Modern Algebra

Chapter V. Fields and Galois Theory

V.1. Field Extensions—Proofs of Theorems

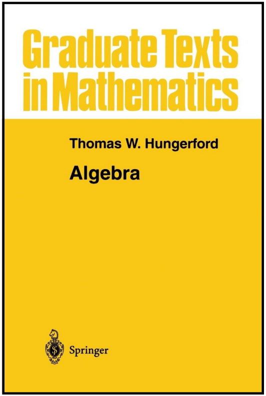

Table of contents

Theorem V.1.3(vi)

Theorem V.1.3. If F is an extension field of a field K, $u, u_i \in F$, and $X \subset F$, then

(vi) the subfield $K(X)$ consists of all elements of the form

$$f(u_1, u_2, \ldots, u_n)/g(u_1, u_2, \ldots, u_n)$$

$$= f(u_1, u_2, \ldots, u_n)g(u_1, u_2, \ldots, u_n)^{-1}$$

where $n \in \mathbb{N}$, $f, g \in K[x_1, x_2, \ldots, x_n]$, $u_1, u_2, \ldots, u_n \in X$, and $g(u_1, u_2, \ldots, u_n) \neq 0$.

Proof. **(vi)** Every field that contains K and X must contain the set

$$E = \{f(u_1, u_2, \ldots, u_n)/g(u_1, u_2, \ldots, u_n) \mid n \in \mathbb{N}; f, g \in K[x_1, x_2, \ldots, x_n];$$

$$u_i \in X; g(u_1, u_2, \ldots, u_n) \neq 0\}.$$

Whence $K(X) \supset E$.

Theorem V.1.3(vi)

Theorem V.1.3. If F is an extension field of a field K, $u, u_i \in F$, and $X \subset F$, then

(vi) the subfield $K(X)$ consists of all elements of the form

$$f(u_1, u_2, \ldots, u_n)/g(u_1, u_2, \ldots, u_n)$$

$$= f(u_1, u_2, \ldots, u_n)g(u_1, u_2, \ldots, u_n)^{-1}$$

where $n \in \mathbb{N}$, $f, g \in K[x_1, x_2, \ldots, x_n]$, $u_1, u_2, \ldots, u_n \in X$, and $g(u_1, u_2, \ldots, u_n) \neq 0$.

Proof. (vi) Every field that contains K and X must contain the set

$$E = \{f(u_1, u_2, \ldots, u_n)/g(u_1, u_2, \ldots, u_n) \mid n \in \mathbb{N}; f, g \in K[x_1, x_2, \ldots, x_n];$$

$$u_i \in X; g(u_1, u_2, \ldots, u_n) \neq 0\}.$$

Whence $K(X) \supset E$.

Theorem V.1.3(vi) (continued 1)

Proof (continued). (vi) Conversely, if $f, g \in K[x_1, x_2, \ldots, x_m]$ and $f_1, g_1 \in K[x_1, x_2, \ldots, x_n]$ then define $h, k \in K[x_1, x_2, \ldots, x_{m+n}]$ by

$$h(x_1, x_2, \ldots, x_{m+n}) = f(x_1, x_2, \ldots, x_m) g_1(x_{m+1}, x_{m+2}, \ldots, x_{m+n})$$

$$-g(x_1, x_2, \ldots, x_m) f_1(x_{m+1}, x_{m+2}, \ldots x_{m+n})$$

and $k(x_1, x_2, \ldots, x_{m+n}) = g(x_1, x_2, \ldots, x_m) g_1(x_{m+1}, x_{m+2}, \ldots, x_{m+n})$.
Then for any $u_1, u_2, \ldots, u_m, v_1, v_2, \ldots, v_n \in X$ such that $g(u_1, u_2, \ldots, u_m) \neq 0$, $g(v_1, v_2, \ldots, v_n) \neq 0$,

$$\frac{f(u_1, u_2, \ldots, u_m)}{g(u_1, u_2, \ldots, u_m)} - \frac{f_1(v_1, v_2, \ldots, v_n)}{g_1(v_1, v_2, \ldots, v_n)} = \frac{h(u_1, u_2, \ldots, u_m, v_1, v_2, \ldots, v_n)}{k(u_1, u_2, \ldots, u_m, v_1, v_2, \ldots, v_n)} \in E.$$

Theorem V.1.3(vi) (continued 1)

Proof (continued). (vi) Conversely, if $f, g \in K[x_1, x_2, \ldots, x_m]$ and $f_1, g_1 \in K[x_1, x_2, \ldots, x_n]$ then define $h, k \in K[x_1, x_2, \ldots, x_{m+n}]$ by

$$h(x_1, x_2, \ldots, x_{m+n}) = f(x_1, x_2, \ldots, x_m) g_1(x_{m+1}, x_{m+2}, \ldots, x_{m+n})$$

$$-g(x_1, x_2, \ldots, x_m) f_1(x_{m+1}, x_{m+2}, \ldots x_{m+n})$$

and $k(x_1, x_2, \ldots, x_{m+n}) = g(x_1, x_2, \ldots, x_m) g_1(x_{m+1}, x_{m+2}, \ldots, x_{m+n})$. Then for any $u_1, u_2, \ldots, u_m, v_1, v_2, \ldots, v_n \in X$ such that $g(u_1, u_2, \ldots, u_m) \neq 0$, $g(v_1, v_2, \ldots, v_n) \neq 0$,

$$\frac{f(u_1, u_2, \ldots, u_m)}{g(u_1, u_2, \ldots, u_m)} - \frac{f_1(v_1, v_2, \ldots, v_n)}{g_1(v_1, v_2, \ldots, v_n)} = \frac{h(u_1, u_2, \ldots, u_m, v_1, v_2, \ldots, v_n)}{k(u_1, u_2, \ldots, u_m, v_1, v_2, \ldots, v_n)} \in E.$$

Therefore, E is an additive subgroup of $\langle F, + \rangle$ by Theorem I.2.5.

Theorem V.1.3(vi) (continued 1)

Proof (continued). (vi) Conversely, if $f, g \in K[x_1, x_2, \ldots, x_m]$ and $f_1, g_1 \in K[x_1, x_2, \ldots, x_n]$ then define $h, k \in K[x_1, x_2, \ldots, x_{m+n}]$ by

$$h(x_1, x_2, \ldots, x_{m+n}) = f(x_1, x_2, \ldots, x_m)g_1(x_{m+1}, x_{m+2}, \ldots, x_{m+n})$$

$$-g(x_1, x_2, \ldots, x_m)f_1(x_{m+1}, x_{m+2}, \ldots x_{m+n})$$

and $k(x_1, x_2, \ldots, x_{m+n}) = g(x_1, x_2, \ldots, x_m)g_1(x_{m+1}, x_{m+2}, \ldots, x_{m+n})$. Then for any $u_1, u_2, \ldots, u_m, v_1, v_2, \ldots, v_n \in X$ such that $g(u_1, u_2, \ldots, u_m) \neq 0$, $g(v_1, v_2, \ldots, v_n) \neq 0$,

$$\frac{f(u_1, u_2, \ldots, u_m)}{g(u_1, u_2, \ldots, u_m)} - \frac{f_1(v_1, v_2, \ldots, v_n)}{g_1(v_1, v_2, \ldots, v_n)} = \frac{h(u_1, u_2, \ldots, u_m, v_1, v_2, \ldots, v_n)}{k(u_1, u_2, \ldots, u_m, v_1, v_2, \ldots, v_n)} \in E.$$

Therefore, E is an additive subgroup of $\langle F, + \rangle$ by Theorem I.2.5.

Theorem V.1.3(vi) (continued 2)

Proof (continued). Similarly,

$$\frac{f(u_1, u_2, \ldots, u_m)}{g(u_1, u_2, \ldots, u_m)} \Big/ \frac{f_1(v_1, v_2, \ldots, v_n)}{g_1(v_1, v_2, \ldots, v_n)}$$

$$= \frac{f_2(u_1, u_2, \ldots, u_m, v_1, v_2, \ldots, v_n)}{g_2(u_1, u_2, \ldots, u_m, v_1, v_2, \ldots, v_n)} \in E$$

and so $E \setminus \{0\}$ is a multiplicative subgroup of $\langle F, \times \rangle$ by Theorem I.2.5. So E is a field. Since $K(x)$ is the intersection of all fields containing $K \cup X$, then $K(X) \subset E$. Therefore $K(X) = E$. □

Theorem V.1.3(vi) (continued 2)

Proof (continued). Similarly,

$$\frac{f(u_1, u_2, \ldots, u_m)}{g(u_1, u_2, \ldots, u_m)} \bigg/ \frac{f_1(v_1, v_2, \ldots, v_n)}{g_1(v_1, v_2, \ldots, v_n)}$$

$$= \frac{f_2(u_1, u_2, \ldots, u_m, v_1, v_2, \ldots, v_n)}{g_2(u_1, u_2, \ldots, u_m, v_1, v_2, \ldots, v_n)} \in E$$

and so $E \setminus \{0\}$ is a multiplicative subgroup of $\langle F, \times \rangle$ by Theorem I.2.5. So E is a field. Since $K(x)$ is the intersection of all fields containing $K \cup X$, then $K(X) \subset E$. Therefore $K(X) = E$. □

Theorem V.1.3(vii)

Theorem V.1.3. If F is an extension field of a field K, $u, u_i \in F$, and $X \subset F$, then

(vii) For each $v \in K(X)$ (respectively, $K[X]$) there is a finite subset X' of X such that $v \in K(X')$ (respectively, $K[X']$).

