over K, then the proof of (i)⇒(ii) above (which was given "element wise" for $u \in F$ purely inseparable over K) we have that $u^{p^n} \in K$ for some $n \geq 0$. If $u \in F$ is an arbitrary element of F (maybe not purely inseparable over K, but generated by purely inseparable over K, but generated by purely inseparables) then by Theorem V.1.3(vi) we have that $u = f(u_1, u_2, \ldots, u_n)/g(u_1, u_2, \ldots, u_n)$ where $n \in \mathbb{N}$, $f, g \in K[x_1, x_2, \ldots, x_n]$, $u_1, u_2, \ldots, u_n$ are purely inseparable over K, and $g(u_1, u_2, \ldots, u_n) \neq 0$.

Theorem V.6.4 (continued 7)

Proof (continued). (v)⇒(iii) Now for any such $f \in K[x_1, x_2, \ldots, x_n]$ we have by "The Freshman's Dream" (Exercise III.1.11) that

$$\begin{aligned}(f(u_1, u_2, \ldots, u_n))^{p^n} &= \left(\sum a_{k_1,k_2,\ldots,k_n} u_1^{k_1} u_2^{k_2} \cdots u_n^{k_n}\right)^{p^n} \\ &\qquad \text{by Theorem III.5.4} \\ &= \sum \left(a_{k_1,k_2,\ldots,k_n} u_1^{k_1} u_2^{k_2} \cdots u_n^{k_n}\right)^{p^n} \\ &\qquad \text{by the Freshman's Dream} \\ &= \sum (a_{k_1,k_2,\ldots,k_n})^{p^n} (u_1^{p^n})^{k_1} (u_2^{p^n})^{k_2} \cdots (u_n^{p^n})^{k_n} \\ &\in K\end{aligned}$$

since $a_{k_1,k_2,\ldots,k_n} \in K$ and $u_1^{p^n}, u_2^{p^n}, \ldots, u_n^{p^n} \in K$ since each u_i is purely inseparable over K and this implies (as above) that $u_i^{p^n} \in K$. Therefore, $u^{p^n} = (f(u_1, u_2, \ldots, u_n)/g(u_1, u_2, \ldots, u_n))^{p^n} \in K$ and (iii) follows. □

Corollary V.6.5

Corollary V.6.5. If F is a finite dimensional purely inseparable extension field of K and $\text{char}(K) = p \neq 0$, then $[F : K] = p^n$ for some $n \geq 0$.

Proof. By Theorem V.1.11, F is finitely generated and algebraic over K, so $F = K(u_1, u_2, \ldots, u_m)$. By hypothesis, each $u_i \in F$ is purely inseparable over K and hence, by Exercise V.6.2, is inseparable over any intermediate field and so u_i is purely inseparable over $K(u_1, u_2, \ldots, u_{i-1})$. By Theorem V.6.4 (the (i)⇒(ii) part) we know that the irreducible polynomial for u_i over $K(u_1, u_2, \ldots, u_{i-1})$ is of the form $x^{p^n} - a$ for some $n \geq 0$ and some $a \in K(u_1, u_2, \ldots, u_{i-1})$. By Theorem V.1.6 (parts (i) and (ii)) we have that $[K(u_1, u_2, \ldots, u_i) : K(u_1, u_2, \ldots, u_{i-1})] = p^{n_i}$ for some $n_i \geq 0$. So for the "towers" $K \subset K(u_1) \subset K(u_1, u_2) \subset \cdots \subset K(u_1, u_2, \ldots, u_m) = F$, we have that in each step the dimension is a power of p. Therefore, by Theorem V.1.2, $[F : K] = p^n$ for some $n \geq 0$. □

Lemma V.6.6

Lemma V.6.6. If F is an extension field of K, X is a subset of F such that $F = K(X)$, and every element of X is separable over K, then F is a separable extension of K.

