7. Ring Extensions and Field Extensions

7.1 Notation: Let S be a commutative **extension ring** of R, that is $R \subseteq S$, and let $U \subseteq S$. The **ring generated by** U over R, denoted by $R[U]$ (or by $R[u_1, \cdots, u_n]$ in the case that $U = \{u_1, \cdots, u_n\}$), is the ring

$$R[U] = \left\{ f(u_1, \cdots, u_n) \middle| n \in \mathbf{N}, f \in R[x_1, \cdots, x_n] \right\}.$$

The R**-module generated by** U (or **spanned by** U) over R is the R-module

$$\text{span}_R U = \left\{ \sum_{i=1}^{n} a_i u_i \middle| n \in \mathbf{N}, a_i \in R, u_i \in U \right\}.$$

We also say that U **spans** the set $\text{span}_R U$ over R. Notice that $U \subseteq \text{span}_R U \subseteq R[U]$.

An element $u \in S$ is called **integral** over R if u is a root of some monic polynomial $f \in R[x]$. We say that S is **integral** over R if every element in S is integral over R.

7.2 Example: Verify that $\sqrt{2}$ is integral over $\mathbf{Z}$, $\frac{1}{2}$ is not integral over $\mathbf{Z}$, $x \in \mathbf{F}[x]$ is integral over $\mathbf{F}[x^2]$, and $\frac{1}{x} \in \mathbf{F}(x)$ is not integral over $\mathbf{F}[x]$.

7.3 Note: Let R, S and T be commutative rings with $R \subseteq S \subseteq T$. Notice that if $S = \text{span}_R\{u_1, \cdots, u_n\}$ and $T = \text{span}_S\{v_1, \cdots, v_m\}$ then $T = \text{span}_R\{u_i v_j\}$. Indeed, given $t \in T$, we can write $t = \sum s_j v_j$ for some $s_j \in S$, and we can write each s_j as $s_j = \sum r_{ij} u_i$ for some $r_{ij} \in R$, and then $t = \sum_{i,j} r_{ij} u_i v_j \in \text{span}_R\{u_i v_j\}$.

7.4 Theorem: *Let R and S be integral domains with $R \subseteq S$ and let $u \in S$. Then the following statements are equivalent.*

(1) u is integral over R.
(2) $R[u]$ is finitely generated as an R-module.
(3) $R[u]$ is contained in some ring $T \subseteq S$ which is finitely generated as an R-module.
(4) $R[u]$ is integral over R.

Proof: First we show that (1) $\Longrightarrow$ (2). Suppose that u is integral over R. Choose a monic polynomial $f \in R[x]$ such that $f(u) = 0$, and say $\deg(f) = n$. Let $a \in R[u]$, say $a = g(u)$ where $g \in R[x]$. Since f is monic, we can use the division algorithm to write $g = fq + r$ where $q, r \in R[x]$ and $\deg(r) < n$. Since $f(u) = 0$ we have $a = g(u) = r(u)$. And since $\deg(r) < n$, we have $r(u) \in \text{span}_R\{1, u, u^2, \cdots, u^{n-1}\}$. Thus $R[u] = \text{span}_R\{1, u, \cdots, u^{n-1}\}$.

The implication (2) $\Longrightarrow$ (3) is clear (simply let $T = R[u]$), so we show next that (3) $\Longrightarrow$ (4). Suppose that $R[u] \subseteq T = \text{span}_R\{v_1, \cdots, v_n\} \subseteq S$, and let $w \in R[u]$. Then for each $i = 1, \cdots, n$, we have $w\, v_i \in T = \text{span}_R\{v_1, \cdots, v_n\}$, so we can write $w\, v_i = \sum_{i=1}^{n} a_{ij} v_j$ for some $a_{ij} \in R$. Let A be the $n \times n$ matrix with entries a_{ij}, and let v be the $n \times 1$ matrix with entries v_i. Then we have $(wI)v = Av$ so $(wI - A)\, v = 0$. Since $v \neq 0$, this implies that $\det(uI - A) = 0$ in the quotient field of S. Thus w is a root of the monic polynomial $f(x) = \det(xI - A)$, which is in $R[x]$, so w is integral over R. This shows that $R[u]$ is integral over R.

Finally note that (4) clearly implies (1).