Proof. **(vi)** If $u \in K(X)$ then by part (vi), $u = f(u_1, u_2, \ldots, u_n)/g(u_1, u_2, \ldots, u_n)$ for some $n \in \mathbb{N}$ and $f, g \in K[x_1, x_2, \ldots, x_n]$. So with $X' = \{u_1, u_2, \ldots, u_n\}$, $u \in K(X')$. □

Theorem V.1.3(vii)

Theorem V.1.3. If F is an extension field of a field K, $u, u_i \in F$, and $X \subset F$, then

(vii) For each $v \in K(X)$ (respectively, $K[X]$) there is a finite subset X' of X such that $v \in K(X')$ (respectively, $K[X']$).

Proof. (vi) If $u \in K(X)$ then by part (vi), $u = f(u_1, u_2, \ldots, u_n)/g(u_1, u_2, \ldots, u_n)$ for some $n \in \mathbb{N}$ and $f, g \in K[x_1, x_2, \ldots, x_n]$. So with $X' = \{u_1, u_2, \ldots, u_n\}$, $u \in K(X')$. □

Theorem V.1.5

Theorem V.1.5. If F is an extension field of K and $u \in F$ is transcendental over K, then there is an isomorphism of fields $K(u) \cong K(x)$ which is the identity when restricted to K.

Proof. Since u is transcendental then $f(u) \neq 0$, $g(u) \neq 0$ for all nonzero $f, g \in K[x]$. Define $\varphi : K(x) \to F$ as $f/g \mapsto f(u)/g(u)$. "Clearly" φ is a homomorphism. Now for $f_1/g_1 \neq f_2/g_2$, we have $\varphi(f_1/g_1) = f_1(u)/g_1(u)$ and $\varphi(f_2/g_2) = f_2(u)/g_2(u)$ and since $f_1/g_1 \neq f_2/g_2$ then $f_1 g_2 \neq f_2 g_1$ and $f_1 g_2 - f_2 g_1 \neq 0$ (not the 0 polynomial, that is). Now $f_1(u)g_2(u) - f_2(u)g_1(u) \neq 0$ (or else u is algebraic over K), and so $\varphi(f_1/g_1) = f_1(u)/g_1(u) \neq f_2(u)/g_2(u) = \varphi(f_2/g_2)$. Therefore φ is one to one (a monomorphism).

Theorem V.1.5

Theorem V.1.5. If F is an extension field of K and $u \in F$ is transcendental over K, then there is an isomorphism of fields $K(u) \cong K(x)$ which is the identity when restricted to K.

Proof. Since u is transcendental then $f(u) \neq 0$, $g(u) \neq 0$ for all nonzero $f, g \in K[x]$. Define $\varphi : K(x) \to F$ as $f/g \mapsto f(u)/g(u)$. "Clearly" φ is a homomorphism. Now for $f_1/g_1 \neq f_2/g_2$, we have $\varphi(f_1/g_1) = f_1(u)/g_1(u)$ and $\varphi(f_2/g_2) = f_2(u)/g_2(u)$ and since $f_1/g_1 \neq f_2/g_2$ then $f_1g_2 \neq f_2g_1$ and $f_1g_2 - f_2g_1 \neq 0$ (not the 0 polynomial, that is). Now $f_1(u)g_2(u) - f_2(u)g_1(u) \neq 0$ (or else u is algebraic over K), and so $\varphi(f_1/g_1) = f_1(u)/g_1(u) \neq f_2(u)/g_2(u) = \varphi(f_2/g_2)$. Therefore φ is one to one (a monomorphism). Also, φ is the identity on K (treating K as a subfield of $K(x)$; think of K as the constant rational functions in $F(x)$). By Theorem V.1.3(iv), the image of φ is $K(u)$. So φ is an isomorphism from $K(x)$ to $K(u)$ which is the identity on K. □

Theorem V.1.5

Theorem V.1.5. If F is an extension field of K and $u \in F$ is transcendental over K, then there is an isomorphism of fields $K(u) \cong K(x)$ which is the identity when restricted to K.

Proof. Since u is transcendental then $f(u) \neq 0$, $g(u) \neq 0$ for all nonzero $f, g \in K[x]$. Define $\varphi : K(x) \to F$ as $f/g \mapsto f(u)/g(u)$. "Clearly" φ is a homomorphism. Now for $f_1/g_1 \neq f_2/g_2$, we have $\varphi(f_1/g_1) = f_1(u)/g_1(u)$ and $\varphi(f_2/g_2) = f_2(u)/g_2(u)$ and since $f_1/g_1 \neq f_2/g_2$ then $f_1g_2 \neq f_2g_1$ and $f_1g_2 - f_2g_1 \neq 0$ (not the 0 polynomial, that is). Now $f_1(u)g_2(u) - f_2(u)g_1(u) \neq 0$ (or else u is algebraic over K), and so $\varphi(f_1/g_1) = f_1(u)/g_1(u) \neq f_2(u)/g_2(u) = \varphi(f_2/g_2)$. Therefore φ is one to one (a monomorphism). Also, φ is the identity on K (treating K as a subfield of $K(x)$; think of K as the constant rational functions in $F(x)$). By Theorem V.1.3(iv), the image of φ is $K(u)$. So φ is an isomorphism from $K(x)$ to $K(u)$ which is the identity on K. □

Theorem V.1.6

Theorem V.1.6. If F is an extension field of K and $u \in F$ is algebraic over K, then

(i) $K(u) = K[u]$;

(ii) $K(u) \cong K[x]/(f)$ where $f \in K[x]$ is an irreducible monic polynomial of degree $n \geq 1$ uniquely determined by the conditions that $f(u) = 0$ and $g(u) = 0$ (where $g \in K[x]$) if and only if f divides g;

(iii) $[K(u) : K] = n$;

(iv) $\{1_K, u, u^2, \ldots, u^{n-1}\}$ is a basis of the vector space $K(u)$ over K;

(v) every element of $K(u)$ can be written uniquely in the form $a_0 + a_1 u + a_2 u^2 + \cdots + a_{n-1} u^{n-1}$ where each $a_i \in K$.

Proof. (i) and (ii) Define $\varphi : K[x] \to K[u]$ as $g \mapsto g(u)$. Then "clearly" φ is a ring homomorphism. By Theorem V.1.3(i), φ is onto (an epimorphism). Since K is a field, by Corollary III.6.4, $K[x]$ is a principal ideal domain.

Theorem V.1.6

Theorem V.1.6. If F is an extension field of K and $u \in F$ is algebraic over K, then

(i) $K(u) = K[u]$;

(ii) $K(u) \cong K[x]/(f)$ where $f \in K[x]$ is an irreducible monic polynomial of degree $n \geq 1$ uniquely determined by the conditions that $f(u) = 0$ and $g(u) = 0$ (where $g \in K[x]$) if and only if f divides g;

(iii) $[K(u) : K] = n$;

(iv) $\{1_K, u, u^2, \ldots, u^{n-1}\}$ is a basis of the vector space $K(u)$ over K;

(v) every element of $K(u)$ can be written uniquely in the form $a_0 + a_1 u + a_2 u^2 + \cdots + a_{n-1} u^{n-1}$ where each $a_i \in K$.

Proof. (i) and (ii) Define $\varphi : K[x] \to K[u]$ as $g \mapsto g(u)$. Then "clearly" φ is a ring homomorphism. By Theorem V.1.3(i), φ is onto (an epimorphism). Since K is a field, by Corollary III.6.4, $K[x]$ is a principal ideal domain.

Theorem V.1.6(i) and (ii)

Proof (continued). (i) and (ii) Now Ker(φ) is an ideal by Theorem III.2.8, so Ker(φ) = (f) for some $f \in K[x]$. Notice that $\varphi(f) = f(u) = 0$. Since u is algebraic, Ker(φ) $\neq \{0\}$. Also, Ker(φ) $\neq K[x]$ (for example, nonzero constant polynomials are not mapped to 0). So $f \neq 0$ and $\deg(f) \geq 1$. Furthermore, if c is the leading coefficient of f then c is a unit in $K[x]$ by Corollary III.6.4 and so polynomial $c^{-1}f$ is monic.