Proof. If $v \in F$, then by Theorem V.1.3, there is a finite subset $X' = \{u_1, u_2, \ldots, u_n\} \subseteq X$ such that $v \in K(X') = K(u_1, u_2, \ldots, u_n\} \subseteq X$ such that $v \in K(X') = K(u_1, u_2, \ldots, u_n)$. Let $f_i \in K[x]$ be the irreducible separable polynomial of u_i and let E be a splitting field of $\{f_1, f_2, \ldots, f_n\}$ over $K(u_1, u_2, \ldots, u_n)$. By Exercise V.3.3, E is also a splitting field of $\{f_1, f_2, \ldots, f_n\}$ over K. By Theorem V.3.11 (the (iii) implies the first part of (ii) part), E is separable over K (in fact, Galois over K by Theorem V.3.11, the (iii)⇒(i) part). So element $v \in F$ satisfies $v \in K(u_1, u_2, \ldots, u_n) \subset E$ and since E is separable over K then every element of E is separable over K (see Definition V.3.10) and so v is separable over K. Since $v \in F$ is arbitrary, then F is separable over K. □

Theorem V.6.7

Theorem V.6.7. Let F be an algebraic extension field of K, let S be the set of all elements of F which are separable over K, and let P be the set of all elements of F which are purely inseparable over K.

(i) S is a separable extension field of K.

(ii) F is purely inseparable over S.

(iii) P is a purely inseparable extension field of K.

(iv) $P \cap S = K$.

(v) F is separable over P if and only if $F = SP$.

(iv) If F is normal over K, then S is Galois over K, F is Galois over P, and $\mathrm{Aut}_K(S) \cong \mathrm{Aut}_P(F) = \mathrm{Aut}_K(F)$.

Theorem V.6.7(i)

Theorem V.6.7. Let F be an algebraic extension field of K, let S be the set of all elements of F which are separable over K, and let P be the set of all elements of F which are purely inseparable over K.

(i) S is a separable extension field of K.

(ii) F is purely inseparable over S.

(iv) $P \cap S = K$.

Proof. (i) If $u, v \in S$ and $v \neq 0$, then $K(u, v)$ is separable over K by Lemma V.6.6 with $X = \{u, v\}$. Since $K(u, v)$ is a field, then $u - v$ and $uv^{-1} \in K(u, v)$. Since $K(u, v)$ is separable over K then $u - v, uv^{-1} \in S$ and S is a subfield of F. Of course S is separable over K.

(ii) If $\mathrm{char}(K) = 0$ then every algebraic element over K is separable over K (see the comment at the top of page 283 or the Note before Lemma V.6.3) so every element of F is separable over K and $S + F$.

Theorem V.6.7(ii)

Theorem V.6.7. Let F be an algebraic extension field of K, let S be the set of all elements of F which are separable over K, and let P be the set of all elements of F which are purely inseparable over K.

(ii) F is purely inseparable over S.

(iv) $P \cap S = K$.

Proof (continued). (ii) By Theorem V.6.2, every element $u \in F$ is both separable and purely inseparable over S since $u \in S = F$. Then F is purely inseparable over S. If $\mathrm{char}(K) = p \neq 0$, then by Lemma V.6.3, every element $u \in F$ satisfies u^{p^n} is separable over K for some $n \geq 0$. Therefore $u^{p^n} \in S'$. So by Theorem V.6.4 (the (iii)⇒(i) part with K replaced with S), F is purely inseparable over S.

(iv) The elements of $P \cap S$ are both separable and purely inseparable over K. So by Theorem V.6.2, $P \cap S = K$. □

Corollary V.6.8

Corollary V.6.8. If F is a separable extension of E and E is a separable extension field of K, then F is separable over K.

Proof. If S is the set of all elements of F which are separable over K, then by the Note above, separable extension E satisfies $E \subset S$. By Theorem V.6.7(ii), F is purely inseparable over S. But F is separable over E (by hypothesis) and so by Exercise V.3.12, F is separable over the intermediate field S. But the only elements of F which are purely inseparable and separable over F are elements of F (by Theorem V.6.2). So $S = F$ and F is separable over K (by the definition of S). □

Corollary V.6.9

Corollary V.6.9. Let F be an algebraic extension field of K, with $\mathrm{char}(K) = p \neq 0$. If F is separable over K, then $F = KF^{p^n}$ for each $n \geq 1$. If $[F : K]$ is finite and $F = KF^p$ (KF^p is the smallest subfield of F containing $K \cup F^p$), then F is separable over K. In particular, $u \in F$ is separable over K if and only if $K(u^p) = K(u)$.

