INTEGRAL EXTENSIONS, VALUATION RINGS, AND THE NULLSTELLENSATZ

K. N. RAGHAVAN

Conventions

Throughout this set of notes, a *ring* means a commutative ring with identity, ring homomorphisms respect identities, and modules are unital. A *subring* A of a ring B is a non-empty additively closed and multiplicatively closed subset of B containing the (multiplicative) identity of B.

The expression "$A \subseteq B$ is a *ring extension*" or "B is a ring extension of A" is often used in place of "A is a subring of a ring B". If $A \subseteq B$ is a ring extension, then B is naturally an A-module. A *subextension* of a ring extension B of a ring A is just a subring C of B containing A. Given a collection $\{b_\beta \,|\, \beta \in I\}$ of elements of B, the smallest subextension of B containing all the b_β is denoted $A[b_\beta \,|\, \beta \in I]$. This notation is justified as follows: $A[b_\beta \,|\, \beta \in I]$ is the image of the natural ring homomorphism from the polynomial ring $A[x_\beta \,|\, \beta \in I]$ to B defined by $x_\beta \mapsto b_\beta$.

1. Integral extensions

Let $A \subseteq B$ be a ring extension. Generalizing to rings the notion of algebraic elements and extensions from field theory, we say that an element b in B is *integral over A* if there exists a monic polynomial $f(x)$ in the variable x with coefficients in A such that $f(b) = 0$; we say that the extension is *integral* if every element of B is integral over A. We sometimes refer to the equation $f(b) = 0$ as above as an *integral equation for b over A*.

It is easy to see that if $A \subseteq B$ is integral then so are:

- $A/\mathfrak{b}^c \subseteq B/\mathfrak{b}$, where $\mathfrak{b}$ is any ideal of B and $\mathfrak{b}^c = A \cap \mathfrak{b}$ is its contraction to A.
- $S^{-1}A \subseteq S^{-1}B$, where S is any multiplicatively closed set of A.

There are two other natural definitions about a ring extension $A \subseteq B$:

- It is *finite* if B is finitely generated as an A-module. This notion generalizes that of finite extension of fields.
- It is *finitely generated* if there exist finitely many elements $b_1, \ldots, b_n$ of B such that $A[b_1, \ldots, b_n] = B$.[1]

These are notes of lectures given as part of the Ring Theory module of AFS-II during May 2014 at Almora. Corrections, comments, suggestions for improvement, criticisms, etc. are welcome. Please send them to the author at knr.imsc@gmail.com or knr@imsc.res.in.

[1] A field extension $E \subseteq F$ is said to be *finitely generated* if there exist finitely many elements $f_1, \ldots, f_n$ of F such that the smallest (field) subextension $E(f_1, \ldots, f_n)$ containing $f_1, \ldots, f_n$ equals F. As we will see later on, a field extension that is finitely generated as a ring extension is algebraic. This is one version of Hilbert's Nullstellensatz.

A finite extension is clearly finitely generated. As in the field case, we have:

$$\textit{A finite extension of a finite extension is finite.} \tag{1}$$

Proof: Indeed if $A \subseteq B$ and $B \subseteq C$ be finite extensions with $b_1, \ldots, b_m$ being a generating set for B as an A-module and $c_1, \ldots, c_n$ being a generating set for C as a B-module, then $b_i c_j$, $1 \leq i \leq m$ and $1 \leq j \leq n$, is a generating set for C as an A-module. □

Generalizing the well known fact that a finite field extension is algebraic, we have

$$\textit{A finite extension of rings is integral.} \tag{2}$$

Proof: This is more complicated than the standard proof in the field case[2]. Let $b_1, \ldots, b_n$ be a finite set of generators of B as an A-module. Given b in B, we may write $bb_j = a_{j1}b_1 + \cdots + a_{jn}b_n$ with a_{jk} in A. Expressing this in matrix form we have:

$$b \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

Denoting by M the $n \times n$ matrix on the right hand side with entries in A, by $\underline{b}$ the $n \times 1$ column matrix whose entry in row j is b_j, and by I the $n \times n$ identity matrix, we can rewirte the above equation as $(bI - M)\underline{b} = 0$. Multiplying the adjoint of $bI - M$, we get $\det(bI - M)I\underline{b} = 0$. This means $\det(bI - M)$ kills all of B and so is zero (since 1 is in B). But $\det(bI - M)$ is of the form $b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0$, so b satisfies a monic polynomial with coefficients in A. □

Again, generalizing the well known fact that a finitely generated algebraic extension of fields is finite, we have:

$$\textit{A finitely generated integral extension is finite.} \tag{3}$$

Proof: The standard proof from the field case generalizes. Indeed, if $A \subseteq B$ is a ring extension and b in B is integral over A, then the subextension $A[b]$ is finite: it is generated as an A-module by $1, b, \ldots, b^{n-1}$ if the degree is n of a monic polynomial over A that b satisfies. Now, if $A[b_1, \ldots, b_m]$ be a finitely generated integral extension, then we get a sequence of extensions $A \subseteq A[b_1] \subseteq A[b_1, b_2] \subseteq \ldots \subseteq A[b_1, \ldots, b_m]$ each of which is finite over the previous one since, for every j, $A[b_1, \ldots, b_j] = A[b_1, \ldots, b_{j-1}][b_j]$ and b_j is integral over $A[b_1, \ldots, b_{j-1}]$ since it is integral over A. □

[2] Which runs as follows: Let n be the dimension of the extension field F over the base field E. Given $f \in F$, the elements $1, f, \ldots, f^n$ cannot be E-linearly independent, and so satisfy a non-trivial linear dependence relation: $e_0 1 + e_1 f^1 + \cdots + e_n f^n = 0$. Let k be the maximum such that e_k is non-zero (observe that $k \geq 1$) and we may assume that $e_k = 1$ (by dividing the given relation by e_k).

