1 Integral ring extensions

Let S be commutative ring (with 1) and let R be a subring. We call $R \subseteq S$ a **ring extension**. An element $s \in S$ is called **integral** over R if there exists a monic polynomial $f \in R[x]$ such that $f(s) = 0$. If every $s \in S$ is integral over R, then S is said to be integral over R.

Observations: If s is integral over R, then it is also algebraic over R. If R is a field, then the converse holds as well. For the ring extension $\mathbb{Z} \subset \mathbb{Q}$, an element $s \in \mathbb{Q}$ is integral over $\mathbb{Z}$ if and only if s is an integer (this explains where the name comes from).

Lemma 1 *Let $R \subseteq S$ be a ring extension and let $s \in S$. The following are equivalent:*

1. *s is integral over R.*
2. *$R[s]$ is finitely generated as an R-module.*
3. *There exists a ring extension $R[s] \subseteq S'$ such that S' is finitely generated as an R-module.*

Proof: "1 $\Rightarrow$ 2": There exists a representation $s^n = \sum_{i=0}^{n-1} r_i s^i$ for some $r_i \in R$. Thus $R[s] = {}_R\langle 1, s, \ldots, s^{n-1} \rangle$.

"2 $\Rightarrow$ 3": Take $S' = R[s]$.

"3 $\Rightarrow$ 1": Let S' be generated by $g_1, \ldots, g_n \in S'$. Since $sg_i \in S'$ for all i, we have a matrix equation $sg = Ag$ for some $A \in R^{n \times n}$ and $g = [g_1, \ldots, g_n]^T$. Then $(sI_n - A)g = 0$, which implies $\det(sI_n - A)g = 0$ and hence $\det(sI_n - A)S' = 0$ and finally $\det(sI_n - A) = 0$. However, $\det(sI_n - A)$ is a monic polynomial in s of degree n with coefficients in R. This shows that s is integral over R. $\square$

Theorem 1 *Let $R \subseteq S$ be a ring extension.*

1. *If S is finitely generated as an R-module, then S is integral over R.*
2. *If $s_1, \ldots, s_n \in S$ are integral over R, then $R[s_1, \ldots, s_n]$ is finitely generated as an R-module.*
3. *$\bar{R} := \{s \in S \mid s \text{ is integral over } R\}$ is a subring of S and integral over R.*
4. *Let $R \subseteq S \subseteq T$ be ring extensions. If S is integral over R, and T is integral over S, then T is integral over R.*

Proof: 1. Let $s \in S$, then $R[s] \subseteq S$. If S is finitely generated as an R-module, then s is integral over R by the previous lemma.

2. Let $s_i^{n_i} = \sum_{j=0}^{n_i-1} r_{ij} s_i^j$ for some $r_{ij} \in R$. Then $R[s_1, \ldots, s_n]$ is generated, as an R-module, by the elements $s_1^{j_1} \cdots s_n^{j_n}$ with $0 \leq j_i < n_i$.

3. Let $s_1, s_2 \in S$ be integral over R. By part 2, $R[s_1, s_2]$ is finitely generated as an R-module and thus (by part 1) integral over R. Hence also $s_1 + s_2$ and $s_1 s_2$ are integral over R, that is, $\bar{R}$ is closed w.r.t. addition and multiplication. Thus $\bar{R}$ is a subring of S and it is clearly integral over R.

4. Let $t \in T$. Since T is integral over S, we have $t^n = \sum_{i=0}^{n-1} s_i t^i$ for some $s_i \in S$. Since S is integral over R, the ring $R' := R[s_0, \ldots, s_{n-1}]$ is finitely generated as an R-module by part 2. Since t is integral over R', the ring $R'[t] = R[s_0, \ldots, s_{n-1}, t]$ is finitely generated as an R'-module, and then also as an R-module. By part 1, it is integral over R, in particular, t is integral over R. □

The ring $\bar{R}$ is called the **integral closure** of R in S. If $\bar{R} = R$, then R is said to be **integrally closed** in S. A domain which is integrally closed in its quotient field is called **normal**. For example, $\mathbb{Z}$ is normal. This observation from above can be generalized as follows.