Proof. Let S be the set of all elements of F which are separable over K. Notice that S is a subfield of F by Theorem V.6.7(i). Suppose $[F : K]$ is finite. Then by Theorem V.1.11, F is finitely generated and algebraic over K. So $F = K(u_1, u_2, \ldots, u_m)$ for some $u_1, u_2, \ldots, u_m \in F$. Now every element of K is separable over K (for $k \in K$, the irreducible polynomial is $x - k$), so $K \subseteq S \subseteq F$. Hence $F = K(u_1, u_2, \ldots, u_m) = S(u_1, u_2, \ldots, u_m)$. By Theorem V.6.7(iii), each u_i is purely inseparable over S. By Theorem V.6.4 (the (i)⇒(iii) part), there is $n \geq 1$ such that $u_i^{p^n} \in S$ for every i (the finiteness of collection $u_1, u_2, \ldots, u_m$ is used here). Take this n as fixed now.

Corollary V.6.9 (continued 1)

Proof (continued). Let $u \in F$ and $u^{p^n} \in F^{p^n}$. Since $u \in F$ then by Theorem V.1.3(v), there are $h, k \in S[x_1, x_2, \ldots, x_m]$ such that $u = h(u_1, u_2, \ldots, u_m)/k(u_1, u_2, \ldots, u_m)$. Now $u^{p^n} = (h(u_1, u_2, \ldots, u_m)/k(u_1, u_2, \ldots, u_m))^{p^n}$. By the Freshman's Dream (Exercise III.1.11) applied inductively to a multinomial gives that u^{p^n} is in fact a quotient of polynomials with coefficients in S evaluated at $u_1^{p^n}, u_2^{p^n}, \ldots, u_m^{p^n}$. Since S is a field and each $u_i^{p^n} \in S$ from above, then $u^{p^n} \in S$ and so $F^{p^n} \subset S$. Since F is purely inseparable over F^{p^n} by Theorem V.6.4 (the (iii)⇒(i) part), then $S \subset F$ is purely inseparable over F^{p^n}. By Exercise V.6.2, since KF^{p^n} is a field intermediate to F^{p^n} and S (notice that both $K \subseteq S$ and $F^{p^n} \subseteq S$, so $KF^{p^n} \subseteq S$), we then have that S is purely inseparable over KF^{p^n}. S is separable over K by Theorem V.6.7 and hence (by Exercise V.3.12(b)) S is separable over the intermediate field KF^{p^n}. So S is both separable and purely inseparable over KF^{p^n}, and so by Theorem V.6.2, $S = KF^{p^n}$.

Corollary V.6.9 (continued 2)

Proof (continued). As observed above, if $h \in K[x_1, x_2, \ldots, x_m]$ then by the Freshman's Cream (Exercise III.1.11) applied inductively $h(x_1, x_2, \ldots, x_m)^{p^t}$ equals the polynomial in $x_1^{p^t}, x_2^{p^t}, \ldots, x_m^{p^t}$ with each coefficient corresponding to a coefficient of h to power p^t:

$$\left(\sum_i a_i x_1^{k_{i,1}} x_2^{k_{i,2}} \cdots x_m^{k_{i,m}}\right)^{p^t} = \sum_i \left(a_i x_1^{k_{i,1}} x_2^{k_{i,2}} \cdots x_m^{k_{i,m}}\right)^{p^t}$$

$$= \sum_i a_i^{p^t} (x_1^{k_{i,1}})^{p^t} (x_2^{k_{i,2}})^{p^t} \cdots (x_m^{k_{i,m}})^{p^t} = \sum_i a_i^{p^t} (x_1^{p^t})^{k_{i,1}} (x_2^{p^t})^{k_{i,2}} \cdots (x_m)^{p^t})^{k_{i,m}}.$$

So by Theorem V.1.3(v), for any $t \geq 1$,

$$F^{p^t} = [K(u_1, u_2, \ldots, u_m)]^{p^t} = K^{p^t}(u_1^{p^t}, u_2^{p^t}, \ldots, u_m^{p^t}).$$

Consequently for any $t \geq 1$ we have

$$KF^{p^t} = KK^{p^t}(u_1^{p^t}, u_2^{p^t}, \ldots, u_m^{p^t}) = K(u_1^{p^t}, u_2^{p^t}, \ldots, u_m^{p^t})$$

(notice that $KK^{p^t} = K$ since $1 \in K^{p^t}$).