7.5 Corollary: *Let R, S and T be commutative rings with $R \subseteq S \subseteq T$. Suppose that T is integral over S, and S is integral over R. Then T is integral over R.*

Proof: Let $t \in T$. Then t is integral over S. Say $a_0 + a_1 t + \cdots + a_{n-1}t^{n-1} + t^n = 0$ with each $a_i \in S$. Since each $a_i \in R[a_0, \cdots, a_{n-1}]$, t is also integral over the ring $R[a_0, \cdots, a_{n-1}]$. By the above theorem, there is a finite set which spans $R[a_0, \cdots, a_{n-1}, t]$ over $R[a_0, \cdots, a_{n-1}]$. But since each a_k is integral over R and hence also over $R[a_0, \cdots, a_{k-1}]$, we have a chain of ring extensions $R \subseteq R[a_0] \subseteq \cdots \subseteq R[a_1, \cdots, a_{n-1}] \subseteq R[a_0, \cdots, a_{n-1}, t]$ in which each ring is spanned by a finite set over the previous ring. By the above note, this implies that $R[a_0, \cdots, a_{n-1}, t]$ is spanned by a finite set over R

7.6 Definition: Let S be a commutative extension ring of R. When A is an ideal in R and B is an ideal in S with $B \cap R = A$ we say that B **lies over** A.

7.7 Theorem: *(The Lying Over Theorem) Let R and S be integral domains with $R \subseteq S$ and with S integral over R.*

(1) If $M \subseteq R$ is a maximal ideal then there is a maximal ideal $N \subseteq S$ such that $N \cap R = M$.
(2) If $P \subseteq R$ is a prime ideal then there is a prime ideal $Q \subseteq S$ such that $Q \cap R = P$.

Proof: We only provide a proof of Part (1). Let $\mathcal{U}$ be the set of all ideals $A \subseteq S$ such that $A \cap R \subseteq M$. Then $\mathcal{U}$ is not empty since $\{0\} \in \mathcal{U}$, and every chain of ideals $A_1 \subseteq A_2 \subseteq \cdots$ in $\mathcal{U}$ has an upper bound in $\mathcal{U}$, namely the ideal $\bigcup_{i=1}^{\infty} A_i$, so by Zorn's Lemma, $\mathcal{U}$ has a maximal element, say N. We shall show that in fact N is a maximal ideal in S and that $N \cap R = M$.

First, we shall show that $N \cap R = M$. Since $N \in \mathcal{U}$ we know that $N \cap R \subseteq M$. Suppose, for a contradiction, that $N \cap R \subsetneqq M$. Choose $m \in M \setminus (N \cap R)$. Then $N \subsetneqq N + mS$. We cannot have $(N + mS) \cap R \subseteq M$ since otherwise $N + mS$ would be in $\mathcal{U}$ and then N would not be maximal in $\mathcal{U}$. So we can choose $r \in N + mS$ with $r \in R$ but $r \notin M$. Since $r \in N + mS$, we can write $r = n + ms$ for some $n \in N$, $s \in S$, and then $ms = r - n$. Since S is integral over R and $s \in S$, we have $0 = a_0 + a_1 s + \cdots + a_{k-1}s^{k-1} + s^k$ for some $a_i \in R$. Multiply this by m^k to get

$$\begin{aligned} 0 &= a_0 m^k + a_1 m^{k-1}(ms) + \cdots + a_{k-1} m (ms)^{k-1} + (ms)^k \\ &= a_0 m^k + a_1 m^{k-1}(r-n) + \cdots + a_{k-1} m (r-n)^{k-1} + (r-n)^k . \end{aligned}$$

After expanding this expression, all the terms involving n lie in N, and hence the sum of the remaining terms, which is $u = a_0 m^k + a_1 m^{k-1} r + \cdots + a_{k-1} m r^{k-1} + r^k$, must also lie in N. But notice that we also have $u \in R$, so $u \in N \cap R \subseteq M$. All the terms involving m lie in M, so the remaining term r^k also lies in M. Since M is maximal and hence prime, we also have $r \in M$. This gives the desired contradiction, since $r \notin M$. We leave it as a short exercise to verify that N must be maximal.

7.8 Example: The ring $\mathbf{Z}[\sqrt{2}]$ is integral over the ring $\mathbf{Z}$, and the ideal $M = \langle 2 \rangle \subseteq \mathbf{Z}$ is maximal in $\mathbf{Z}$. According to the Lying Over Theorem, we should be able to find a maximal ideal $N \subseteq \mathbf{Z}[\sqrt{2}]$ which lies over M. If we let $A = \langle 2 \rangle \subseteq \mathbf{Z}[\sqrt{2}]$ then $A \cap \mathbf{Z} = M$, but A is not maximal in $\mathbf{Z}[\sqrt{2}]$. If we let $N = \langle \sqrt{2} \rangle \subseteq \mathbf{Z}[\sqrt{2}]$, then N is maximal and $N \cap \mathbf{Z} = M$.