Imitating the proof from field theory that an algebraic extension of an algebraic extension is algebraic, we get (item 1 of Exercise set 1):

An integral extension of an integral extension is integral. (4)

Again, imitating the proof from field theory that the set of elements in an extension field that are algebraic over a base fied is a field, we get:

Let $C \subseteq D$ be a ring extension. Let $E := \{d \in D \mid d \text{ is integral over } C\}$.
Then E is a subring of D containing C. It is called the integral closure of C in D. (5)

Proof: Given d and e in E, consider the extesnion $C \subseteq C[d, e]$. Since $C \subseteq C[d]$ and $C[d] \subseteq C[d, e]$ are both integral and finitely generated, they are both finite by (3). So $C \subseteq C[d, e]$ is finite by (1) and in turn integral by (2). Since $d + e$ and de are both contained in $C[d, e]$, they are both integral over C. Thus E is closed under addition and multiplication. That $C \subseteq E$ is clear. □

A domain is said to be *integrally closed* if it equals its integral closure in its quotient field. UFDs (in particular, PIDs) are integrally closed (see item 3 of Exercise set 1).

2. Going up theorem

Let $A \subseteq B$ be an integral extension. We are concerned here with properties of the map $\operatorname{Spec} A \leftarrow \operatorname{Spec} B$ given by $\mathfrak{q}^c \leftarrow \mathfrak{q}$. Let us begin with a basic observation:

If B is a field, then so is A. If A is a field and B is a domain, then B is a field. (6)

Proof: First suppose that B is a field. Let $a \neq 0$ be in A. Let α be the inverse of a in B and let $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$ be an integral equation for α over A. Multiplying by a^n we have $1 + a_{n-1}a + \cdots + a_0 a^n = 0$, which we can rewrite as $1 = -(a_{n-1} + \cdots + a_0 a^{n-1})a$, so $\alpha = -(a_{n-1} + \cdots + a_0 a^{n-1})$ belongs to A.

Now suppose that A is a field and that B is a domain. Let $b \neq 0$ be an element of B and let $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$ be an integral equation for b over A such that n is least. We can rewrite this as $b(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) = -a_0$. If a_0 were 0, then since B is a domain and $b \neq 0$, we have $b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1 = 0$, which contradicts minimality of n. Thus $a_0 \neq 0$, which means that it is a unit (since A is af field), so b is also a unit. □
The above observation translates to:

A prime ideal $\mathfrak{q}$ of B is maximal iff its contraction $\mathfrak{q}^c$ in A is maximal. (7)

Proof: Indeed, $A/\mathfrak{q}^c \subseteq B/\mathfrak{q}$ is an integral extension of domains. So one of them is a field iff the other is too. □

We now prove that the map on spectra is surjective:

Every prime ideal of A is contracted from a prime of B. (8)

Proof: Fix a prime $\mathfrak{p}$ of A. We need to show that there exists a prime $\mathfrak{q}$ of B such that $\mathfrak{q} \cap A = \mathfrak{p}$. Localizing at $\mathfrak{p}$, we obtain the integral extension $A_{\mathfrak{p}} \subseteq B_{\mathfrak{p}}$. It is enough to show that there exists a prime in $B_\mathfrak{p}$ that contracts to the maximal ideal $\mathfrak{p}A_\mathfrak{p}$ of $A_\mathfrak{p}$, for the contraction of that prime to B in turn contracts to $\mathfrak{p}$ in A. Now recall the following (item 6 of Exercise set 1): a maximal ideal is contracted from a prime if its extension is not the whole ring. Thus it is enough to show that $\mathfrak{p}B_\mathfrak{p} \neq B_\mathfrak{p}$. Suppose equality held. Then there exist finitely many elements b_1, …, b_n such that $\mathfrak{p}A_\mathfrak{p}[b_1, \ldots, b_p] = A_\mathfrak{p}[b_1, \ldots, b_n]$. But by the integrality hypothesis and (3), $A_\mathfrak{p}[b_1, \ldots, b_n]$ is a finitely generated $A_\mathfrak{p}$-module. By the Nakayama lemma, $A_\mathfrak{p}[b_1, \ldots, b_n] = 0$, a contradiction. □

The following result, called the going up theorem, now follows easily:

Let $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ be primes in A and $\mathfrak{q}_1$ be a prime in B such that $\mathfrak{q}_1^c = \mathfrak{p}_1$. Then there exists a prime ideal $\mathfrak{q}_2$ in B that contains $\mathfrak{q}_1$ and contracts to $\mathfrak{p}_2$. (9)

Proof: $A/\mathfrak{p}_1 \subseteq B/\mathfrak{q}_1$ is an integral extension. Let $\mathfrak{q}_2$ be the pull-back to B of a prime in $B/\mathfrak{q}_1$ that contracts to the image of $\mathfrak{p}_2$ in $A/\mathfrak{p}_1$ (such a prime in $B/\mathfrak{q}_1$ exists by (8)). □

The *length* of a sequence $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_\ell$ of prime ideals in a ring is ℓ. The *Krull dimension* of a ring R, denoted $\dim R$, is the supremum of lengths of such sequences. Clearly, every field has Krull dimension 0 and every PID that is not a field has Krull dimension 1.

$$\dim A = \dim B \tag{10}$$

Proof: From (8) and (9), it follows that $\dim A \leq \dim B$. To prove that $\dim A \geq \dim B$ it is enough to show that the contractions to A are not the same of prime ideals $\mathfrak{q}_1 \subsetneq \mathfrak{q}_2$ of B. Suppose both of them contract to $\mathfrak{p}$. Then consider the integral extension $(A/\mathfrak{p})_\mathfrak{p} \subseteq (B/\mathfrak{q}_1)_\mathfrak{p}$. Observe that $(A/\mathfrak{p})_\mathfrak{p}$ is a field but that $(B/\mathfrak{q}_1)_\mathfrak{p}$ is not (since it has a non-trival ideal $(\mathfrak{q}_2/\mathfrak{q}_1)_\mathfrak{p}$). But this contradicts (7). □