Corollary V.6.9 (continued 3)

Proof (continued). Notice that this argument holds for ANY generators (not just the $u_1, u_2, \ldots, u_m$ we started with above). Now to establish the claims of the corollary.

Suppose $F = KF^p$. Then $K(u_1, u_2, \ldots, u_m) = F = KF^p = K(u_1^p, u_2^p, \ldots, u_m^p)$ (the last equality holding from above with $t = 1$). Iterating this argument gives

$$\begin{aligned} F = K(u_1, u_2, \ldots, u_m) &= K(u_1^p, u_2^p, \ldots, u_m^p) \\ &= K(u_1^{p^2}, u_2^{p^2}, \ldots, u_m^{p^2}) \\ &\vdots \\ &= K(u_1^{p^n}, u_2^{p^n}, \ldots, u_m^{p^n}) \\ &= KF^{p^n} \text{ by above (with } t = n) \\ &= S \text{ as shown above.} \end{aligned}$$

Corollary V.6.9 (continued 4)

Corollary V.6.9. Let F be an algebraic extension field of K, with $\mathrm{char}(K) = p \neq 0$. If F is separable over K, then $F = KF^{p^n}$ for each $n \geq 1$. If $[F : K]$ is finite and $F = KF^p$ (KF^p is the smallest subfield of F containing $K \cup F^p$), then F is separable over K. In particular, $u \in F$ is separable over K if and only if $K(u^p) = K(u)$.

Proof (continued). Since S is separable over K (Theorem V.6.7(i)), then F is separable over K and the second claim of the corollary holds.

Conversely, if F is separable over K, then F is both separable and purely inseparable over KF^{p^n} (for all $n \geq 1$). Therefore, by Theorem V.6.2, $F = KF^{p^n}$ and the first claim of the corollary holds. □

Lemma V.6.11

Lemma V.6.11. Let F be an extension field of E, E an extension field of K, and N a normal extension field of K containing F. If r is the cardinal number of distinct E-monomorphisms mapping $F :\to N$ and t is the cardinal number of distinct K-monomorphisms mapping $E :\to N$, then rt is the cardinal number of distinct K-monomorphisms mapping $F \to N$.

Proof. First, suppose r, t are both finite. Let $\tau_1, \tau_2, \ldots, \tau_r$ be all the distinct E-monomorphisms mapping $F \to N$ and $\sigma_1, \sigma_2, \ldots, \sigma_t$ all the distinct K-monomorphisms mapping $E \to N$. Since N is normal over K then by Theorem V.3.14 (the (i)⇒(ii) part), N is a splitting field over K of some set of polynomials in $K[x]$. By Exercise V.3.2, N is also a splitting field over E of the same set of polynomials. Since σ_i fixes K it fixes the set of polynomials. By Theorem V.3.8 (with $L = \sigma_i(K)$, $S = S'$ the set of polynomials, $M = N$, and F of Theorem V.3.8 as N), each σ_i extends to a K-automorphism of N. We also denote the extension as σ_i.