Theorem V.1.6(i) and (ii)

Proof (continued). (i) and (ii) Now $\text{Ker}(\varphi)$ is an ideal by Theorem III.2.8, so $\text{Ker}(\varphi) = (f)$ for some $f \in K[x]$. Notice that $\varphi(f) = f(u) = 0$. Since u is algebraic, $\text{Ker}(\varphi) \neq \{0\}$. Also, $\text{Ker}(\varphi) \neq K[x]$ (for example, nonzero constant polynomials are not mapped to 0). So $f \neq 0$ and $\deg(f) \geq 1$. Furthermore, if c is the leading coefficient of f then c is a unit in $K[x]$ by Corollary III.6.4 and so polynomial $c^{-1}f$ is monic. By Theorem III.3.2(ii) we have that $(f) = (c^{-1}f)$. Consequently, WLOG we assume that f is monic. By the First Isomorphism Theorem (Corollary III.2.10), $K[x]/(f) = K[x]/\text{Ker}(\varphi) \cong \text{Im}(\varphi) = K[u]$.

Theorem V.1.6(i) and (ii)

Proof (continued). (i) and (ii) Now $\text{Ker}(\varphi)$ is an ideal by Theorem III.2.8, so $\text{Ker}(\varphi) = (f)$ for some $f \in K[x]$. Notice that $\varphi(f) = f(u) = 0$. Since u is algebraic, $\text{Ker}(\varphi) \neq \{0\}$. Also, $\text{Ker}(\varphi) \neq K[x]$ (for example, nonzero constant polynomials are not mapped to 0). So $f \neq 0$ and $\deg(f) \geq 1$. Furthermore, if c is the leading coefficient of f then c is a unit in $K[x]$ by Corollary III.6.4 and so polynomial $c^{-1}f$ is monic. By Theorem III.3.2(ii) we have that $(f) = (c^{-1}f)$. Consequently, WLOG we assume that f is monic. By the First Isomorphism Theorem (Corollary III.2.10), $K[x]/(f) = K[x]/\text{Ker}(\varphi) \cong \text{Im}(\varphi) = K[u]$. Since $K[u]$ is an integral domain (because K is a field), by Theorem III.2.16, the ideal (f) is prime. Since (f) is a prime ideal, by Theorem III.3.4(i), f itself is a prime element of $K[x]$ and by Theorem III.3.4(iii), f is irreducible in $K[x]$ (notice that $K[x]$ is a principal ideal domain as explained above), and by Theorem III.3.4(ii), (f) is a maximal ideal in $K[x]$. Consequently, $K[x]/(f)$ is a field by Theorem III.2.20(i).

Theorem V.1.6(i) and (ii)

Proof (continued). (i) and (ii) Now $\text{Ker}(\varphi)$ is an ideal by Theorem III.2.8, so $\text{Ker}(\varphi) = (f)$ for some $f \in K[x]$. Notice that $\varphi(f) = f(u) = 0$. Since u is algebraic, $\text{Ker}(\varphi) \neq \{0\}$. Also, $\text{Ker}(\varphi) \neq K[x]$ (for example, nonzero constant polynomials are not mapped to 0). So $f \neq 0$ and $\deg(f) \geq 1$. Furthermore, if c is the leading coefficient of f then c is a unit in $K[x]$ by Corollary III.6.4 and so polynomial $c^{-1}f$ is monic. By Theorem III.3.2(ii) we have that $(f) = (c^{-1}f)$. Consequently, WLOG we assume that f is monic. By the First Isomorphism Theorem (Corollary III.2.10), $K[x]/(f) = K[x]/\text{Ker}(\varphi) \cong \text{Im}(\varphi) = K[u]$. Since $K[u]$ is an integral domain (because K is a field), by Theorem III.2.16, the ideal (f) is prime. Since (f) is a prime ideal, by Theorem III.3.4(i), f itself is a prime element of $K[x]$ and by Theorem III.3.4(iii), f is irreducible in $K[x]$ (notice that $K[x]$ is a principal ideal domain as explained above), and by Theorem III.3.4(ii), (f) is a maximal ideal in $K[x]$. Consequently, $K[x]/(f)$ is a field by Theorem III.2.20(i).

Theorem V.1.6(i) and (ii) (continued)

Proof (continued). Since $K(u)$ is the smallest subfield of F containing $K \cup \{u\}$ (since $K(u)$ is the intersection of all subfields of F containing $K \cup \{u\}$), and $K[u]$ is a ring containing $K \cup \{u\}$, but $K[u]$ is a field since $K[u] \cong K[x]/(f)$, then $K(u) \subset K[u]$. However, in general, the ring $K[u]$ is a subset of the field $K(u)$; that is $K(u) \supset K[u]$, so we must have $K(u) = K[u]$ and (i) follows. We have established (ii), except for the uniqueness claim. Suppose $g(u) = 0$ for $g \in K[x]$. Then $\varphi(g) = g(u) = 0$ and so $g \in \text{Ker}(\varphi) = (f)$. Since principal ideal (f) consists of all multiples of f (by, say, Theorem III.2.5(v)) then g is a multiple of f; that is, f divides g. So (i) follows.

Theorem V.1.6(i) and (ii) (continued)

Proof (continued). Since $K(u)$ is the smallest subfield of F containing $K \cup \{u\}$ (since $K(u)$ is the intersection of all subfields of F containing $K \cup \{u\}$), and $K[u]$ is a ring containing $K \cup \{u\}$, but $K[u]$ is a field since $K[u] \cong K[x]/(f)$, then $K(u) \subset K[u]$. However, in general, the ring $K[u]$ is a subset of the field $K(u)$; that is $K(u) \supset K[u]$, so we must have $K(u) = K[u]$ and (i) follows. We have established (ii), except for the uniqueness claim. Suppose $g(u) = 0$ for $g \in K[x]$. Then $\varphi(g) = g(u) = 0$ and so $g \in \text{Ker}(\varphi) = (f)$. Since principal ideal (f) consists of all multiples of f (by, say, Theorem III.2.5(v)) then g is a multiple of f; that is, f divides g. So (i) follows.

Theorem V.1.6(iv)

Theorem V.1.6. If F is an extension field of K and $u \in F$ is algebraic over K, then

(iv) $\{1_K, u, u^2, \ldots, u^{n-1}\}$ is a basis of the vector space $K(u)$ over K.

Proof. (iv) By Theorem V.1.3(i), every element of $K[u] = K(u)$ is of the form $g(u)$ for some $g \in K[x]$. By the Division Algorithm (Theorem III.6.2) we know that $g(x) = q(x)f(x) + h(x)$ with $q, h \in K[x]$ and $\deg(h) < \deg(f)$. Therefore,
$g(u) = q(u)f(u) + h(u) = 0 + h(u) = b_0 + b_1 u + \cdots + b_m u^m$ with $m < n = \deg(f)$.

Theorem V.1.6(iv)

Theorem V.1.6. If F is an extension field of K and $u \in F$ is algebraic over K, then

(iv) $\{1_K, u, u^2, \ldots, u^{n-1}\}$ is a basis of the vector space $K(u)$ over K.

Proof. (iv) By Theorem V.1.3(i), every element of $K[u] = K(u)$ is of the form $g(u)$ for some $g \in K[x]$. By the Division Algorithm (Theorem III.6.2) we know that $g(x) = q(x)f(x) + h(x)$ with $q, h \in K[x]$ and $\deg(h) < \deg(f)$. Therefore, $g(u) = q(u)f(u) + h(u) = 0 + h(u) = b_0 + b_1 u + \cdots + b_m u^m$ with $m < n = \deg(f)$. Thus, every element of $K(u)$ can be written as a linear combination of $1_K, u, u^2, \ldots, u^{n-1}$. That is, $\{1_K, u, u^2, \ldots, u^{n-1}\}$ spans the K-vector space $K(u)$. [HERE, a "K-vector space" is a vector space with scalars from K. A basis is a linearly independent spanning set; see page 181.]

Theorem V.1.6(iv)

Theorem V.1.6. If F is an extension field of K and $u \in F$ is algebraic over K, then

(iv) $\{1_K, u, u^2, \ldots, u^{n-1}\}$ is a basis of the vector space $K(u)$ over K.

Proof. (iv) By Theorem V.1.3(i), every element of $K[u] = K(u)$ is of the form $g(u)$ for some $g \in K[x]$. By the Division Algorithm (Theorem III.6.2) we know that $g(x) = q(x)f(x) + h(x)$ with $q, h \in K[x]$ and $\deg(h) < \deg(f)$. Therefore, $g(u) = q(u)f(u) + h(u) = 0 + h(u) = b_0 + b_1 u + \cdots + b_m u^m$ with $m < n = \deg(f)$. Thus, every element of $K(u)$ can be written as a linear combination of $1_K, u, u^2, \ldots, u^{n-1}$. That is, $\{1_K, u, u^2, \ldots, u^{n-1}\}$ spans the K-vector space $K(u)$. [HERE, a "K-vector space" is a vector space with scalars from K. A basis is a linearly independent spanning set; see page 181.]

Theorem V.1.6(iv) (continued)

Theorem V.1.6. If F is an extension field of K and $u \in F$ is algebraic over K, then

(iv) $\{1_K, u, u^2, \ldots, u^{n-1}\}$ is a basis of the vector space $K(u)$ over K.