3. Integrality over an ideal

Let $A \subseteq B$ be a ring extension and $\mathfrak{a}$ an ideal of A. An element b of B is *integral over* $\mathfrak{a}$ if there exists a monic polynomial $f(x)$ with all coefficients other than the leading one being in $\mathfrak{a}$ such that $f(b) = 0$. In this case, $f(b) = 0$ is called an *integral equation for b over $\mathfrak{a}$*. The following result tells us about integrality over $\mathfrak{a}$ in terms of integrality over A:

The set of elements of B that are integral over $\mathfrak{a}$ is precisely the radical $\mathfrak{r}(\mathfrak{a}C)$ of the extension $\mathfrak{a}C$ of $\mathfrak{a}$ to the integral closure C of A in B. (11)

Proof: If b is integral over $\mathfrak{a}$, then it is clearly so over A, and so belongs to C. Let $f(b) = b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$ is an integral equation for b over $\mathfrak{a}$. Rewriting this as $b^n = -(a_{n-1}b^{n-1} + \cdots + a_0)$, we see that b belongs to $\mathfrak{r}(\mathfrak{a}C)$.

Now suppose b belongs to $\mathfrak{r}(\mathfrak{a}C)$. Then $b^n = a_1c_1 + \cdots + a_kc_k$ for some n, $a_i \in \mathfrak{a}$, and $c_i \in C$, so that b^n belongs to $\mathfrak{a}C'$ where $C' := A[c_1, \ldots, c_k]$. Now C' is finite over A by (3). Let c'_1, $\ldots c'_n$ be a finite generating set as an A-module. We have $b^nC' \subseteq \mathfrak{a}C'$, which we can express in matrix notation as:

$$b^n \begin{pmatrix} c_1' \\ \vdots \\ c_n' \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} c_1' \\ \vdots \\ c_n' \end{pmatrix}$$

where the $n \times n$ matrix on the right hand side—let us call it M—has entries in $\mathfrak{a}$. Denoting by $\underline{c'}$ the $n \times 1$ column matrix whose entry in row j is c_j', and by I the $n \times n$ identity matrix, we can rewirte the above equation as $(b^n I - M)\underline{c'} = 0$. Multiplying the adjoint of $b^n I - M$, we get $\det(b^n I - M) I \underline{c'} = 0$. This means $\det(b^n I - M)$ kills all of C' and so is zero (since 1 is in C'). But $\det(b^n I - M)$ is of the form $(b^n)^m + a_{m-1}(b^n)^{m-1} + \cdots + a_1 b^n + a_0$, so b satisfies a monic polynomial with coefficients in $\mathfrak{a}$. □

The following result will be used in the proofs of the important results of the next section. Let A be an integrally closed domain and K its quotient field. Let x be an element of a ring extension B of A. Suppose that B is a domain and that x is integral over an ideal $\mathfrak{a}$ of A. Consider the minimal polynomial over K of x (thought of say in the quotient field of B which is an extension field of K).

All non-leading coefficients of this minimal polynomial are in the radical $\mathfrak{r}(\mathfrak{a})$ *of* $\mathfrak{a}$. (12)

Proof: Look at the conjugates of x (the roots of the minimal polynomial, in some large enough extension of K). Since the minimal polynomial divides the integral equation for x over A, these conjugates are also integral over $\mathfrak{a}$. Since the coefficients of the minimal polynomial are polynomials (with integer coefficients) in the conjugates, it follows that the coefficients are also integral over $\mathfrak{a}$ (since integral elements over ideals are closed under multiplication and addition, by (11)). The coefficients are moreover also in K. So, by (11) and the hypothesis that A is integrally closed, they are in $\mathfrak{r}(\mathfrak{a})$. □

4. Finiteness of integral closure; the Going-down theorem

Let L be a finite field extension of the field $\mathbb{Q}$ of rational numbers. The integral closure C of the ring $\mathbb{Z}$ in L, called the *ring of algebraic integers in L*, is of interest in number theory:

The domain C has L for its quotient field. It is a Dedekind domain, *which means it is integrally closed, of Krull dimension* 1, *and Noetherian.* (13)

Proof: Since C is integral over $\mathbb{Z}$, it is clear from (10) that it has Krull dimension 1. To show that C is Noetherian, it is enough to show that it is a finite $\mathbb{Z}$-module. In turn it is enough to show that it is contained in a finite $\mathbb{Z}$-module, which fact follows from the more general result (14) below. It also follows from (14) that L is the quotient field of C, from which it is clear that C is integrally closed. □

Let A be an integrally closed domain and K its quotient field. Let L be a finite separable extension of K and C the integral closure of A in L. Then:

$$\text{\textit{The domain } } C \text{ \textit{has} } L \text{ \textit{for its quotient field. There exists}} \atop a\ K\text{-\textit{basis} } v_1,\,\ldots,\,v_n \text{ \textit{of} } L \text{ \textit{such that} } C \subseteq Av_1 + \ldots + Av_n. \tag{14}$$

Proof: It is easy to see that L is the quotient field of C. Indeed, $S^{-1}C = L$, where $S = A \setminus \{0\}$: given λ in L, if $a \in A$ is a common denominator for the coefficients (which are in K) of an algebraic equation for λ over K of degree say n, then, multiplying that equation by a^n, we obtain an integral equation for $a\lambda$ over A, which shows that $a\lambda$ belongs to C.