Lemma V.6.11 (continued)

Proof. Each composite map $\sigma_i\tau_j$ then maps $F \to N$, is one to one, and fixes K (that is, each $\sigma_i\tau_j$ is a K-monomorphism mapping $F \to N$). If $\sigma_i\tau_j = \sigma_a\tau_b$ then $\sigma_a^{-1}\sigma_i\tau_j = \tau_b$. Since τ_j and τ_b fix E then $\sigma_a^{-1}\sigma_i|_E = 1_E$. So $\sigma_a = \sigma_i$ and $a = i$ (σ_a, σ_i are originally defined on E and then extended; since $\sigma_a = \sigma_i$ on E the extensions are also equal). Since σ_i is one to one, then $\sigma_i\tau_j = \sigma_i\tau_b$ implies that $\tau_j = \tau_b$ and $j = b$. Therefore, the rt K-monomorphisms $\sigma_i\tau_j$ mapping $F \to N$ where $1 \leq i \leq t$ and $1 \leq j \leq r$ are all distinct. To show this is all such mappings, let $\sigma : F \to N$ be any K-monomorphism. Then $\sigma|_E = \sigma_i$ for some i (since $\sigma_1, \sigma_2, \ldots, \sigma_t$ is the complete collection of such maps). So $\sigma_i^{-1}\sigma$ is a K-monomorphism mapping $F \to N$ which ithe identity on E. Therefore $\sigma_i^{-1}\sigma = \tau_j$ for some j, whence $\sigma = \sigma_i\tau_j$ and so σ is in the collection of rt mappings above.

The proof for r or t not finite is similar. With I as the index set for the σ_i's and J as the index set for the τ_j's, we again take the collection $\sigma_i\tau_j$ where $i \in I$ and $j \in J$. □

Proposition V.6.12

Proposition V.6.12. Let F be a finite dimensional extension field of K and N a normal extension field of K containing F. The number of distinct K-monomorphisms mapping $F \to N$ is precisely $[F : K]_s$, the separable degree of F over K.

Proof. Let S be the maximal subfield of F separable over K (see Theorem V.6.7(i) and the Remark following Theorem V.6.7). As argued in the proof of Lemma V.6.11, Theorem V.3.14, Exercise V.3.2, and Theorem V.3.8 imply that every K-monomorphism mapping $S \to N$ extends to a K-monomorphism of N. By restricting such a mapping to F we have a K-monomorphism mapping $F \to N$.
We claim that the number of distinct K-monomorphisms mapping $F \to N$ is the same as the number of distinct K-monomorphisms mapping $S \to N$. If $\mathrm{char}(K) = 0$, this is trivially true since Theorem V.6.2 (and the note following it) then implies that $F = S$. So let $\mathrm{char}(K) = p \neq 0$ and suppose σ, τ are K-monomorphisms mapping $F \to N$ such that $\sigma = \tau$ on S.

Proposition V.6.12 (continued 1)

Proof (continued). If $u \in F$ then, since F is an algebraic extension of K (Theorem V.1.11) and F is purely inseparable over S (Theorem V.6.7, the (i)⇒(ii) part and Theorem V.6.4, the (i)⇒(iii) part) implies that $u^{p^n} \in S$ for some $n \geq 0$. Therefore

$$\begin{aligned} \sigma(u)^{p^n} &= \sigma(u^{p^n}) \text{ since } \sigma \text{ is a homomorphism} \\ &= \tau(u^{p^n}) \text{ since } \sigma = \tau \text{ on } S \text{ and } u^{p^n} \in S \\ &= \tau(u)^{p^n} \text{ since } \tau \text{ is a homomorphism.} \end{aligned}$$

Then $\sigma(u)^{p^n} - \tau(u)^{p^n} = 0$ and by the Freshman's Dream (Exercise III.1.11), $(\sigma(u) - \tau(u))^{p^n} = 0$ and $\sigma(u) = \tau(u)$ (we are in a field, so there are no zero divisors). This is $\sigma = \tau$ on S then $\sigma = \tau$ on F and so $\sigma = \tau$, proving our claim. Consequently, it suffices WLOG to assume that F is separable over K (that is, $F = S$).

Proposition V.6.12 (continued 2)

Proof (continued). In this case we have

$$\begin{aligned} [F : K] &= [F : S][S : K] \text{ by Theorem V.1.2} \\ &= (1)[F : K]_s \text{ by the definition of } [F : K]_s \\ &= [F : K]_s. \end{aligned}$$

Let E be a field intermediate to K and F (i.e., $K \subset E \subset F$). By Exercise V.3.12, since F is separable over K, then F is separable over E and E is separable over K. So $[F : E] = [F : E]_s$ and $[E : K] = [E : K]_s$ (see the Remark after Definition V.6.10).