Proof (continued). (iv) To see that $\{1_K, u, u^2, \ldots, u^{n-1}\}$ is linearly independent over K (and hence a basis), suppose $a_0 + a_1 u + \cdots + a_{n-1}u^{n-1} = 0$ for some $a_i \in K$. Then $g = a_0 + a_1 u + \cdots + a_{n-1}u^{n-1} \in K[x]$ has u as a root and has a degree of at most $n-1$ (some a_i's could be 0). By (ii), f divides g and $\deg(f) = n$, so it must be that $g = 0$ (the zero polynomial); that is, $a_i = 0$ for all i, whence $\{1_K, u, u^2, \ldots, u^{n-1}\}$ is linearly independent and hence is a basis of $K(u)$. □

Theorem V.1.6(iv) (continued)

Theorem V.1.6. If F is an extension field of K and $u \in F$ is algebraic over K, then

(iv) $\{1_K, u, u^2, \ldots, u^{n-1}\}$ is a basis of the vector space $K(u)$ over K.

Proof (continued). (iv) To see that $\{1_K, u, u^2, \ldots, u^{n-1}\}$ is linearly independent over K (and hence a basis), suppose $a_0 + a_1 u + \cdots + a_{n-1}u^{n-1} = 0$ for some $a_i \in K$. Then $g = a_0 + a_1 u + \cdots + a_{n-1}u^{n-1} \in K[x]$ has u as a root and has a degree of at most $n-1$ (some a_i's could be 0). By (ii), f divides g and $\deg(f) = n$, so it must be that $g = 0$ (the zero polynomial); that is, $a_i = 0$ for all i, whence $\{1_K, u, u^2, \ldots, u^{n-1}\}$ is linearly independent and hence is a basis of $K(u)$. □

Theorem V.1.6(iii) and (v)

Theorem V.1.6. If F is an extension field of K and $u \in F$ is algebraic over K, then

(iii) $[K(u) : K] = n$;

(v) every element of $K(u)$ can be written uniquely in the form $a_0 + a_1 u + a_2 u^2 + \cdots + a_{n-1} u^{n-1}$ where each $a_i \in K$.

Proof. (iii) Now $[K(u) : K]$ denotes the dimension of $K(u)$ as a K-vector space (more precisely, the cardinality of a basis). So part by (iv), $[K(u) : K] = n$.

Theorem V.1.6(iii) and (v)

Theorem V.1.6. If F is an extension field of K and $u \in F$ is algebraic over K, then

(iii) $[K(u) : K] = n$;

(v) every element of $K(u)$ can be written uniquely in the form $a_0 + a_1 u + a_2 u^2 + \cdots + a_{n-1} u^{n-1}$ where each $a_i \in K$.

Proof. (iii) Now $[K(u) : K]$ denotes the dimension of $K(u)$ as a K-vector space (more precisely, the cardinality of a basis). So part by (iv), $[K(u) : K] = n$.

(v) By (iv), every element of $K(u)$ can be written in the form $a_0 + a_1 u + \cdots + a_{n-1} u^{n-1}$ for some $a_i \in K$ because $\{1_K, u, u^2, \ldots, u^{n-1}\}$ is a basis. For uniqueness, suppose $a_0 + a_1 u + \cdots + a_{n-1} u^{n-1} = b_0 + b_1 u + \cdots + b_{n-1} u^{n-1}$.

Theorem V.1.6(iii) and (v)

Theorem V.1.6. If F is an extension field of K and $u \in F$ is algebraic over K, then

(iii) $[K(u) : K] = n$;

(v) every element of $K(u)$ can be written uniquely in the form $a_0 + a_1 u + a_2 u^2 + \cdots + a_{n-1} u^{n-1}$ where each $a_i \in K$.

Proof. (iii) Now $[K(u) : K]$ denotes the dimension of $K(u)$ as a K-vector space (more precisely, the cardinality of a basis). So part by (iv), $[K(u) : K] = n$.

(v) By (iv), every element of $K(u)$ can be written in the form $a_0 + a_1 u + \cdots + a_{n-1} u^{n-1}$ for some $a_i \in K$ because $\{1_K, u, u^2, \ldots, u^{n-1}\}$ is a basis. For uniqueness, suppose $a_0 + a_1 u + \cdots + a_{n-1} u^{n-1} = b_0 + b_1 u + \cdots + b_{n-1} u^{n-1}$. Then $(a_0 - b_0) + (a_1 - b_1)u + \cdots + (a_{n-1} - b_{n-1})u^{n-1} = 0$ and since $\{1_K, u, u^2, \ldots, u^{n-1}\}$ is linearly independent (it is a basis by part (iv)) then $a_0 - b_0 = a_1 - b_1 = \cdots = a_{n-1} - b_{n-1} = 0$ and so $a_0 = b_0$, $a_1 = b_1$, $\ldots$, $a_{n-1} = b_{n-1} = 0$ and the representation is in fact unique. □

Theorem V.1.6(iii) and (v)

Theorem V.1.6. If F is an extension field of K and $u \in F$ is algebraic over K, then

(iii) $[K(u) : K] = n$;

(v) every element of $K(u)$ can be written uniquely in the form $a_0 + a_1 u + a_2 u^2 + \cdots + a_{n-1} u^{n-1}$ where each $a_i \in K$.

Proof. (iii) Now $[K(u) : K]$ denotes the dimension of $K(u)$ as a K-vector space (more precisely, the cardinality of a basis). So part by (iv), $[K(u) : K] = n$.

(v) By (iv), every element of $K(u)$ can be written in the form $a_0 + a_1 u + \cdots + a_{n-1} u^{n-1}$ for some $a_i \in K$ because $\{1_K, u, u^2, \ldots, u^{n-1}\}$ is a basis. For uniqueness, suppose $a_0 + a_1 u + \cdots + a_{n-1} u^{n-1} = b_0 + b_1 u + \cdots + b_{n-1} u^{n-1}$. Then $(a_0 - b_0) + (a_1 - b_1)u + \cdots + (a_{n-1} - b_{n-1})u^{n-1} = 0$ and since $\{1_K, u, u^2, \ldots, u^{n-1}\}$ is linearly independent (it is a basis by part (iv)) then $a_0 - b_0 = a_1 - b_1 = \cdots = a_{n-1} - b_{n-1} = 0$ and so $a_0 = b_0$, $a_1 = b_1$, $\ldots$, $a_{n-1} = b_{n-1} = 0$ and the representation is in fact unique. □

Theorem V.1.8

Theorem V.1.8. Let $\sigma : K \to L$ be an isomorphism of fields, u an element of some extension field of K and v an element of some extension field of L. Assume either:

(i) u is transcendental over K and v is transcendental over L; or

(ii) u is a root of an irreducible polynomial $f \in K[x]$ and v is a root of $\sigma f \in L[x]$.

Then σ extends to an isomorphism of fields $K(u) \cong L(v)$ which maps u onto v.

Proof. (i) Since $\sigma : K \to L$ is an isomorphism, then, by Exercise III.5.1, the mapping $K[x] \to L[x]$ given by $\sum_{i=0}^{n} r_i x^i \mapsto \sum_{i=0}^{m} \sigma(r_i) x^i$ is an isomorphism. By Theorem V.1.3(iv), every element of $K(x)$ is of the form h/g for some $h, g \in K[x]$ and every element of $L(x)$ is of the form k/ℓ for some $k, \ell \in L(x)$.

Theorem V.1.8

Theorem V.1.8. Let $\sigma : K \to L$ be an isomorphism of fields, u an element of some extension field of K and v an element of some extension field of L. Assume either:

(i) u is transcendental over K and v is transcendental over L; or

(ii) u is a root of an irreducible polynomial $f \in K[x]$ and v is a root of $\sigma f \in L[x]$.

Then σ extends to an isomorphism of fields $K(u) \cong L(v)$ which maps u onto v.

Proof. (i) Since $\sigma : K \to L$ is an isomorphism, then, by Exercise III.5.1, the mapping $K[x] \to L[x]$ given by $\sum_{i=0}^{n} r_i x^i \mapsto \sum_{i=0}^{m} \sigma(r_i) x^i$ is an isomorphism. By Theorem V.1.3(iv), every element of $K(x)$ is of the form h/g for some $h, g \in K[x]$ and every element of $L(x)$ is of the form k/ℓ for some $k, \ell \in L(x)$. Since the mapping above (which we also denote as σ) is one to one and onto, then σ extends to a one to one and onto mapping of $K(x)$ to $L(x)$ as $g/\ell \mapsto \sigma(g)/\sigma(\ell)$. It is straightforward to verify that this extended σ is a field isomorphism.

Theorem V.1.8

Theorem V.1.8. Let $\sigma : K \to L$ be an isomorphism of fields, u an element of some extension field of K and v an element of some extension field of L. Assume either:

(i) u is transcendental over K and v is transcendental over L; or

(ii) u is a root of an irreducible polynomial $f \in K[x]$ and v is a root of $\sigma f \in L[x]$.

Then σ extends to an isomorphism of fields $K(u) \cong L(v)$ which maps u onto v.