Since L is finite separable, the bilinear form $(x, y) \to \mathrm{Tr}\,(xy)$ (where Tr means the trace as a K-endomorphism of L) is a non-degenerate bilinear form on the K-vector space L. Let $u_1, \ldots, u_n$ be a K-basis of L. Multiplying by a common denominator from C, we may assume that the u_i all belong to C. Let $v_1, \ldots, v_n$ be the dual basis. We claim that $C \subseteq Av_1 + \cdots + Av_n$. Given c in C, let $c = \kappa_1 v_1 + \cdots + \kappa_n v_n$ be the expression for c with κ_i in K. It suffices to show that the κ_i all belong to A. Multiplying the expression for c above by u_i and taking trace, we see that $\mathrm{Tr}\,(cu_i) = \sum_j \mathrm{Tr}\,(\kappa_j u_i v_j) = \sum_j \kappa_j \mathrm{Tr}\,(u_i v_j) = \sum_j \kappa_i \delta_{ij} = \kappa_i$. But cu_i belongs to C, and the minimal polynomial over K of cu_i has coefficients in C, by (12). The trace of an element being an integral multiple of a coefficient of the minimal polynomial, it follows that $\kappa_i = \mathrm{Tr}\,(cu_i)$ belongs to C. □

We now prove the going down theorem. Given that we have called (9) as the "going up" theorem, the name in the present case is only to be expected. Observe that the hypothesis in the going down theorem is stronger than in the going up theorem.

Let $A \subseteq B$ be an integral extension of domains, with A integrally closed. Then given prime ideals $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ in A and a prime ideal $\mathfrak{q}_2$ in B with $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$ there exists prime ideal $\mathfrak{q}_1$ in B such that $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ and $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$. (15)

Proof: Recall that a prime is contracted from a prime ideal if it is contracted from its extension. Since we are looking for a prime $\mathfrak{q}_1$ contained in $\mathfrak{q}_2$, it is natural to look at the composite extension $A \subseteq B \subseteq B_{\mathfrak{q}_2}$. It suffices to show that $\mathfrak{p}_1 B_{\mathfrak{q}_2} \cap A = \mathfrak{p}_1$. Moreover, since the left side clearly contains the right side in general, it suffices to prove that $\mathfrak{p}_1 B_{\mathfrak{q}_2} \cap A \subseteq \mathfrak{p}_1$. A general element of the left side is of the form $y/s = a$, with $y \in \mathfrak{p}_1 B$, $s \in B \setminus \mathfrak{q}_2$, and $a \in A$. We consider the minimal polynomials $f(t)$ and $g(t)$ of y and s over the quotient field K of A: observe that y and s are algebraic over K by the integrality hypothesis on $A \subseteq B$. Since $y = as$ with $a \in A \subseteq K$, it follows that the f and g are of the same degree, say n. In fact, the algebraic equation for y is obtained by multiplying the one for s by a^n, so the coefficients f_j and g_j of t^j in f and g respectively satisfy $f_j = g_j a^{n-j}$.

Now we use the hypothesis that A is integrally closed and invoke (11) and (12). By (11), since $y \in \mathfrak{p}_1 B$, it follows that the y is integral over $\mathfrak{p}_1$, so by (12) that the f_j belongs to $\mathfrak{p}_1$ for $j < n$. Again, by (11) $s \notin \mathfrak{r}(\mathfrak{p}_1 B)$ (because $\mathfrak{p}_1 B \subseteq \mathfrak{p}_2 B \subseteq \mathfrak{q}_2$, so $\mathfrak{r}(\mathfrak{p}_1 B) \subseteq \mathfrak{q}_2$), and by (12) at least one of the g_j with $j < n$ does not belong to $\mathfrak{p}_1$. But now, since $f_j = g_j a^{n-j}$, we conclude that a belongs to $\mathfrak{p}_1$. □

5. Valuations: a criterion for domains to be integrally closed

Our goal is to characterize the integral closure of a subring of a field by means of "valuation rings" (see (17) below). A domain V with quotient field K is a *valuation ring (of K)* if for every $x \neq 0$ in K either x or x^{-1} (or both) belong to V. We first prove:

$$\textit{A valuation ring is local and integrally closed.} \tag{16}$$

Proof: Let V be a valuation ring of a field K. To show that a ring is local, it is enough to show that the non-units are closed under addition. Let x and y be non-units in V. Either $x^{-1}y$ or $y^{-1}x$ belongs to V. In the former case, we have $x+y=(1+x^{-1}y)x$ is a non-unit since x is; in the latter, $x+y=(y^{-1}x+1)y$ is a non-unit since y is.

To show that V is integrally closed, let $x \in K$ and suppose that $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ is an integral equation for x over A. If x^{-1} belongs to V, then, multiplying the integral equation by $(x^{-1})^{n-1}$ and rearranging terms we get $x = -(a_{n-1} + a_{n-2}x^{-1} + \cdots + a_0(x^{-1})^{n-1})$, so x belongs to V. □

The characterization that we are after is:

$$\begin{array}{l}\textit{Let } A \textit{ be a subring of a field } K\textit{. The integral closure of } A \textit{ in } K \textit{ is}\\ \textit{the intersection of the valuation rings of } K \textit{ that contain } A\textit{.}\end{array} \tag{17}$$

Since valuation rings are integrally closed, so is their intersection, so one part of the assertion is proved. The harder part is to show that if an element x of K is not integral over A then there exists a valuation ring V of K containing A but not containing x. This motivates the question: how to find valuation rings?