We now complete the proof by induction on $n = [F : K] = [F : K]_s$. The case $n = 1$ is trivial since this implies that $F = k$ (by Exercise V.1.1(a)) and there is only $n = 1$ K-monomorphism mapping $K = F$ into N (namely, the identity mapping).

Proposition V.6.12 (continued 3)

Proof (continued). Now for the induction hypothesis, suppose the result holds for all $k < n$; that is, suppose that if F' is any field where F' is a finite dimensional extension field of field K', say $k = [E' : K']$, and field N' is a normal extension field of K' containing E', then the number of distinct K-monomorphisms mapping $E' \to N'$ is precisely $[E' : K']_s$.

If $n > 1$ then $F \neq K$, so there is $u \in F \setminus K$ where $[F : K(u)][K(u) : K] = [F : K]$ by Theorem V.1.2 where $[K(u) : K] = r > 1$.

(1) If $r < n$, then by the induction hypothesis with $E = K(u)$, there are $r = [E : K] = [E : K]_s$ distinct K-monomorphisms mapping $E \to N$. So $n = [F : K] = [F : E][E : K] = [F : E]_s[E : K]_s = [F : E]_s r$. By Exercise V.3.A, N is a normal extension of E and $[F : E] = n/r < n$, so by the induction hypothesis (with $N = N'$, $F' = F$, and $K' = E$) the number of distinct E-monomorphisms mapping $F \to N$ is $[F : E]_s$.

Proposition V.6.12 (continued 4)

Proof (continued). By Lemma V.6.11, the number of distinct K-monomorphisms mapping $F \to N$ is $[F : E]_s[E : K]_s = [F : K]_s$, and so the result holds for $r < n$.

(2) If $r = [K(u) : K] = n = [F : K]$ then by Theorem V.1.2, $[F : K] = [F : K(u)][K(u) : K]$ and so $[F : K(u)] = 1$ and by Exercise V.1.1(a), $F = K(u)$. So $[F : K] = [K(u) : K]$ is the degree of the (separable) irreducible polynomial $f \in K[x]$ of u by Theorem V.1.6(iii). Every K-monomorphism $\sigma : F \to N$ (or $K(u) \to N$) is completely determined by its value at u, say $v = \sigma(u)$. By Theorem V.2.2, $v = \sigma(u)$ is also a root of f. There are at most $[F : K] = \deg(f)$ such roots and so at most $[F : K]$ such K-monomorphisms. Since $u \in N$ is a root of f and since N is normal over K then (by the definition of normal, see Definition V.3.13) f splits in N. Also, f is separable and so each of the roots of $f$is a simple root and so there are $[F : K] = \deg(f)$ such roots and hence (by Corollary V.1.9) $F : K$ such K-monomorphisms mapping $F \to N$. The result now holds by induction. □

Corollary V.6.14

Corollary V.6.14. Let $f \in K[x]$ be an irreducible monic polynomial over a field K, F a splitting field of f over K and u_i a root of f in F. Then

(i) every root of f has multiplicity $[K(u_1) : K]_i$ so that in $F[x]$

$$f(x) = ((x - u_1)(x - u_2) \cdots (x - u_n))^{[K(u_1):K]_i},$$

where $u_1, u_2, \ldots, u_n$ are all the distinct roots of f and $n = [K(u_1) : K]_s$;

(ii) $u_1^{[K(u_1):K]_i}$ is separable over K.

Proof. If $\mathrm{char}(K) = 0$ then the purely inseparable extensions of K are trivial, $[K(u) : K]_i = 1$, and every algebraic element over K is separable over K (see the comment after Theorem V.6.2). So f is separable in $F[x]$ and u_1 is separable over K; hence (i) and (ii) follow. Now let $\mathrm{char}(K) = p \neq 0$.