For a similar illustration, note that the ring $\mathbf{F}[x]$ is integral over $\mathbf{F}[x^2]$. The ideal $M = \langle x^2 \rangle \subseteq \mathbf{F}[x^2]$ is maximal in $\mathbf{F}[x^2]$, so by the Lying Over Theorem we should be able to find a maximal ideal $N \subseteq \mathbf{F}[x]$ which lies over M. If we let $A = \langle x^2 \rangle \subseteq \mathbf{F}[x]$, then we have $A \cap \mathbf{F}[x^2] = M$, but A is not maximal. If we let $N = \langle x \rangle \subseteq \mathbf{F}[x]$ then N is maximal and $N \cap \mathbf{F}[x^2] = M$.

7.9 Definition: Let $\mathbf{F}$ be a subfield of $\mathbf{K}$. We denote the **field of rational functions** over $\mathbf{F}$ on the variables $x_1, \cdots, x_n$ by $\mathbf{F}(x_1, \cdots, x_n)$. It is the quotient field of the integral domain $\mathbf{F}[x_1, \cdots, x_n]$. The elements of $\mathbf{F}(x_1, \cdots, x_n)$ can be written in the form $f = p/q$ for some $p, q \in \mathbf{F}[x_1, \cdots, x_n]$ with $q \neq 0$, and we have

$$\frac{p}{q} = \frac{r}{s} \in \mathbf{F}(x_1, \cdots, x_n) \iff ps - qr = 0 \in \mathbf{F}[x_1, \cdots, x_n] .$$

For $U \subseteq \mathbf{K}$, the **field generated** by U over $\mathbf{F}$, denoted by $\mathbf{F}(U)$ (or by $f(u_1, \cdots, u_n)$ in the case that $U = \{u_1, \cdots, u_n\}$) is the field

$$\mathbf{F}(U) = \left\{ \frac{f(u_1, \cdots, u_n)}{g(u_1, \cdots, u_n)} \;\middle|\; n \in \mathbf{N}, u_1, \cdots, u_n \in U, f, g \in \mathbf{F}[x_1, \cdots, x_n], g(u_1, \cdots, u_n) \neq 0 \right\} .$$

An element $u \in \mathbf{K}$ is called **algebraic** over $\mathbf{F}$ if u is the root of some polynomial $f \in \mathbf{F}[x]$, otherwise u is called **transcendental** over $\mathbf{F}$. If u is algebraic over $\mathbf{F}$ for every $u \in \mathbf{K}$ then $\mathbf{K}$ is **algebraic** over $\mathbf{F}$, otherwise $\mathbf{K}$ is **transcendental** over $\mathbf{F}$.

7.10 Example: $\mathbf{C}$ is algebraic over $\mathbf{R}$, $\mathbf{R}$ is transcendental over $\mathbf{Q}$, and for any field $\mathbf{F}$, the element $x \in \mathbf{F}(x)$ is transcendental over $\mathbf{F}$.

7.11 Theorem: *Let $\mathbf{F} \subseteq \mathbf{K} \subseteq \mathbf{L}$ be fields.*

(1) If $u \in \mathbf{K}$ is algebraic over $\mathbf{F}$ then there is a unique monic irreducible polynomial $f \in \mathbf{F}[x]$, called the **irreducible polynomial of** *u, such that $f(u) = 0$ in $\mathbf{K}$.*
(2) If $u \in \mathbf{K}$ is algebraic over $\mathbf{F}$ then $\mathbf{F}[u] = \mathbf{F}(u) \cong \mathbf{F}[x]/\langle f \rangle$, where f is the irreducible polynomial of u, and if $\deg(f) = n$ then $\{1, u, \cdots, u^{n-1}\}$ forms a basis for $\mathbf{F}[u]$ as a vector space over $\mathbf{F}$.
(3) If $u \in \mathbf{K}$ is transcendental over $\mathbf{F}$ then $\mathbf{F}[u] \subsetneqq \mathbf{F}(u)$, $\mathbf{F}[u] \cong \mathbf{F}[x]$, $\mathbf{F}(u) \cong \mathbf{F}(x)$ and the dimension of $\mathbf{F}(u)$ over $\mathbf{F}$ is infinite.
(4) If every element of a subset $U \subseteq \mathbf{K}$ is algebraic over $\mathbf{F}$ then $\mathbf{F}(U)$ is algebraic over $\mathbf{F}$.
(5) If $\mathbf{L}$ is algebraic over $\mathbf{K}$, and $\mathbf{K}$ is algebraic over $\mathbf{F}$, then $\mathbf{L}$ is algebraic over $\mathbf{F}$.