In order to find valuation rings, we make an observation. Let K be a field, C a subring of K, and $\varphi : C \to \Omega$ be a ring homomorphism of C to an algebraically closed field Ω. Consider the set Σ of pairs $(B, \tilde{\varphi})$ where B is a subring of K containing C and $\tilde{\varphi}$ is a homomorphism $B \to \Omega$ that lifts φ. We impose a partial order on Σ: $(B, \tilde{\varphi}) \leq (B', \tilde{\varphi}')$ if $B \subseteq B'$ and $\tilde{\varphi}'$ extends $\tilde{\varphi}$. A standard Zorn's lemma argument now implies that Σ has maximal elements. We claim:

$$\textit{Maximal elements of } \Sigma \textit{ are valuation rings of } K. \tag{18}$$

Assuming for the moment this claim, let us finish the proof of (17). Let x in K be not integral over A. Then $x \notin A[x^{-1}]$ (see item 1 of Exercise set 2), so x^{-1} is not a unit in $A[x^{-1}]$. Put $C := A[x^{-1}]$, choose a maximal ideal $\mathfrak{m}$ of C containing x^{-1}, let Ω be an algebraically closed extension field of $C/\mathfrak{m}$, and consider $\varphi : C \to C/\mathfrak{m} \subseteq \Omega$. Let Σ be as in the previous paragraph and $(B, \tilde{\varphi})$ be a maximal element of Σ. Then B is a valuation ring of K by (18). And x is not contained in B since x^{-1} is zero under $\tilde{\varphi}$ and so not a unit in B. This finishes the proof of (17) assuming (18).

We now prove (18). Let $(B, \tilde{\varphi})$ be a maximal element in Σ. We first show that

$$B \textit{ is local with } \mathfrak{m} := \operatorname{Ker} \tilde{\varphi} \textit{ as maximal ideal.} \tag{19}$$

Since $B/\mathfrak{m} \hookrightarrow \Omega$, it follows that $\mathfrak{m}$ is a (proper) prime ideal. To show $\mathfrak{m}$ is maximal, it is enough to show that every element in B outside of $\mathfrak{m}$ is a unit. Since $B \setminus \mathfrak{m}$ intersects $\operatorname{Ker} \tilde{\varphi}$ trivially, the image under $\tilde{\varphi}$ of $B \setminus \mathfrak{m}$ consists of units in Ω. By the universal property of localization, there exists a homomorphism $B_{\mathfrak{m}} \to \Omega$ that lifts $\tilde{\varphi}$. By the maximality of $(B, \tilde{\varphi})$, this means $B_{\mathfrak{m}} = B$. In other words, all elements outside of $\mathfrak{m}$ are units in B. So $\mathfrak{m}$ is a maximal ideal, and (19) is proved.

Continuing with the proof of (18), we now prove

> *Suppose that D is a local domain with maximal ideal $\mathfrak{n}$ and let L be a field containing D. Then, for $0 \neq x$ in L, either $\mathfrak{n}[x] \neq D[x]$ or $\mathfrak{n}[x^{-1}] \neq D[x^{-1}]$.* (20)

By way of contradiction, suppose equality held in both places. Choose n and m least such that $d_n x^n + d_{n-1}x^{n-1} + \cdots + d_0 = 1$ and $e_m x^{-m} + e_{m-1}x^{-(m-1)} + \cdots + e_0 = 1$ with d_i and e_j in $\mathfrak{n}$. Suppose that $n \geq m$. Then multiplying the second equation by x^n and rewriting, we obtain $e_m x^{n-m} + e_{m-1}x^{n-(m-1)} + \cdots + e_1 x^{n-1} = (1-e_0)x^n$. Since $1-e_0$ is a unit, multiplying by its inverse gives us $e'_m x^{n-m} + e'_{m-1}x^{n-(m-1)} + \cdots + e'_1 x^{n-1} = x^n$ with $e'_i \in \mathfrak{n}$. Substituting this into the first equation, we get a contradiction to the minimality of n. The case $m \geq n$ is handled analogously, and the proof of (20) is complete.

Back to the proof of (18), let $(B, \tilde{\varphi})$ be a a maximal element of Σ. Put $\mathfrak{m} := \operatorname{Ker} \tilde{\varphi}$. Let $0 \neq x$ be in K. Thanks to (19), we may apply (20) with B, $\mathfrak{m}$, and K respectively in place of D, $\mathfrak{n}$, and L. So either $\mathfrak{m}[x] \neq B[x]$ or $\mathfrak{m}[x^{-1}] \neq B[x^{-1}]$. We will assume $\mathfrak{m}[x] \neq B[x]$ and show that x belongs to B. This will suffice, for if $\mathfrak{m}[x^{-1}] \neq B[x^{-1}]$, then this will mean x^{-1} belongs to B.

So suppose that $\mathfrak{m}[x] \neq B[x]$. Let $\mathfrak{m}'$ be a maximal ideal of $B[x]$ containing $\mathfrak{m}[x]$. Since $\mathfrak{m}' \cap B = \mathfrak{m}$, we have $B/\mathfrak{m} \subseteq B[x]/\mathfrak{m}'$. This extension of fields is algebraic (see item 4 of Exercise set 3). Thus $\tilde{\varphi} : B \twoheadrightarrow B/\mathfrak{m} \hookrightarrow \Omega$ can be lifted to $\tilde{\varphi}' : B[x] \twoheadrightarrow B[x]/\mathfrak{m}' \hookrightarrow \Omega$. By the maximality of $(B, \tilde{\varphi})$, it follows that $x \in B$, and (18) is proved. □

6. Hilbert's Nullstellensatz

The Nullstellensatz, meaning "zero point theorem", is due to David Hilbert and dates from the last decade the nineteenth century. There are several different versions of its statement and several different proofs. Four versions are discussed below (Theorems 1–4). The discussion of the first version follows that in the text by Atiyah–Macdonald (see the section on "Valuation rings" in Chapter 5 of that book).