Corollary V.6.14 (continued 1)

Proof (continued). (i) For any $i > 1$, $u_i \neq u_1$ is also a root of f in F, so by Corollary V.1.9 there is a K-isomorphism σ giving $K(u_1) \cong K(u_i)$ and with $\sigma(u_1) = u_i$. By Exercise V.3.2, F is a splitting field of f over both of the intermediate fields $K(u_1)$ and $K(u_i)$. By Theorem V.3.8 (with $K = L$, $F = M$, and $S = S' = \{f\}$), σ extends to a K-automorphism of F. Since $f \in K[x]$ we have by Theorem V.2.2 that each $\sigma(u_j)$ is a root of f and so

$$(x - u_1)^{r_1}(x - u_2)^{r_2} \cdots (x - u_n)^{r_n} = f$$

$$= \sigma f = (x - \sigma(u_1))^{r_1}(x - \sigma(u_2))^{r_2} \cdots (x - \sigma(u_n))^{r_n}.$$

Since $u_1, u_2, \ldots, u_n$ are distinct, σ is one to one, the fact that $K[x]$ is a unique factorization domain by Theorem III.6.14, and $\sigma(u_1) = u_i$, then $(x - u_i)^{r_i} = (x - \sigma(u_1))^{r_1}$. So we must have that $r_i = r_1$. Similarly by changing σ so that it maps u_1 to the other u_i, we have that each $r_i = r$. That is, every root of f has multiplicity $r = r_1$ so that $f = (x - u_1)^r(x - u_2)^r \cdots (x - u_n)^r$ and $[K(u_1) : K] = \deg(f) = nr$.

Corollary V.6.14 (continued 2)

Proof (continued). Now Corollary V.1.9 and Theorem V.2.2 imply that the *only* K-monomorphisms (Corollary V.1.9 is "if an only if") mapping $K(u)1) \to F$ are the n σ's which map u_1 to u_i (respectively). Since f is a splitting field of $\{f\}$ over K, by Theorem V.3.14 (the (ii)⇒(i) part), F is normal over K. So by Proposition V.6.12 (with th eF of Proposition V.6.12 as $K(u_1)$, and the N of Proposition V.6.12 as F, so that the $[F : K]_s$ of Proposition V.6.12 is $[F(u_1) : K]_s$), $[K(u_1) : K]_s$ is the number of K-monomorphisms mapping $K(u_1) \to F$. That is, $[K(u_1) : K]_s = n$. Therefore, since $[K(u_1) : K] = [K(u_1) : K]_i[K(u_1) : K]_s$ (see the Remark after Definition V.6.10), $[K(u_1) : K]_i = [K(u_1) : K]/[K(u_1) : K]_s = nr/n = r$, and (i) follows.

Proposition V.6.15(i)

Proposition V.6.15. The Primitive Element Theorem.
Let F be a finite dimensional extension field of K.

(i) If F is separable over K, then F is a simple extension of K.
(ii) (Artin) More generally, F is a simple extension of K if and only if there are only finitely many intermediate fields.

Proof. (i) Since F is a separable extension of K, then it is an algebraic extension and so by Theorem V.3.16(iii), there is a Galois extension F_1 of K that contains F. Since we hypothesize $[F : K]$ is finite, then by Theorem V.3.15(iv) $[F : K]$ is finite. By the Fundamental Theorem of Galois Theory (Theorem V.2.5(i)), $\mathrm{Aut}_K F_1$ is finite (since $\mathrm{Aut}_K F_i = [F_1 : K]$) and, since there is a one to one correspondence between the set of intermediate fields of the extension and the set of all subgroups of $\mathrm{Aut}_K F_1$ (by the Fundamental Theorem) with $|\mathrm{Aut}_K F_i| = [F_i : K]$ for each intermediate field F_i then there are only finitely many intermediate fields between K and F_1. Therefore, there can be only a finite number of intermediate fields in the extension of K by F. This proves (i).

Proposition V.6.15(ii)

Proposition V.6.15. The Primitive Element Theorem.
Let F be a finite dimensional extension field of K.

(ii) (Artin) More generally, F is a simple extension of K if and only if there are only finitely many intermediate fields.