Proof: We omit the proof

7.12 Definition: Let $\mathbf{F} \subseteq \mathbf{K}$ be fields. For $f \in \mathbf{F}[x]$, we say that f **splits** in $\mathbf{K}[x]$ when f factors as a product of linear polynomials in $\mathbf{K}[x]$. Note that when f splits in $\mathbf{K}[x]$ the roots of f all lie in $\mathbf{K}$. For $f \in \mathbf{F}[x]$, we say that $\mathbf{K}$ is a **splitting field** of f when f splits in $\mathbf{K}[x]$ and $\mathbf{K}$ is generated over $\mathbf{F}$ by the roots of f. For a set of polynomials $S \subseteq \mathbf{F}[x]$, we say that $\mathbf{K}$ is a **splitting field** of S when every $f \in S$ splits in $\mathbf{K}[x]$ and $\mathbf{K}$ is generated over $\mathbf{F}$ by the roots of all the polynomials in S.

7.13 Theorem: *Let $\mathbf{F}$ be a field and let $S \subseteq \mathbf{F}[x]$. Then there exists a splitting field $\mathbf{K}$ of S, and it is unique up to isomorphism.*

Proof: We omit the proof.

7.14 Definition: Let $\mathbf{F} \subseteq \mathbf{K}$ be fields. We say that $\mathbf{K}$ is **algebraically closed** when every $f \in \mathbf{K}[x]$ splits in $\mathbf{K}[x]$. We say that $\mathbf{K}$ is the **algebraic closure** of $\mathbf{F}$ when $\mathbf{K}$ is algebraic over $\mathbf{F}$ and $\mathbf{K}$ is algebraically closed.

7.15 Theorem: *Let $\mathbf{F}$ be a field. Then there exists an algebraic closure $\mathbf{K}$ of $\mathbf{F}$, it is unique up to isomorphism, and it is the splitting field of the set $\mathbf{F}[x]$ of all polynomials over $\mathbf{F}$.*

Proof: We omit the proof.

7.16 Definition: Let $\mathbf{F} \subseteq \mathbf{K}$ be fields. A subset $U \subseteq \mathbf{K}$ is said to be **algebraically independent** over $\mathbf{F}$ when for every $n \in \mathbf{Z}^+$, for every $0 \neq f \in \mathbf{F}[x_1, \cdots, x_n]$, and for all distinct elements $u_1, u_2, \cdots, u_n \in U$, we have $f(u_1, \cdots, u_n) \neq 0$. In particular, the empty set is algebraically independent over $\mathbf{F}$. A **transcendence basis** for $\mathbf{K}$ over $\mathbf{F}$ is a maximal algebraically independent set.

7.17 Note: We can see that $\{x_1, \cdots, x_n\}$ is a transcendence basis for $\mathbf{F}(x_1, \cdots, x_n)$ over $\mathbf{F}$ as follows. First note that $\{x_1, \cdots, x_n\}$ is algebraically independent over $\mathbf{F}$, since for $f \in \mathbf{F}[t_1, \cdots, t_n]$, if $f(x_1, \cdots, x_n) = 0 \in \mathbf{F}(x_1, \cdots, x_n)$ then $f = 0 \in \mathbf{F}[t_1, \cdots, t_n]$. Then, note that $\{x_1, \cdots, x_n\}$ is a maximal algebraically independent set, since given any element $\frac{p(x_1, \cdots, x_n)}{q(x_1, \cdots, x_n)} \in \mathbf{F}(x_1, \cdots, x_n)$ we can let $f(t_1, \cdots, t_{n+1}) = p(t_1, \cdots, t_n) - q(t_1, \cdots, t_n)t_{n+1}$, and then $f \neq 0 \in \mathbf{F}[t_1, \cdots, t_{n+1}]$ but $f\big(x_1, \cdots, x_n, \frac{p(x_1, \cdots, x_n)}{q(x_1, \cdots, x_n)}\big) = 0 \in \mathbf{F}(x_1, \cdots, x_n)$, which shows that $\big\{x_1, \cdots, x_n, \frac{p(x_1, \cdots, x_n)}{q(x_1, \cdots, x_n)}\big\}$ is algebraically dependent over $\mathbf{F}$.