Proof. (i) Since $\sigma : K \to L$ is an isomorphism, then, by Exercise III.5.1, the mapping $K[x] \to L[x]$ given by $\sum_{i=0}^{n} r_i x^i \mapsto \sum_{i=0}^{m} \sigma(r_i) x^i$ is an isomorphism. By Theorem V.1.3(iv), every element of $K(x)$ is of the form h/g for some $h, g \in K[x]$ and every element of $L(x)$ is of the form k/ℓ for some $k, \ell \in L(x)$. Since the mapping above (which we also denote as σ) is one to one and onto, then σ extends to a one to one and onto mapping of $K(x)$ to $L(x)$ as $g/\ell \mapsto \sigma(g)/\sigma(\ell)$. It is straightforward to verify that this extended σ is a field isomorphism.

Theorem V.1.8(i)

Theorem V.1.8. Let $\sigma : K \to L$ be an isomorphism of fields, u an element of some extension field of K and v an element of some extension field of L. Assume either:

(i) u is transcendental over K and v is transcendental over L.

Then σ extends to an isomorphism of fields $K(u) \cong L(v)$ which maps u onto v.

Proof (continued). (i) Since u is transcendental, by Theorem V.1.5, we have $K(u) \cong K(x) \cong L(x) \cong L(v)$. The isomorphism form $K(u)$ to $L(v)$ is an extension of σ and so the extension still maps K to L. Since the isomorphism of $K(u)$ to $K(x)$ maps u to x, the isomorphism of $K(x)$ to $L(x)$ maps x to x, and the isomorphism of $L(x)$ to $L(v)$ maps x to v, then the extension of σ maps u to v. □

Theorem V.1.8(i)

Theorem V.1.8. Let $\sigma : K \to L$ be an isomorphism of fields, u an element of some extension field of K and v an element of some extension field of L. Assume either:

(i) u is transcendental over K and v is transcendental over L.

Then σ extends to an isomorphism of fields $K(u) \cong L(v)$ which maps u onto v.

Proof (continued). (i) Since u is transcendental, by Theorem V.1.5, we have $K(u) \cong K(x) \cong L(x) \cong L(v)$. The isomorphism form $K(u)$ to $L(v)$ is an extension of σ and so the extension still maps K to L. Since the isomorphism of $K(u)$ to $K(x)$ maps u to x, the isomorphism of $K(x)$ to $L(x)$ maps x to x, and the isomorphism of $L(x)$ to $L(v)$ maps x to v, then the extension of σ maps u to v. □

Theorem V.1.8(ii)

Theorem V.1.8. Let $\sigma : K \to L$ be an isomorphism of fields, u an element of some extension field of K and v an element of some extension field of L. Assume either:

(ii) u is a root of an irreducible polynomial $f \in K[x]$ and v is a root of $\sigma f \in L[x]$.

Then σ extends to an isomorphism of fields $K(u) \cong L(v)$ which maps u onto v.

Proof. (ii) WLOG, we assume f is monic (since the extended isomorphism $\sigma : K[x] \to L[x]$ maps polynomial kf to $\sigma(kf) = k\sigma(f)$ for all $k \in K$ and the roots of f and kf (and σf and $k\sigma f$) coincide. Since $\sigma : K[x] \to L[x]$ is an isomorphism, then $\sigma f \in L[x]$ is monic and irreducible.

Theorem V.1.8(ii)

Theorem V.1.8. Let $\sigma : K \to L$ be an isomorphism of fields, u an element of some extension field of K and v an element of some extension field of L. Assume either:

(ii) u is a root of an irreducible polynomial $f \in K[x]$ and v is a root of $\sigma f \in L[x]$.

Then σ extends to an isomorphism of fields $K(u) \cong L(v)$ which maps u onto v.

Proof. (ii) WLOG, we assume f is monic (since the extended isomorphism $\sigma : K[x] \to L[x]$ maps polynomial kf to $\sigma(kf) = k\sigma(f)$ for all $k \in K$ and the roots of f and kf (and σf and $k\sigma f$) coincide. Since $\sigma : K[x] \to L[x]$ is an isomorphism, then $\sigma f \in L[x]$ is monic and irreducible. In the proof of Theorem V.1.6(ii) the mappings $\varphi : K[x]/(f) \to K[u] = K(u)$ and $\psi : L[x]/(\sigma f) \to L[v] = L[v]$ given respectively by $\varphi[g + (f)] = g(u)$ and $\psi[h + (\sigma f)] = h(v)$ are isomorphisms.

Theorem V.1.8(ii)

Theorem V.1.8. Let $\sigma : K \to L$ be an isomorphism of fields, u an element of some extension field of K and v an element of some extension field of L. Assume either:

(ii) u is a root of an irreducible polynomial $f \in K[x]$ and v is a root of $\sigma f \in L[x]$.

Then σ extends to an isomorphism of fields $K(u) \cong L(v)$ which maps u onto v.

Proof. **(ii)** WLOG, we assume f is monic (since the extended isomorphism $\sigma : K[x] \to L[x]$ maps polynomial kf to $\sigma(kf) = k\sigma(f)$ for all $k \in K$ and the roots of f and kf (and σf and $k\sigma f$) coincide. Since $\sigma : K[x] \to L[x]$ is an isomorphism, then $\sigma f \in L[x]$ is monic and irreducible. In the proof of Theorem V.1.6(ii) the mappings $\varphi : K[x]/(f) \to K[u] = K(u)$ and $\psi : L[x]/(\sigma f) \to L[v] = L[v]$ given respectively by $\varphi[g + (f)] = g(u)$ and $\psi[h + (\sigma f)] = h(v)$ are isomorphisms.

Theorem V.1.8(ii) (continued)

Theorem V.1.8. Let $\sigma : K \to L$ be an isomorphism of fields, u an element of some extension field of K and v an element of some extension field of L. Assume either:

(ii) u is a root of an irreducible polynomial $f \in K[x]$ and v is a root of $\sigma f \in L[x]$.

Then σ extends to an isomorphism of fields $K(u) \cong L(v)$ which maps u onto v.

Proof (continued). By Corollary III.2.11, the mapping $\theta : K[x]/(f) \to L[x]/(\sigma f)$ given by $\theta(g + (f)) = \sigma g + (\sigma f)$ is an isomorphism. Therefore the composition $K(u) \xrightarrow{\varphi^{-1}} K[x]/(f) \xrightarrow{\theta} L[x]/(\sigma f) \xrightarrow{\psi} L(v)$ is an isomorphism of fields $K(u)$ and $L(v)$ such that $g(u) \mapsto g(x) + (f) \mapsto \sigma g(x) + (\sigma f) \mapsto \sigma g(v)$. Also, $\psi\theta\varphi^{-1}$ agrees with σ on K (the "constant" rational functions of u in $K(u)$) and maps $u \mapsto x + (f) \mapsto x + (\sigma f) \mapsto v$. □

Theorem V.1.8(ii) (continued)

Theorem V.1.8. Let $\sigma : K \to L$ be an isomorphism of fields, u an element of some extension field of K and v an element of some extension field of L. Assume either:

(ii) u is a root of an irreducible polynomial $f \in K[x]$ and v is a root of $\sigma f \in L[x]$.

Then σ extends to an isomorphism of fields $K(u) \cong L(v)$ which maps u onto v.

Proof (continued). By Corollary III.2.11, the mapping $\theta : K[x]/(f) \to L[x]/(\sigma f)$ given by $\theta(g + (f)) = \sigma g + (\sigma f)$ is an isomorphism. Therefore the composition $K(u) \stackrel{\varphi^{-1}}{\to} K[x]/(f) \stackrel{\theta}{\to} L[x]/(\sigma f) \stackrel{\psi}{\to} L(v)$ is an isomorphism of fields $K(u)$ and $L(v)$ such that $g(u) \mapsto g(x) + (f) \mapsto \sigma g(x) + (\sigma f) \mapsto \sigma g(v)$. Also, $\psi\theta\varphi^{-1}$ agrees with σ on K (the "constant" rational functions of u in $K(u)$) and maps $u \mapsto x + (f) \mapsto x + (\sigma f) \mapsto v$. □

Corollary V.1.9

Corollary V.1.9. Let E and F each be extension fields of K and let $u \in E$ and $v \in F$ be algebraic over K. Then u and v are roots of the same irreducible polynomial $f \in K[x]$ if and only if there is an isomorphism of fields $K(u) \cong K(v)$ which sends u onto v and it the identity on K.

Proof. First, suppose u and v are roots of the same irreducible polynomial $f \in K[x]$. Then by Theorem V.1.8(ii) with $\sigma = 1_K$ (the identity on K) we have $\sigma f = f$ and so u (a root of f) and v (a root of $f = \sigma f$) and $K(u) \cong K(v)$ where the isomorphism between $K(u)$ and $K(v)$ sends u onto v.

Corollary V.1.9

Corollary V.1.9. Let E and F each be extension fields of K and let $u \in E$ and $v \in F$ be algebraic over K. Then u and v are roots of the same irreducible polynomial $f \in K[x]$ if and only if there is an isomorphism of fields $K(u) \cong K(v)$ which sends u onto v and it the identity on K.

Proof. First, suppose u and v are roots of the same irreducible polynomial $f \in K[x]$. Then by Theorem V.1.8(ii) with $\sigma = 1_K$ (the identity on K) we have $\sigma f = f$ and so u (a root of f) and v (a root of $f = \sigma f$) and $K(u) \cong K(v)$ where the isomorphism between $K(u)$ and $K(v)$ sends u onto v.