Proof. (ii) If K is a finite field and $F = K(u)$ is a simple finite dimensional extension of K (say $[F : K] = n$). If F_i is any intermediate field then by Theorem V.1.2, $[F : K] = [F : F_i][F_i : K]$. So there are only a finite number of possibilities for $[F_i : K]$ (the number of divisors of $[F : K]$). By Corollary V.5.8, any two extension fields of K of the same dimension are K-isomorphic. So, up to isomorphism, there are only finitely many possible intermediate fields. Conversely, if F is a finite dimensional extension of K, say $[F : K] = n$, then by Corollary V.5.8 there is a simple extension of K, $K(u)$, and $F \cong K(u)$.

Proposition V.6.15(ii) (continued 1)

Proof (continued). (ii) Now suppose K is infinite and that F is a finite dimensional extension of K with only finitely many intermediate fields. Since $[F : K]$ is finite, we can choose $u \in F$ such that $[K(u) : K]$ is maximal. ASSUME $K(u) \neq F$. Then there exists $v \in F \setminus K(u)$. Consider all (simple extension) intermediate fields of the form $K(u + zv)$ with $a \in K$. Since K is an infinite field then there are infinitely many elements of F of the form $u + av$ where $u \in F$, $v \in F \setminus K(U)$, and $a \in K$. However, there are by hypothesis only finitely many intermediate fields between K and F. So for some $a, b \in K$ with $a \neq b$ we must have $K(u_a v) = K(u + bv)$ (or else we have infinitely many simple extensions of K intermediate to K and F). So for this a and b, $u - bv \in K(u - av)$ and $(a - b)v = (u + av) - (u - bv) \in K(u + az)$. Since $a, b \in K$ and $a \neq b$, then $(a - b), (a - b)^{-1} \in K$ and so $v = (a - b)^{-1}(a - b)v \in K(u + av)$ and $v \notin K(u)$ (by the choice of v), so $K \subset K(u) \subsetneq K(u + av)$. Whence $[K(u + av) : K] > [K(u) : K]$.

Proposition V.6.15(ii) (continued 2)

Proof (continued). (ii) But this CONTRADICTS the choice of u such that $[K(u) : K]$ is maximal (for all simple extensions of K). So the assumption that $K(u) \neq F$ is false and hence $F = K(u)$ and F is a simple extension of K.

Conversely, assume K is infinite and that $F = K(u)$ is a simple extension. Since $[F : K]$ is finite, then by Theorem V.1.11 F is an algebraic extension of K and so u is algebraic over K. Let E be an intermediate field an $\mathrm{d}g \in E[x]$ the irreducible monic polynomial of u over E. If $g = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ then $[F : E] = [K(u) : E] = [E(u) : E] = n$ by Theorem V.1.6 (parts (ii) and (iii)). Now $F = K(u) \supseteq E \supseteq K(a_0, a_1, \ldots, a_{n-1}) \supseteq K$ (since $g \in E[x]$ then $a_0, a_1, \ldots, a_{n-1} \in E$) and since g is irreducible over E then it is irreducible over $K(a_0, a_1, \ldots, a_{n-1})$.

Proposition V.6.15(ii) (continued 3)

Proof (continued). (ii) Also, $K(u) = K(a_0, a_1, \ldots, a_{n-1})(u)$, so again by Theorem V.1.6 (parts (ii) and (iii)) we have $[F : K(a_0, a_1, \ldots, a_{n-1}] = [K(u) : K(a_0, a_1, \ldots, a_{n-1}] = n$. By Theorem V.1.2, $[F : E][E : K(a_0, a_1, \ldots, a_n)] = n$ and so $[E : K(a_0, a_1, \ldots, a_{n-1})] = 1$ and $E = K(a_0, a_1, \ldots, a_{n-1})$. Thus every intermediate field E is uniquely determined by the irreducible monic polynomial g of u over E. If f is the monic irreducible polynomial of u over K, then $g \mid f$ by Theorem V.1.6(ii). Since f factors uniquely in any splitting field (by Corollary III.6.4, $F[x]$ is a unique factorization domain for any field F), then f can have only a finite number of distinct monic divisors. Consequently, there are only a finite number of intermediate fields. □