7.18 Note: If $\{u_1, \cdots, u_n\}$ is algebraically independent over $\mathbf{F}$ then we have natural isomorphisms $\mathbf{F}[u_1, \cdots, u_n] \cong \mathbf{F}[x_1, \cdots, x_n]$ and $\mathbf{F}(u_1, \cdots, u_n) \cong \mathbf{F}(x_1, \cdots, x_n)$. Indeed the maps $\phi : \mathbf{F}[x_1, \cdots, x_n] \to \mathbf{F}[u_1, \cdots, u_n]$ and $\phi : \mathbf{F}(x_1, \cdots, x_n) \to \mathbf{F}(u_1, \cdots, u_n)$ induced by $\phi(x_i) = u_i$ are easily seen to give isomorphisms; the fact that $\{u_1, \cdots, u_n\}$ is algebraically independent ensures that $\ker \phi = \{0\}$.

7.19 Theorem: *Let $\mathbf{F} \subseteq \mathbf{K}$ be fields, let $U, V \subseteq \mathbf{K}$ and let $u \in \mathbf{K}$. Then*

(1) If U is algebraically independent over $\mathbf{F}$ then $\big($u is transcendental over $\mathbf{F}(U)$ if and only if $U \cup \{u\}$ is algebraically independent over $\mathbf{F}\big)$.
(2) U is a transcendence basis for $\mathbf{K}$ over $\mathbf{F}$ if and only if $\big(U$ is algebraically independent over $\mathbf{F}$ and $\mathbf{K}$ is algebraic over $\mathbf{F}(U)\big)$.
(3) If $\mathbf{K}$ is algebraic over $\mathbf{F}(U)$, then U contains a transcendence basis for $\mathbf{K}$ over $\mathbf{F}$. In particular, a transcendence basis for $\mathbf{K}$ over $\mathbf{F}$ does exist.
(4) If U is algebraically independent over $\mathbf{F}$ then U can be extended to a transcendence basis for $\mathbf{K}$ over $\mathbf{F}$.
(5) If U and V are both transcendence bases for $\mathbf{K}$ over $\mathbf{F}$, then U and V have the same cardinality.

Proof: To prove part (1), let U be algebraically independent over $\mathbf{F}$. Suppose that u is algebraic over $\mathbf{F}(U)$, say $f(u) = 0$ where $0 \neq f \in \mathbf{F}(U)[t]$. Write $f = a_0 + a_1 t + \cdots + a_k t^k$ with each $a_i \in \mathbf{F}(U)$ and $a_k \neq 0$, and say $a_i = \frac{p(u_1, \cdots, u_n)}{q(u_1, \cdots, u_n)}$ where $p_i, q_i \in \mathbf{F}[x_1, \cdots, x_n]$. Set $g(x_1, \cdots, x_{n+1}) = \frac{p_0(x_1, \cdots, x_n)}{q_0(x_1, \cdots, x_n)} + \frac{p_1(x_1, \cdots, x_n)}{q_1(x_1, \cdots, x_n)} x_{n+1} + \cdots + \frac{p_k(x_1, \cdots, x_n)}{q_k(x_1, \cdots, x_n)} {x_{n+1}}^k$ so that we have $0 \neq g \in \mathbf{F}(x_1, \cdots, x_n)[x_{n+1}]$ and $g(u_1, \cdots, u_n, u) = f(u) = 0 \in \mathbf{K}$. By multiplying g by a common multiple of the denominators q_i, we obtain a polynomial $0 \neq h \in \mathbf{F}[x_1, \cdots, x_{n+1}]$ such that $h(u_1, \cdots, u_n, u) = 0 \in \mathbf{K}$, and thus we see that $U \cup \{u\}$ is algebraically dependent.

Conversely, suppose that the set $U \cup \{u\}$ is algebraically dependent over $\mathbf{F}$, say $f(u_1, \cdots, u_n, u) = 0 \in \mathbf{K}$ where $0 \neq f \in \mathbf{F}[x_1, \cdots, x_{n+1}]$ and $u_1, \cdots, u_n \in U$. Write $f = a_0 + a_1 x_{n+1} + \cdots + a_k {x_{n+1}}^k$ with each $a_i \in \mathbf{F}[x_1, \cdots, x_n]$ and $a_k \neq 0$, then let $g(t) = f(u_1, \cdots, u_n, t) = a_0(u_1, \cdots, u_n) + a_1(u_1, \cdots, u_n)t + \cdots + a_k(u_1, \cdots, u_n)t^k$ so that $g \in \mathbf{F}(U)[t]$ and $g(u) = 0 \in \mathbf{K}$. If we had $g = 0 \in \mathbf{F}(U)[t]$ then we would have $a_k(u_1, \cdots, u_n) = 0 \in \mathbf{K}$, but $a_k(u_1, \cdots, u_n) \neq 0$ since $a_k \neq 0 \in \mathbf{F}[x_1, \cdots, x_n]$ and U is algebraically independent. Since $g \neq 0 \in \mathbf{F}(U)[t]$ and $g(u) = 0 \in \mathbf{K}$, it follows that u is algebraic over $\mathbf{F}(U)$.