Conversely, suppose $\sigma : K(u) \to K(v)$ is an isomorphism with $\sigma(u) = v$ and $\sigma(k) = k$ for all $k \in K$. Let $f \in K[x]$ be the irreducible (monic) polynomial for which algebraic u is a root.

Corollary V.1.9

Corollary V.1.9. Let E and F each be extension fields of K and let $u \in E$ and $v \in F$ be algebraic over K. Then u and v are roots of the same irreducible polynomial $f \in K[x]$ if and only if there is an isomorphism of fields $K(u) \cong K(v)$ which sends u onto v and it the identity on K.

Proof. First, suppose u and v are roots of the same irreducible polynomial $f \in K[x]$. Then by Theorem V.1.8(ii) with $\sigma = 1_K$ (the identity on K) we have $\sigma f = f$ and so u (a root of f) and v (a root of $f = \sigma f$) and $K(u) \cong K(v)$ where the isomorphism between $K(u)$ and $K(v)$ sends u onto v.

Conversely, suppose $\sigma : K(u) \to K(v)$ is an isomorphism with $\sigma(u) = v$ and $\sigma(k) = k$ for all $k \in K$. Let $f \in K[x]$ be the irreducible (monic) polynomial for which algebraic u is a root. If $f = \sum_{i=0}^n k_i x^i$ then $0 = f(u) = \sum_{i=0}^n k_i u^i$. Since $\sigma(0) = 0$ then $0 = \sigma(0) = \sigma\left(\sum_{i=0}^n k_i u^i\right) = \sum_{i=0}^n \sigma(k_i u^i) = \sum_{i=0}^n \sigma(k_i)\sigma(u^i) = \sum_{i=0}^n k_i \sigma(u)^i = \sum_{i=0}^n k_i v^i = f(v)$. So v is a root of f as well. □

Corollary V.1.9

Corollary V.1.9. Let E and F each be extension fields of K and let $u \in E$ and $v \in F$ be algebraic over K. Then u and v are roots of the same irreducible polynomial $f \in K[x]$ if and only if there is an isomorphism of fields $K(u) \cong K(v)$ which sends u onto v and it the identity on K.

Proof. First, suppose u and v are roots of the same irreducible polynomial $f \in K[x]$. Then by Theorem V.1.8(ii) with $\sigma = 1_K$ (the identity on K) we have $\sigma f = f$ and so u (a root of f) and v (a root of $f = \sigma f$) and $K(u) \cong K(v)$ where the isomorphism between $K(u)$ and $K(v)$ sends u onto v.

Conversely, suppose $\sigma : K(u) \to K(v)$ is an isomorphism with $\sigma(u) = v$ and $\sigma(k) = k$ for all $k \in K$. Let $f \in K[x]$ be the irreducible (monic) polynomial for which algebraic u is a root. If $f = \sum_{i=0}^n k_i x^i$ then $0 = f(u) = \sum_{i=0}^n k_i u^i$. Since $\sigma(0) = 0$ then $0 = \sigma(0) = \sigma\left(\sum_{i=0}^n k_i u^i\right) = \sum_{i=0}^n \sigma(k_i u^i) = \sum_{i=0}^n \sigma(k_i)\sigma(u^i) = \sum_{i=0}^n k_i \sigma(u)^i = \sum_{i=0}^n k_i v^i = f(v)$. So v is a root of f as well. □

Theorem V.1.10. Kronecker's Theorem

Theorem V.1.10. Kronecker's Theorem.
If K is a field and $f \in K[x]$ a polynomial of degree n, then there exists a simple extension field $F = K(u)$ of K such that:

(i) $u \in F$ is a root of f;

(ii) $[K(u) : K] \leq n$, with equality holding if and only if f is irreducible in $K[x]$;

(iii) if f is irreducible in $K[x]$, then $K(u)$ is unique up to an isomorphism which is the identity on K.

Proof. (i) WLOG, we may assume f is irreducible (if not, we replace f by one of its irreducible factors).

Theorem V.1.10. Kronecker's Theorem

Theorem V.1.10. Kronecker's Theorem.
If K is a field and $f \in K[x]$ a polynomial of degree n, then there exists a simple extension field $F = K(u)$ of K such that:

(i) $u \in F$ is a root of f;

(ii) $[K(u) : K] \leq n$, with equality holding if and only if f is irreducible in $K[x]$;

(iii) if f is irreducible in $K[x]$, then $K(u)$ is unique up to an isomorphism which is the identity on K.

Proof. (i) WLOG, we may assume f is irreducible (if not, we replace f by one of its irreducible factors). Then the ideal (f) is maximal in $K[x]$ (by Corollary III.6.4, since K is a field, $K[x]$ is a principal ideal domain and by Theorem III.3.4(ii) (f) is maximal). So by Theorem III.2.20, $F = K[x]/(f)$ is a field.

Theorem V.1.10. Kronecker's Theorem

Theorem V.1.10. Kronecker's Theorem.
If K is a field and $f \in K[x]$ a polynomial of degree n, then there exists a simple extension field $F = K(u)$ of K such that:

(i) $u \in F$ is a root of f;

(ii) $[K(u) : K] \leq n$, with equality holding if and only if f is irreducible in $K[x]$;

(iii) if f is irreducible in $K[x]$, then $K(u)$ is unique up to an isomorphism which is the identity on K.

Proof. (i) WLOG, we may assume f is irreducible (if not, we replace f by one of its irreducible factors). Then the ideal (f) is maximal in $K[x]$ (by Corollary III.6.4, since K is a field, $K[x]$ is a principal ideal domain and by Theorem III.3.4(ii) (f) is maximal). So by Theorem III.2.20, $F = K[x]/(f)$ is a field.

Theorem V.1.10(i). Kronecker's Theorem

Proof (continued). (i) Furthermore, the canonical projection $\pi : K[x] \to K[x]/(f) = F$ mapping $g \mapsto g + (f)$, when restricted to K (the constant polynomials in $K[x]$) is a one to one homomorphism (the canonical projection is a homomorphism, the only "constant" in (f) is the zero function since (f) consists of all multiples of f by elements in $K[x]$, and so the kernel of the canonical projection consists only of $0 \in K$; therefore the canonical projection is one to one by Theorem I.2.3(i)). Since π is one to one, $\pi(K) \cong K$ can be considered as a subfield of field F; that is, F is an extension field of K (provided that K is identified with $\pi(K)$). For $x \in K[x]$, let $u = \pi(x) = x + (f) \in F = K[x]/(f)$.

Theorem V.1.10(i). Kronecker's Theorem

Proof (continued). (i) Furthermore, the canonical projection $\pi : K[x] \to K[x]/(f) = F$ mapping $g \mapsto g + (f)$, when restricted to K (the constant polynomials in $K[x]$) is a one to one homomorphism (the canonical projection is a homomorphism, the only "constant" in (f) is the zero function since (f) consists of all multiples of f by elements in $K[x]$, and so the kernel of the canonical projection consists only of $0 \in K$; therefore the canonical projection is one to one by Theorem I.2.3(i)). Since π is one to one, $\pi(K) \cong K$ can be considered as a subfield of field F; that is, F is an extension field of K (provided that K is identified with $\pi(K)$). For $x \in K[x]$, let $u = \pi(x) = x + (f) \in F = K[x]/(f)$. Then $F = K[x]/(f) \cong K(u)$ by Theorem V.1.6(ii) and, since coset addition and multiplication is performed by representatives, then $f(u) = f(x + (f)) = f(x) + (f) = 0 + (f) = 0$ (since $0 + (f)$ is the additive identity in $K[x]/(f) = F$). So (i) follows.

Theorem V.1.10(i). Kronecker's Theorem

Proof (continued). (i) Furthermore, the canonical projection $\pi : K[x] \to K[x]/(f) = F$ mapping $g \mapsto g + (f)$, when restricted to K (the constant polynomials in $K[x]$) is a one to one homomorphism (the canonical projection is a homomorphism, the only "constant" in (f) is the zero function since (f) consists of all multiples of f by elements in $K[x]$, and so the kernel of the canonical projection consists only of $0 \in K$; therefore the canonical projection is one to one by Theorem I.2.3(i)). Since π is one to one, $\pi(K) \cong K$ can be considered as a subfield of field F; that is, F is an extension field of K (provided that K is identified with $\pi(K)$). For $x \in K[x]$, let $u = \pi(x) = x + (f) \in F = K[x]/(f)$. Then $F = K[x]/(f) \cong K(u)$ by Theorem V.1.6(ii) and, since coset addition and multiplication is performed by representatives, then $f(u) = f(x + (f)) = f(x) + (f) = 0 + (f) = 0$ (since $0 + (f)$ is the additive identity in $K[x]/(f) = F$). So (i) follows.