Theorem 1. (Hilbert's Nullstellensatz, first version) *An extension of fields is algebraic if the extension field is finitely generated as an algebra over the base field.*

In case the base field is uncountable e.g., $\mathbb{R}$ or $\mathbb{C}$, there is an easy proof of this theorem (see item 7 in Exercise set 4). In any case, we now deduce the theorem from (21) below (which in turn is proved by using (18) of §5) by setting $A \subseteq B$ to be the field extension, $f : A \to \Omega$

to be an inclusion of the base field in an algebraic closure, and $v = 1$.

Let $A \subseteq B$ be domains, with B finitely generated as an A-algebra.
Given $v \neq 0$ in B, there exists $u \neq 0$ in A with the following property:
any ring homomorphism $f : A \to \Omega$ with $f(u) \neq 0$, (21)
where Ω is an algebraically closed field,
extends to a ring homomorphism $\tilde{f} : B \to \Omega$ with $\tilde{f}(v) \neq 0$.

Proof: We reduce immediately to the case when B is generated by a single element, say x, over A as an algebra: $B = A[x]$. Let K and L be the quotient fields of A and B respectively. We consider two cases.

First suppose that the element x of L is transcendental over K, or, in other words, that B is a polynomial ring over A in x. Let $v = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with a_i in A and $a_0 \neq 0$. Choose u to be a_n. Let $f : A \to \Omega$ be a ring homomorphism with $f(u) \neq 0$. Choose $\sigma \in \Omega$ so that $a_n\sigma^n + a_{n-1}\sigma^{n-1} + \cdots + a_0 \neq 0$: such a σ exists because Ω is infinite. Now f extends to g on B with $g(x) = \sigma$ (since B is a polynomial ring in x over A). We have $g(v) \neq 0$ by choice of σ.

Now suppose that x is algebraic over K, which means we can write $a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0 = 0$ with $a_i \in A$ and $a_m \neq 0$. Then $K[x]$ is a field extension and so v^{-1} belongs to $K[x]$ (since $0 \neq v$ is an element of $K[x]$). Thus v^{-1} is integral over K, and we can write $a'_n(v^{-1})^n + a'_{n-1}(v^{-1})^{n-1} + \cdots + a'_0 = 0$ with $a'_i \in A$ and $a'_n \neq 0$. Choose $u = a_m a'_n$.

Now suppose that $f : A \to \Omega$ is a homomorphism with Ω an algebraically closed field and $f(u) \neq 0$. Then f extends to $\hat{f} : A[u^{-1}] \to \Omega$: we have $\hat{f}(u^{-1}) = f(u)^{-1}$ (by the universal property of localization, if you so wish). The choice of u is such that the elements x and v^{-1} are integral over $A[u^{-1}]$. Thus $A[u^{-1}, x, v^{-1}]$ is an integral extension of $A[u^{-1}]$, and there is a lift $\tilde{f} : A[u^{-1}, x, v^{-1}] \to \Omega$ of $\hat{f}$ (see item 7 of Exercise set 1). The restriction of $\tilde{f}$ to $B = A[x]$ has the required property: since v is a unit in $A[u^{-1}, x, v^{-1}]$ it follows that $\tilde{f}(v) \neq 0$. □

To introduce another version of the Nullstellensatz, let Ω be an algebraically closed field. Observe that every maximal ideal in the polynomial ring $\Omega[x]$ in one variable is of the form $(x - \alpha)$ with $\alpha \in \Omega$. This generalizes to polynomial rings in more than one variable:

Theorem 2. *Every maximal ideal of the polynomial ring $\Omega[x_1, \ldots, x_n]$, where Ω is an algebraically closed field, is of the form $(x_1 - \alpha_1, \ldots, x_n - \alpha_n)$, with $\alpha_1, \ldots, \alpha_n$ in Ω.*

Proof: It is clear that an ideal of the form $(x_1 - \alpha_1, \ldots, x_n - \alpha_n)$ is maximal. Conversely, given a maximal ideal $\mathfrak{m}$, the extension $\Omega \subseteq \Omega[x_1, \ldots, x_n]/\mathfrak{m}$ is an algebraic extension by (21), and so an isomorphism since Ω is algebraically closed. If $\alpha_1, \ldots, \alpha_n$ are the preimages of $x_1, \ldots, x_n$, then it is clear that $x_j - \alpha_j$ are all zero in $\Omega[x_1, \ldots, x_n]/\mathfrak{m}$, which means that they all belong to $\mathfrak{m}$. Thus $\mathfrak{m} = (x_1 - \alpha_1, \ldots, x_n - \alpha_n)$. □

Towards yet another version of the Nullstellensatz, fix a field extension $K \subseteq L$ and a positive integer n. Denote by A the polynomial ring $K[x_1, \ldots, x_n]$. Given a subset S of A, define the corresponding *zero locus $V_L(S)$ (or just $V(S)$ if L is understood) of S in L^n* by zero locus def

$$V(S) := \{(\alpha_1, \ldots, \alpha_n) \in L^n \mid f(\alpha_1, \ldots, \alpha_n) = 0 \text{ for all } f \in S\}$$

Conversely, define *the ideal* $I(X)$ in A for a subset X of L^n by

$$I(X) := \{f \in A \mid f(\alpha_1, \ldots, \alpha_n) = 0 \text{ for all } (\alpha_1, \ldots, \alpha_n) \in X\}$$

The following statements are evident (the notation too is self-explanatory):

(1) $S \subseteq S' \Rightarrow V(S) \supseteq V(S')$ and $X \subseteq X' \Rightarrow I(X) \supseteq I(X')$.
(2) $I(V(S)) \supseteq S$ and $V(I(X)) \supseteq X$.
(3) $I(X)$ is a radical ideal: $\mathfrak{r}(I(X)) = I(X)$.