Part (2) follows easily from part (1). To prove part (3), suppose that $\mathbf{K}$ is algebraic over $\mathbf{F}(U)$. Let $\mathcal{U}$ be the collection of all subsets of U which are algebraically independent over $\mathbf{F}$. Then $\mathcal{U} \neq \emptyset$ since $\emptyset \in \mathcal{U}$, and every chain $U_1 \subseteq U_2 \subseteq \cdots$ in $\mathcal{U}$ has an upper bound in $\mathcal{U}$, namely $\bigcup_{i=1}^{\infty} U_i$, and so by Zorn's Lemma, $\mathcal{U}$ has a maximal element, say V. We claim that V is a transcendence basis for $\mathbf{K}$ over $\mathbf{F}$. Every $u \in U$ is algebraic over $\mathbf{F}(V)$ (otherwise, by part (1), $V \cup \{u\}$ would be algebraically independent so that $V \subsetneqq V \cup \{u\} \in \mathcal{U}$) and so $\mathbf{F}(U)$ is algebraic over $\mathbf{F}(V)$. This implies that $\mathbf{K}$ is algebraic over $\mathbf{F}(V)$ (since $\mathbf{K}$ is algebraic over $\mathbf{F}(U)$ which is algebraic over $\mathbf{F}(V)$). So by part (2), V is a transcendence basis for $\mathbf{K}$ over $\mathbf{F}$. Part (4) can be proven similarly using Zorn's Lemma.

Finally, we prove part (5), but only in the case that at least one of the two transcendence bases is finite. Let $U = \{u_1, \cdots, u_n\}$ be a transcendence basis for $\mathbf{K}$ over $\mathbf{F}$, and let V be another tanscendence basis. We claim that there is an element $v_1 \in V$ such that v_1 is transcendental over $\mathbf{F}(u_2, \cdots, u_n)$. Suppose not. Then every $v \in V$ would be algebraic over $\mathbf{F}(u_2, \cdots, u_n)$ and so $\mathbf{F}(u_2, \cdots, u_n)(V)$ would be algebraic over $\mathbf{F}(u_2, \cdots, u_n)$. Also, $\mathbf{K}$ is algebraic over $\mathbf{F}(V)$ (by part (2), since V is a transcendence basis), and hence also over $\mathbf{F}(u_2, \cdots, u_n)(V)$, So we would have $\mathbf{K}$ algebraic over $\mathbf{F}(u_2, \cdots, u_n)$, and in particular u_1 would be algebraic over $\mathbf{F}(u_2, \cdots, u_n)$, and this is not possible since U is algebraically independent. This proves the claim, so we choose $v_1 \in V$ transcendental over $\mathbf{F}(u_2, \cdots, u_n)$.

Now we claim that $\{v_1, u_2, \cdots, u_n\}$ is another transcendence basis for $\mathbf{K}$ over $\mathbf{F}$. Since v_1 is transcendental over $\mathbf{F}(u_2, \cdots, u_n)$, we know (from part 1) that $\{v_1, u_2, \cdots, u_n\}$ is algebraically independent. Also, u_1 must be algebraic over $\mathbf{F}(v_1, u_2, \cdots, u_n)$, (otherwise $\{v_1, u_1, u_2, \cdots, u_n\}$ would be algebraically independent so U would not be a transcendence basis) and so $\mathbf{F}(v_1, u_1, u_2, \cdots, u_n)$ is algebraic over $\mathbf{F}(v_1, u_2, \cdots, u_n)$. Furthermore, $\mathbf{K}$ is algebraic over $\mathbf{F}(u_1, u_2, \cdots, u_n)$ and hence over $\mathbf{F}(v_1, u_1, u_2, \cdots, u_n)$, and so $\mathbf{K}$ is algebraic over $\mathbf{F}(v_1, u_2, \cdots, u_n)$. Thus $\{v_1, u_2, \cdots, u_n\}$ is a transcendence basis by part (2).