Theorem V.1.10(ii) and (iii). Kronecker's Theorem

Theorem V.1.10. Kronecker's Theorem.
If K is a field and $f \in K[x]$ a polynomial of degree n, then there exists a simple extension field $F = K(u)$ of K such that:

(ii) $[K(u) : K] \leq n$, with equality holding if and only if f is irreducible in $K[x]$;

(iii) if f is irreducible in $K[x]$, then $K(u)$ is unique up to an isomorphism which is the identity on K.

Proof. (ii) Theorem V.1.6(iii) shows that $[K(u) : K] = n$ for irreducible f of degree n. As commented above, if f is not irreducible, then we consider an irreducible factor of f (of degree less than n) and (ii) follows).

Theorem V.1.10(ii) and (iii). Kronecker's Theorem

Theorem V.1.10. Kronecker's Theorem.
If K is a field and $f \in K[x]$ a polynomial of degree n, then there exists a simple extension field $F = K(u)$ of K such that:

(ii) $[K(u) : K] \leq n$, with equality holding if and only if f is irreducible in $K[x]$;

(iii) if f is irreducible in $K[x]$, then $K(u)$ is unique up to an isomorphism which is the identity on K.

Proof. (ii) Theorem V.1.6(iii) shows that $[K(u) : K] = n$ for irreducible f of degree n. As commented above, if f is not irreducible, then we consider an irreducible factor of f (of degree less than n) and (ii) follows).

(iii) Corollary V.1.9 implies (iii) and that the extension field does not depend on "which" root of f is used. □

Theorem V.1.10(ii) and (iii). Kronecker's Theorem

Theorem V.1.10. Kronecker's Theorem.
If K is a field and $f \in K[x]$ a polynomial of degree n, then there exists a simple extension field $F = K(u)$ of K such that:

(ii) $[K(u) : K] \leq n$, with equality holding if and only if f is irreducible in $K[x]$;

(iii) if f is irreducible in $K[x]$, then $K(u)$ is unique up to an isomorphism which is the identity on K.

Proof. (ii) Theorem V.1.6(iii) shows that $[K(u) : K] = n$ for irreducible f of degree n. As commented above, if f is not irreducible, then we consider an irreducible factor of f (of degree less than n) and (ii) follows).

(iii) Corollary V.1.9 implies (iii) and that the extension field does not depend on "which" root of f is used. □

Theorem V.1.11

Theorem V.1.11. If F is a finite dimensional extension field of K, then F is finitely generated and algebraic over K.

Proof. If E is a finite dimensional extension of K, say $[F:K]=n$. Let $u \in F$ (arbitrary). Then the set of $n+1$ elements $\{1_K, u, u^2, \ldots, u^n\}$ must be linearly dependent over F.

Theorem V.1.11

Theorem V.1.11. If F is a finite dimensional extension field of K, then F is finitely generated and algebraic over K.

Proof. If E is a finite dimensional extension of K, say $[F : K] = n$. Let $u \in F$ (arbitrary). Then the set of $n + 1$ elements $\{1_K, u, u^2, \ldots, u^n\}$ must be linearly dependent over F. So there are $a_i \in K$, not all zero, such that $a_0 + a_1 u + a_2 u^2 + \cdots + a_n u^n = 0$, which implies that u is algebraic over K. Since u was arbitrary, F is an algebraic extension of K. If $\{v_1, v_2, \ldots, v_n\}$ is a basis of F over K, then "it is easy to see" (use Theorem V.1.3(v)) that $F = K(v_1, v_2, \ldots, v_n)$. $\square$

Theorem V.1.11

Theorem V.1.11. If F is a finite dimensional extension field of K, then F is finitely generated and algebraic over K.

Proof. If E is a finite dimensional extension of K, say $[F : K] = n$. Let $u \in F$ (arbitrary). Then the set of $n+1$ elements $\{1_K, u, u^2, \ldots, u^n\}$ must be linearly dependent over F. So there are $a_i \in K$, not all zero, such that $a_0 + a_1 u + a_2 u^2 + \cdots + a_n u^n = 0$, which implies that u is algebraic over K. Since u was arbitrary, F is an algebraic extension of K. If $\{v_1, v_2, \ldots, v_n\}$ is a basis of F over K, then "it is easy to see" (use Theorem V.1.3(v)) that $F = K(v_1, v_2, \ldots, v_n)$. □

Theorem V.1.12

Theorem V.1.12. If F is an extension field of K and X is a subset of F such that $F = K(X)$ and every element of X is algebraic over K, then F is an algebraic extension of K. If X is a finite set, then F is finite dimensional over K.

Proof. If $v \in F$, then by Theorem V.1.3(iv), $v = f(u_1, u_2, \ldots, u_n)/g(u_1, u_2, \ldots, u_n)$ for some $n \in \mathbb{N}$, some $f, g \in F[x_1, x_2, \ldots, x_n]$ and some $u_1, u_2, \ldots, u_n \in X$. So $v \in K(u_1, u_2, \ldots, u_n)$.

Theorem V.1.12

Theorem V.1.12. If F is an extension field of K and X is a subset of F such that $F = K(X)$ and every element of X is algebraic over K, then F is an algebraic extension of K. If X is a finite set, then F is finite dimensional over K.

Proof. If $v \in F$, then by Theorem V.1.3(iv), $v = f(u_1, u_2, \ldots, u_n)/g(u_1, u_2, \ldots, u_n)$ for some $n \in \mathbb{N}$, some $f, g \in F[x_1, x_2, \ldots, x_n]$ and some $u_1, u_2, \ldots, u_n \in X$. So $v \in K(u_1, u_2, \ldots, u_n)$. So there is a tower of subfields $K \subset K(u_1) \subset K(u_1, u_2) \subset \cdots \subset K(u_1, u_2, \ldots, u_n)$. For a given $i \geq 2$, u_i is algebraic over K and so u_i is algebraic over $K(u_1, u_2, \ldots, u_{i-1})$, say u_i is of degree r_i over $K(u_1, u_2, \ldots, u_{i-1})$.

Theorem V.1.12

Theorem V.1.12. If F is an extension field of K and X is a subset of F such that $F = K(X)$ and every element of X is algebraic over K, then F is an algebraic extension of K. If X is a finite set, then F is finite dimensional over K.

Proof. If $v \in F$, then by Theorem V.1.3(iv), $v = f(u_1, u_2, \ldots, u_n)/g(u_1, u_2, \ldots, u_n)$ for some $n \in \mathbb{N}$, some $f, g \in F[x_1, x_2, \ldots, x_n]$ and some $u_1, u_2, \ldots, u_n \in X$. So $v \in K(u_1, u_2, \ldots, u_n)$. So there is a tower of subfields $K \subset K(u_1) \subset K(u_1, u_2) \subset \cdots \subset K(u_1, u_2, \ldots, u_n)$. For a given $i \geq 2$, u_i is algebraic over K and so u_i is algebraic over $K(u_1, u_2, \ldots, u_{i-1})$, say u_i is of degree r_i over $K(u_1, u_2, \ldots, u_{i-1})$. Since $K(u_1, u_2, \ldots, u_{i-1})(u_i) = K(u_1, u_2, \ldots, u_i)$ by Exercise V.1.4(b), we have $[K(u_1, u_2, \ldots, u_i) : K(u_1, u_2, \ldots, u_{i-1})] = r_i$ by Theorem V.1.6(iii).

Theorem V.1.12

Theorem V.1.12. If F is an extension field of K and X is a subset of F such that $F = K(X)$ and every element of X is algebraic over K, then F is an algebraic extension of K. If X is a finite set, then F is finite dimensional over K.

Proof. If $v \in F$, then by Theorem V.1.3(iv), $v = f(u_1, u_2, \ldots, u_n)/g(u_1, u_2, \ldots, u_n)$ for some $n \in \mathbb{N}$, some $f, g \in F[x_1, x_2, \ldots, x_n]$ and some $u_1, u_2, \ldots, u_n \in X$. So $v \in K(u_1, u_2, \ldots, u_n)$. So there is a tower of subfields $K \subset K(u_1) \subset K(u_1, u_2) \subset \cdots \subset K(u_1, u_2, \ldots, u_n)$. For a given $i \geq 2$, u_i is algebraic over K and so u_i is algebraic over $K(u_1, u_2, \ldots, u_{i-1})$, say u_i is of degree r_i over $K(u_1, u_2, \ldots, u_{i-1})$. Since $K(u_1, u_2, \ldots, u_{i-1})(u_i) = K(u_1, u_2, \ldots, u_i)$ by Exercise V.1.4(b), we have $[K(u_1, u_2, \ldots, u_i) : K(u_1, u_2, \ldots, u_{i-1})] = r_i$ by Theorem V.1.6(iii).

Theorem V.1.12 (continued)

Theorem V.1.12. If F is an extension field of K and X is a subset of F such that $F = K(X)$ and every element of X is algebraic over K, then F is an algebraic extension of K. If X is a finite set, then F is finite dimensional over K.

Proof (continued). Let r_1 be the degree of u_1 over K (we had $i \geq 2$ above), then by repeated (i.e., inductive) application of Theorem V.1.2 shows that $[K(u_1, u_2, \ldots, u_n) : K] = r_1 r_2 \cdots r_n$. By Theorem V.1.11, $K(u_1, u_2, \ldots, u_n)$ (since the dimension $r_1 r_2 \cdots r_n$ if finite) is algebraic over K and so $v \in K(u_1, u_2, \ldots, u_n)$ is algebraic over K. Since v was an arbitrary element of F, then F is algebraic over K.