Using these we can prove the following:

Between ideals of A of the form $I(X)$ for subsets X of L^n on the one hand, and subsets of L^n of the form $V(S)$ for subsets S of A on the other, there exists a bijective correspondence given by $I(X) \mapsto V(I(X))$ and $V(S) \mapsto I(V(S))$. (22)

Proof: We will show that the indicated maps are inverses of each other. We have $V(I(V(S))) \supseteq V(S)$ by item (2) above. Also by (2), $I(V(S)) \supseteq S$, so by (1), $V(I(V(S))) \subseteq V(S)$. It follows that $V(I(V(S))) = V(S)$. In other words, $V \circ I$ is identity on subsets of L^n of the form $V(S)$. A similar argument shows that $I \circ V$ is identity on ideals of the form $I(X)$ for some subset X of L^n. □

If in the above set up, L happens to be an algebraically closed field Ω, then the zero loci $V(S)$ in Ω^n of sets of polynomials with coefficients in K are called *affine varieties defined over K (in Ω^n)*. We are now ready for yet another version of the nullstellensatz:

variety
d

Theorem 3. *Let $K \subseteq \Omega$ be fields with Ω algebraically closed. Between affine varieties defined over K of Ω^n on the one hand, and radical ideals of the polynomial ring $A = K[x_1, \ldots, x_n]$ on the other, there is a bijective correspondence given by the maps V and I defined above.*

Proof: Given item (3) above and (22), it only remains to show that $I(V(\mathfrak{a})) = \mathfrak{a}$ for every radical ideal $\mathfrak{a}$ of A. Since $I(V(\mathfrak{a})) \supseteq \mathfrak{a}$ by item (2) above, it remains only to show the other containment. Suppose that f belongs to $I(V(\mathfrak{a}))$. In the polynomial ring $\Omega[x_1, \ldots, x_n, y]$ consider $S = \mathfrak{a} \cup \{fy - 1\}$. It is easy to see that $V(S)$ is empty in Ω^{n+1}. By Theorem 2 it follows that the ideal generated by $\mathfrak{a} \cup \{fy - 1\}$ is the unit ideal: if it were proper, then it would be contained in a maximal ideal and therefore $V(S)$ would not be empty. In turn this means that $\mathfrak{a} \cup \{fy - 1\}$ generates the unit ideal even in $K[x_1, \ldots, x_n, y]$ (see item 4 of Exercise set 4). This means that the extension of $\mathfrak{a}$ to $K[x_1, \ldots, x_n, y]/(fy - 1)$ is the unit ideal. But this last ring is the same as $T^{-1}\Omega[x_1, \ldots, x_n]$ where T denotes the multiplicatively closed set $\{1, f, f^2, \ldots\}$. Thus there exists an integer $n \geq 0$ and $a \in \mathfrak{a}$ such that $a/f^n = 1$, which means f belongs to $\mathfrak{r}\,\mathfrak{a} = \mathfrak{a}$. □

For our final version of the nullstellensatz, define a ring to be *Jacobson* if its quotient by any prime ideal has zero Jacobson radical, or, equivalently, every prime ideal is the intersection of the maximal ideals containing it.

Theorem 4. *Let $R \to S$ be a finitely generated ring extension. If R is Jacobson, so is S.*

Proof: We will deduce the result from (21). Passing to $R/\mathfrak{q} \cap R \subseteq S/\mathfrak{q}$, where $\mathfrak{q}$ is a prime ideal of R, we reduce to showing the following: for domains $R \subseteq S$, if R has Jacobson radical 0, then so does S. To prove this, let $0 \neq v$ be an element of S. Let $0 \neq u$ be an element of R as in (21). Choose maximal ideal $\mathfrak{m}$ of R such that $u \notin \mathfrak{m}$: this is possible since the Jacobson radical of R is 0. Now let Ω be an algebraic closure of the field $R/\mathfrak{m}$. Note that the image of u is non-zero under the composition—call it f—of the natural maps: $R \to R/\mathfrak{m} \subseteq \Omega$ (since $u \notin \mathfrak{m}$). By (21), there exists an extension $\tilde{f} : S \to \Omega$ of f with $\tilde{f}(v) \neq 0$. We have $\operatorname{Ker} \tilde{f} \cap R = \operatorname{Ker} f = \mathfrak{m}$, so that $R/\mathfrak{m} \subseteq S/\operatorname{Ker} \tilde{f} \subseteq \Omega$. Since $R/\mathfrak{m} \subseteq \Omega$ is an algebraic extension, it follows that $S/\operatorname{Ker} \tilde{f}$ is a field (see (6) in §2), in other words, that $\operatorname{Ker} \tilde{f}$ is a maximal ideal. But $v \notin \operatorname{Ker} \tilde{f}$ since $\tilde{f}(v) \neq 0$. □

Exercise set 1

Throughout this set of exercises, a *ring* means a commutative ring with unity.

(1) An integral extension of an integral extension is integral. Hint: Imitate the standard proof from field theory for the fact that an algebraic extension of an algebraic extension is algebraic.

(2) Let $A \subseteq B$ be a ring extension and C be the integral closure of A in B. Then $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.

(3) UFDs (in particular PIDs) are integrally closed.

(4) Let $A \subseteq B$ be an integral extension. An element a of A that is a unit in B is already a unit in A. The Jacobson radical of B contracts to the Jacobson radical of A.

(5) Let $A \subseteq B$ be a ring extension such that $B \setminus A$ is closed under multiplication. Then A is integrally closed in B.

(6) A prime ideal is contracted (under a ring homomorphism) iff it is contracted from a prime ideal. A maximal ideal is contracted (under a ring homomorphism) if its extension is not the whole ring.