By repeating the above procedure, we can choose $v_k \in V$ for $1 \leq k \leq n$ so that $\{v_1, \cdots, v_k, u_{k+1}, \cdots, u_n\}$ is a transcendence basis for $\mathbf{K}$ over $\mathbf{F}$. The procedure must end when we have chosen v_n, and we must have $V = \{v_1, \cdots, v_n\}$.

7.20 Definition: Let $\mathbf{F} \subseteq \mathbf{K}$ be fields. We define the **transcendence degree** of $\mathbf{K}$ over $\mathbf{F}$, written $\text{trans}_{\mathbf{F}}\mathbf{K}$, to be the cardinality of any transcendence basis for $\mathbf{K}$ over $\mathbf{F}$.

7.21 Definition: We define the **dimension** of an irreducible variety $X \subseteq \mathbf{F}^n$ to be the transcendence degree $\dim(X) = \text{trans}_{\mathbf{F}}K(X)$.

7.22 Example: When $X = \{a\}$ with $a \in \mathbf{F}^n$ we have $\dim(X) = 0$ because $\emptyset$ is a transcendence basis for $K(X) = \mathbf{F}$, and when $\mathbf{F}$ is infinite and $X = \mathbf{F}^n$ we have $\dim(X) = n$ because $\{x_1, \cdots, x_n\}$ is a transcendence basis for $K(X) = \mathbf{F}(x_1, \cdots, x_n)$.

7.23 Note: When X and Y are irreducible affine varieties and $f : Y \to X$ is a dominant polynomial or rational map, the pullback $f^* : K(X) \to K(Y)$ is injective so we have $K(X) \cong f^*\big(K(X)\big) \subseteq K(Y)$. It folows that $\dim(X) \leq \dim(Y)$ with $\dim(X) = \dim(Y)$ if and only if $K(Y)$ is algebraic over $f^*\big(K(X)\big)$.

7.24 Theorem: *(Noether's Normalization Lemma) Let* $\mathbf{F}$ *be a field and let* R *be an integral domain of the form* $\mathbf{F}[u_1, \cdots, u_n]$. *Let* $r = \operatorname{trans}_{\mathbf{F}}\mathbf{F}(u_1, \cdots, u_n)$. *Then there is a set of* r *points* $\{v_1, \cdots, v_r\} \subseteq R$ *which is algebraically independent over* $\mathbf{F}$ *such that* R *is integral over* $\mathbf{F}[v_1, \cdots, v_r]$

Proof: If $\{u_1, \cdots, u_n\}$ is algebraically independent over $\mathbf{F}$, then $r = n$ and we can take $v_i = u_i$ and we are done. Suppose that $\{u_1, \cdots, u_n\}$ is algebraically dependent over $\mathbf{F}$, so $r < n$. Choose a nonzero polynomial $f \in \mathbf{F}[x_1, \cdots, x_n]$ such that $f(u_1, \cdots, u_n) = 0$, say $f = \sum_{(i_1,\cdots,i_n)\in I} c_{i_1,\cdots,i_n} {x_1}^{i_1} \cdots {x_n}^{i_n}$, where the coefficients in the sum are all non-zero. Choose an integer b which is larger than every i_j occurring any multi-index $(i_1, \cdots, i_n) \in I$, then think of each i_j as a digit in base b, so that the muli-indices in I determine distinct integers

$$(i_1, \cdots, i_n) \mapsto i_n + i_1 b + \cdots i_{n-1} b^{n-1} .$$

Now, for each $j = 1, \cdots, n-1$, let $v_j = u_j - {u_n}^{b^j}$ so that we have $u_j = v_j + {u_n}^{b^j}$. Notice that $\mathbf{F}[v_1, \cdots, v_{n-1}, u_n] = \mathbf{F}[u_1, \cdots, u_n] = R$. Also,

$$\begin{aligned} 0 = f(u_1, \cdots, u_n) &= f\big(v_1 + {u_n}^{b}, v_2 + {u_n}^{b^2}, \cdots, v_{n-1} + {u_n}^{b^{n-1}}, u_n\big) \\ &= \sum c_{i_1,\cdots,i_n} (v_1 + {u_n}^{b})^{i_1} \cdots \big(v_{n-1} + {u_n}^{b^{n-1}}\big)^{i_{n-1}} (u_n)^{i_n} . \end{aligned}$$