Theorem V.1.12 (continued)

Theorem V.1.12. If F is an extension field of K and X is a subset of F such that $F = K(X)$ and every element of X is algebraic over K, then F is an algebraic extension of K. If X is a finite set, then F is finite dimensional over K.

Proof (continued). Let r_1 be the degree of u_1 over K (we had $i \geq 2$ above), then by repeated (i.e., inductive) application of Theorem V.1.2 shows that $[K(u_1, u_2, \ldots, u_n) : K] = r_1 r_2 \cdots r_n$. By Theorem V.1.11, $K(u_1, u_2, \ldots, u_n)$ (since the dimension $r_1 r_2 \cdots r_n$ if finite) is algebraic over K and so $v \in K(u_1, u_2, \ldots, u_n)$ is algebraic over K. Since v was an arbitrary element of F, then F is algebraic over K.

If X is a finite set, say $X = \{u_1, u_2, \ldots, u_n\}$, then as argued above $[F(u_1, u_2, \ldots, u_n) : K] = r_1 r_2 \cdots r_n$ is finite. □

Theorem V.1.12 (continued)

Theorem V.1.12. If F is an extension field of K and X is a subset of F such that $F = K(X)$ and every element of X is algebraic over K, then F is an algebraic extension of K. If X is a finite set, then F is finite dimensional over K.

Proof (continued). Let r_1 be the degree of u_1 over K (we had $i \geq 2$ above), then by repeated (i.e., inductive) application of Theorem V.1.2 shows that $[K(u_1, u_2, \ldots, u_n) : K] = r_1 r_2 \cdots r_n$. By Theorem V.1.11, $K(u_1, u_2, \ldots, u_n)$ (since the dimension $r_1 r_2 \cdots r_n$ if finite) is algebraic over K and so $v \in K(u_1, u_2, \ldots, u_n)$ is algebraic over K. Since v was an arbitrary element of F, then F is algebraic over K.

If X is a finite set, say $X = \{u_1, u_2, \ldots, u_n\}$, then as argued above $[F(u_1, u_2, \ldots, u_n) : K] = r_1 r_2 \cdots r_n$ is finite. □

Theorem V.1.13

Theorem V.1.13. If F is an algebraic extension field of E and E is an algebraic extension field of K, then F is an algebraic extension of K.

Proof. Let $u \in F$. Since F is an algebraic extension of E, then u is algebraic over E and so $b_n u^n + b_{n-1} u^{n-1} + \cdots b_1 u + b_0 = 0$ for some $b_i \in E$ (where $b_n \neq 0$). Therefore, u is algebraic over the subfield $K(b_0, b_1, \ldots, b_n)$ of E.

Theorem V.1.13

Theorem V.1.13. If F is an algebraic extension field of E and E is an algebraic extension field of K, then F is an algebraic extension of K.

Proof. Let $u \in F$. Since F is an algebraic extension of E, then u is algebraic over E and so $b_n u^n + b_{n-1} u^{n-1} + \cdots b_1 u + b_0 = 0$ for some $b_i \in E$ (where $b_n \neq 0$). Therefore, u is algebraic over the subfield $K(b_0, b_1, \ldots, b_n)$ of E. Consequently, there is a tower of fields $K \subset K(b_0, b_1, \ldots, b_n) \subset K(b_0, b_1, \ldots, b_n)(u)$, where $[K(b_0, b_1, \ldots, b_n)(u) : K(b_0, b_1, \ldots, b_n)]$ is finite by Theorem V.1.6(iii) since u is algebraic over $K(b_0, b_1, \ldots, b_n)$, and $[K(b_0, b_1, \ldots, b_n) : K]$ is finite by Theorem V.1.6(iii) since u is algebraic over $K(b_0, b_1, \ldots, b_n)$, and $[K(b_0, b_1, \ldots, b_n) : K]$ is finite by Theorem V.1.12 since there is a finite number of b_i and each is algebraic over K.

Theorem V.1.13

Theorem V.1.13. If F is an algebraic extension field of E and E is an algebraic extension field of K, then F is an algebraic extension of K.

Proof. Let $u \in F$. Since F is an algebraic extension of E, then u is algebraic over E and so $b_n u^n + b_{n-1} u^{n-1} + \cdots b_1 u + b_0 = 0$ for some $b_i \in E$ (where $b_n \neq 0$). Therefore, u is algebraic over the subfield $K(b_0, b_1, \ldots, b_n)$ of E. Consequently, there is a tower of fields $K \subset K(b_0, b_1, \ldots, b_n) \subset K(b_0, b_1, \ldots, b_n)(u)$, where $[K(b_0, b_1, \ldots, b_n)(u) : K(b_0, b_1, \ldots, b_n)]$ is finite by Theorem V.1.6(iii) since u is algebraic over $K(b_0, b_1, \ldots, b_n)$, and $[K(b_0, b_1, \ldots, b_n) : K]$ is finite by Theorem V.1.6(iii) since u is algebraic over $K(b_0, b_1, \ldots, b_n)$, and $[K(b_0, b_1, \ldots, b_n) : K]$ is finite by Theorem V.1.12 since there is a finite number of b_i and each is algebraic over K. Therefore $[K(b_0, b_1, \ldots, b_n)(u) : K]$ is finite by Theorem V.1.2. Hence, by Theorem V.1.11, u is algebraic over K. Since $u \in F$ is arbitrary, then F is algebraic over K. □

Theorem V.1.13

Theorem V.1.13. If F is an algebraic extension field of E and E is an algebraic extension field of K, then F is an algebraic extension of K.

Proof. Let $u \in F$. Since F is an algebraic extension of E, then u is algebraic over E and so $b_n u^n + b_{n-1} u^{n-1} + \cdots b_1 u + b_0 = 0$ for some $b_i \in E$ (where $b_n \neq 0$). Therefore, u is algebraic over the subfield $K(b_0, b_1, \ldots, b_n)$ of E. Consequently, there is a tower of fields $K \subset K(b_0, b_1, \ldots, b_n) \subset K(b_0, b_1, \ldots, b_n)(u)$, where $[K(b_0, b_1, \ldots, b_n)(u) : K(b_0, b_1, \ldots, b_n)]$ is finite by Theorem V.1.6(iii) since u is algebraic over $K(b_0, b_1, \ldots, b_n)$, and $[K(b_0, b_1, \ldots, b_n) : K]$ is finite by Theorem V.1.6(iii) since u is algebraic over $K(b_0, b_1, \ldots, b_n)$, and $[K(b_0, b_1, \ldots, b_n) : K]$ is finite by Theorem V.1.12 since there is a finite number of b_i and each is algebraic over K. Therefore $[K(b_0, b_1, \ldots, b_n)(u) : K]$ is finite by Theorem V.1.2. Hence, by Theorem V.1.11, u is algebraic over K. Since $u \in F$ is arbitrary, then F is algebraic over K. □

Theorem V.1.14

Theorem V.1.14. Let F be an extension field of K and E the set of all elements of F which are algebraic over K. Then E is a subfield of F (which is, of course, algebraic over K).

Proof. For any $u, v \in E$, $K(u, v)$ is an algebraic extension of K by Theorem V.1.12 (since there is a finite number of algebraic elements "adjoined" to K). Since $K(u, v)$ is a field, then $u - v \in K(u, v)$ and $uv^{-1} \in K(u, v)$ for $v \neq 0$.

Theorem V.1.14

Theorem V.1.14. Let F be an extension field of K and E the set of all elements of F which are algebraic over K. Then E is a subfield of F (which is, of course, algebraic over K).

Proof. For any $u, v \in E$, $K(u, v)$ is an algebraic extension of K by Theorem V.1.12 (since there is a finite number of algebraic elements "adjoined" to K). Since $K(u, v)$ is a field, then $u - v \in K(u, v)$ and $uv^{-1} \in K(u, v)$ for $v \neq 0$. Hence $u - v \in E$ and $uv^{-1} \in E$ (since $K(u, v) \subset E$) and so by Theorem I.2.5, $\langle E, + \rangle$ is a group and $\langle E \setminus \{0\}, \times \rangle$ is a group. Therefore E is a field. □

Theorem V.1.14

Theorem V.1.14. Let F be an extension field of K and E the set of all elements of F which are algebraic over K. Then E is a subfield of F (which is, of course, algebraic over K).

Proof. For any $u, v \in E$, $K(u, v)$ is an algebraic extension of K by Theorem V.1.12 (since there is a finite number of algebraic elements "adjoined" to K). Since $K(u, v)$ is a field, then $u - v \in K(u, v)$ and $uv^{-1} \in K(u, v)$ for $v \neq 0$. Hence $u - v \in E$ and $uv^{-1} \in E$ (since $K(u, v) \subset E$) and so by Theorem I.2.5, $\langle E, + \rangle$ is a group and $\langle E \setminus \{0\}, \times \rangle$ is a group. Therefore E is a field. □