(7) Let $A \subseteq B$ be an integral ring extenstion. Let $f : A \to \Omega$ be a ring homomorphism, where Ω is an algebraically closed field. Show that f can be extended to a homomorphism $B \to \Omega$. Solution: $\operatorname{Ker} f$ is prime. Let $\mathfrak{q}$ be a prime in B such that its contraction $\mathfrak{q} \cap A$ to A is $\operatorname{Ker} f$. The extension $A/\operatorname{Ker} f \subseteq B/\mathfrak{q}$ is integral. Let S be the non-zero elements of $A/\operatorname{Ker} f$. Localizing at S gives us the integral extension $K \subseteq S^{-1}(B/\mathfrak{q})$, where K is the quotient field of $A/\operatorname{Ker} f$. Since K is field, so is $S^{-1}(B/\mathfrak{q})$ (and it is an algebraic extension of K). Now the original f clearly factors through $A/\operatorname{Ker} f$ and lifts to K (by the universal property of quotient fields), and so (since Ω is algebraically closed) lifts (non-uniquely in general) to a homomorphism $\tilde{f} : S^{-1}(B/\mathfrak{q}) \to \Omega$. Now the composition $B \to B/\mathfrak{q} \to S^{-1}(B/\mathfrak{q}) \to \Omega$ where the last map is $\tilde{f}$ is the required lift.

ri Alert

Exercise set 2

(1) Let $A \subseteq B$ be a ring extension and x a unit in B. Observe that x is integral over A if and only if $x \in A[x^{-1}]$.

(2) Let $A \subseteq B$ be a ring extension and $\mathfrak{a}$ an ideal of A. An element b of B is *integral over* $\mathfrak{a}$ if there exists a monic polynomial $f(x)$ with all coefficients other than the leading one being in $\mathfrak{a}$ such that $f(b) = 0$. Show the following:

The set of elements of B that are integral over $\mathfrak{a}$ is precisely the radical $\mathfrak{r}(\mathfrak{a}C)$ of the extension $\mathfrak{a}C$ of $\mathfrak{a}$ to the integral closure C of A in B.

Hint: That b belongs to $\mathfrak{r}(\mathfrak{a}C)$ if it is integral over $\mathfrak{a}$ is straightforward to prove. For the converse, suppose that $b^n = a_1c_1 + \cdots + a_kc_k$ for some n, $a_i \in \mathfrak{a}$, and $c_i \in C$. Then b^n belongs to $\mathfrak{a}C'$ where $C' := A[c_1, \ldots, c_k]$. Note that C' is finite over A. Use the determinant trick to show that b^n and therefore also b is integral over $\mathfrak{a}$.

(3) Consider the integral extension $\mathbb{Z} \subseteq \mathbb{Z}[i]$, where i is a square root of -1. Discuss the map $\operatorname{Spec}\mathbb{Z} \leftarrow \operatorname{Spec}\mathbb{Z}[i]$.

(4) For a complex number α that is integral over $\mathbb{Z}$, the minimal polynomial over $\mathbb{Q}$ of α has coefficients in $\mathbb{Z}$. Hint: Observe that the conjugates of α are all integral over $\mathbb{Z}$.

Exercise set 3

(1) A subring of a field that contains a valuation ring for that field is local.

(2) A domain A is a valuation ring if and only if its ideals are totally ordered. In particular the quotient by a prime ideal of a valuation ring is a valuation ring.

(3) Let K be a field and let

$$\Sigma := \{(B, \mathfrak{m}) \mid B \text{ is a local subring of } K \text{ with maximal ideal } \mathfrak{m}\}$$

Put a poset structure on Σ as follows: $(B, \mathfrak{m}) \leq (B', \mathfrak{m}')$ if $B \subseteq B'$ and $\mathfrak{m} \subseteq \mathfrak{m}'$. Show that Σ admits maximal elements, and that, if $(B, \mathfrak{m})$ is a maximal element, then B is a valuation ring for K.

(4) A field extension that is generated as an algebra over the base field by a single element is algebraic.

Exercise set 4

(1) Let $R \subseteq S$ be finitely generated algebras over a field K. Then the contraction of a maximal ideal of S is maximal in R.

(2) Let $R \subseteq S$ be a finitely generated ring extension. True or false?: If S is Jacobson, so is R.

(3) Let $\mathbb{R}$ be the field of real numbers. Classify the maximal ideals in the polynomial rings $\mathbb{R}[x]$ and $\mathbb{R}[x, y]$.

(4) (This is used in the proof of Theorem 3.) Let $K \subseteq L$ be a field extension and $K[x_1, \ldots, x_n] \subseteq L[x_1, \ldots, x_n]$ the corresponding extension of polynomial rings. If a subset S of $K[x_1, \ldots, x_n]$ generates the unit ideal in $L[x_1, \ldots, x_n]$, then it does so in $K[x_1, \ldots, x_n]$ itself.

(5) Let K be a field that is not algebraically closed. Given n, find a proper ideal in $K[x_1, \ldots, x_n]$ whose zero locus in K^n is empty.

(6) Let $K \subseteq L$ be a field extension. Declaring zero loci $V_L(S)$ in L^n (where S is a subset of the polynomial ring $K[x_1, \ldots, x_n]$) to be closed subsets, we obtain a topology on L^n called the *Zariski topology*.

(7) (Alternative proof of Theorem 1 in case the base field is uncountable.) Suppose that $K \subseteq L$ be a field extension with L finitely generated as a K-algebra. Assuming K to be uncountable, show that the field extension is algebraic. Solution: Note that L has countable dimension over K as a vector space. Suppose that L is not algebraic over K. Then we arrive at a contradiction as follows. Let x be in L transcendental over K. The field $K(t)$ of rational functions in one variable (this is the quotient field of the polynomial ring $K[t]$) injects into L with $t \mapsto x$. But the K-dimension of $K(t)$ is uncountable: observe that $1/(t - \alpha)$, $\alpha \in K$, are K-linearly independent, and K is assumed to be uncountable.