Since the integers $i_n + i_1 b + \cdots + i_{n-1} b^{n-1}$ are distinct for distinct multi-indices, the above sum has a unique term of highest order in u_n, say the term of multi-index $(k_1, \cdots, k_n)$. Thus u_n is a root of the monic polynomial $\frac{1}{c_{k_1,\cdots,k_n}} f\big(v_1 + t^b, v_1 + t^{b^2}, \cdots, v_1 + t^{b^{n-1}}, t\big)$ $\in \mathbf{F}[v_1, \cdots, v_{n-1}][t]$. This shows that u_n is integral over $\mathbf{F}[v_1, \cdots, v_{n-1}]$ and hence $R = \mathbf{F}[v_1, \cdots, v_{n-1}, u_n]$ is integral over $\mathbf{F}[v_1, \cdots, v_{n-1}]$. If $\{v_1, \cdots, v_{n-1}\}$ is algebraically independent then we have $r = n - 1$ and we are done. Otherwise, we can relabel each v_i as u_i and repeat the above procedure on $\mathbf{F}[u_1, \cdots, u_{n-1}]$.

7.25 Example: Let $R = \mathbf{F}\big[x, \frac{1}{x}\big] \subseteq \mathbf{F}(x)$. Find $v \in R$ such that R is integral over $\mathbf{F}[v]$.

Solution: The set $\big\{x, \frac{1}{x}\big\}$ is algebraically dependent since $\big(x, \frac{1}{x}\big)$ is a root of the polynomial $f(s,t) = st - 1 \in \mathbf{F}[s,t]$. As in the proof of Noether's Normalization Lemma, using the base $b = 2$, we let $v = x - \frac{1}{x^2}$ and then $R = \mathbf{F}\big[v, \frac{1}{x}\big]$ which is integral over $\mathbf{F}[v]$ since $\frac{1}{x}$ is a root of the monic polynomial $f(v + t^2, t) = (v + t^2)t - 1 = t^3 + vt - 1 \in \mathbf{F}[v][t]$.

The above element v, for which $R = \mathbf{F}\big[v, \frac{1}{x}\big]$ is integral over $\mathbf{F}[v]$, is not unique. For example, $v = x - \frac{1}{x}$ also works, and $\frac{1}{x}$ is a root of the monic polynomial $t^2 + vt - 1 \in \mathbf{F}[v][t]$.

7.26 Remark: When $f : X \to Y$ is a dominant rational map so that $f^* : A(Y) \to A(X)$ is injective, the ring $A(Y)$ is isomorphic to its image $f^*\big(A(Y)\big)$. When $A(X)$ is integral over $f^*\big(A(Y)\big)$ and the field $\mathbf{F}$ is algebraically closed, the map $f : X \to Y$ is surjective, and when $f(a) = b$, the maximal ideal $M \subseteq A(Y)$ corresponding to the point b lies over the maximal ideal $N \subseteq A(X)$ corresponding to the point a.

When $X = V(xy - 1)$ so that $A(X) = \mathbf{F}[x,y]/\langle xy - 1\rangle = \mathbf{F}\big[x, \frac{1}{x}\big]$, and $f : X \to \mathbf{F}$ is given by $f(x,y) = x$ so that $f^* : \mathbf{F}[t] \to \mathbf{F}\big[x, \frac{1}{x}\big]$ is given by $f^*(g)(x,y) = g(x)$, we have $f^*\big(\mathbf{F}[t]\big) = \mathbf{F}[x] \subseteq \mathbf{F}\big[x, \frac{1}{x}\big]$. In this case the map $f : X \to \mathbf{F}$ is not surjective and the ring $A(X) = \mathbf{F}\big[x, \frac{1}{x}\big]$ is not integral over the image $f^*\big(\mathbf{F}[t]\big) = \mathbf{F}[x]$.

When $X = V(xy-1)$ and $f : X \to \mathbf{F}$ is given by $f(x,y) = x - y$ so $f^* : \mathbf{F}[t] \to \mathbf{F}\big[x, \frac{1}{x}\big]$ is given by $f^*(g)(x,y) = g(x-y) = g\big(x - \frac{1}{x}\big)$, we have $f^*\big(\mathbf{F}[t]\big) = \mathbf{F}[v] \subseteq \mathbf{F}\big[x, \frac{1}{x}\big]$ where $v = x - \frac{1}{x}$ (as in the previous example). In this case the map $f : X \to \mathbf{F}$ is surjective and the ring $A(X) = \mathbf{F}\big[x, \frac{1}{x}\big]$ is integral over the image $f^*\big(\mathbf{F}[t]\big) = \mathbf{F}[v]$.