Theorem 2 *Factorial rings are normal.*

Proof: Let R be a factorial ring and let $\frac{r}{s} \in \mathrm{Quot}(R)$ be integral over R. We may assume that $\gcd(r, s) = 1$. Then we have $(\frac{r}{s})^n = \sum_{i=0}^{n-1} r_i (\frac{r}{s})^i$ for some $r_i \in R$. Multiplying this by s^n, we get

$$r^n = \sum_{i=0}^{n-1} r_i r^i s^{n-i} = (r_0 s^{n-1} + r_1 r s^{n-2} + \ldots + r_{n-1} r^{n-1}) s.$$

If p is any prime divisor of s, then it also divides r^n and thus r. Since $\gcd(r, s) = 1$, this implies that s must be a unit of R. Thus $\frac{r}{s} \in R$. □

The following lemma will be needed later on, in the proof of the Noether normalization theorem and its corollaries.

Lemma 2 *1. If a domain L is integral over a field K, then L is itself a field.*

2. Let $R \subseteq S$ be an integral ring extension and let R, S be domains. Then $\mathrm{Quot}(R) \subseteq \mathrm{Quot}(S)$ is an integral ring extension (or equivalently, an algebraic field extension).

Proof: 1. Let $0 \neq s \in L$. There exists a representation $s^n = \sum_{i=0}^{n-1} r_i s^i$ with $r_i \in K$. Without loss of generality, let n be minimal. Then

$$(s^{n-1} - r_{n-1}s^{n-2} - \ldots - r_1)s = r_0,$$

and since both factors on the left are non-zero and L is a domain, we have $0 \neq r_0 \in K$. Thus r_0 is invertible, and we obtain

$$r_0^{-1}(s^{n-1} - r_{n-1}s^{n-2} - \ldots - r_1)s = 1,$$

showing that s is invertible. Thus L is a field.

2. It is easy to see that $\mathrm{Quot}(R) \subseteq (R \setminus \{0\})^{-1}S$ is an integral ring extension. By part 1, $(R \setminus \{0\})^{-1}S \subseteq \mathrm{Quot}(S)$ is a field. However, $\mathrm{Quot}(S)$ is the smallest field that contains S. Thus we must have $(R \setminus \{0\})^{-1}S = \mathrm{Quot}(S)$. □

2 Going up and going down

"Going up" and "going down" are the colloquial names of two important results in commutative algebra, which are due to Cohen and Seidenberg. They are both concerned with associating a prime ideal chain $\mathfrak{q}_0 \subsetneq \ldots \subsetneq \mathfrak{q}_l$ in S to a given prime ideal chain $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_l$ in R, where $R \subseteq S$ is an integral ring extension. "Going up" starts with the construction of $\mathfrak{q}_0$ and extends the chain "upwards" the inclusion chain. Its main consequence is the fact that the Krull dimensions of R and S coincide if $R \subseteq S$ is an integral ring extension. "Going down", which is more difficult and requires stronger assumptions on the ring extension, starts with the construction of $\mathfrak{q}_l$ and extends the chain "downwards". Its most important consequence is a relation between the heights of certain prime ideals in S and R.

Let $R \subseteq S$ be a ring extension. If J is an ideal of S, then $J \cap R$ is an ideal of R called the **contraction** of J to R. Conversely, if I is an ideal of R, then IS is an ideal of S called the **extension** of I in S. Note that the contraction of a prime ideal is a prime ideal, whereas the extension of a prime ideal is not necessarily prime (e.g., the extension of $2\mathbb{Z}$ in $\mathbb{Q}$).

Lemma 3 *Let $R \subseteq S$ be an integral ring extension. Let I be a proper ideal of R. Then IS is a proper ideal of S.*

Proof: Suppose that $IS = S$. Then we can write $1 = \sum_{i=1}^{n} r_i s_i$, where $r_i \in I$ and $s_i \in S$. By Theorem 1, $S' := R[s_1, \ldots, s_n]$ is finitely generated as an R-module, say, by $g_1, \ldots, g_m \in S'$. Since $S' = IS'$, there exist $a_{ij} \in I$ such that $g_i = \sum_j a_{ij} g_j$ for all i. The matrix equation $g = Ag$ yields $(I_m - A)g = 0$ and thus $\det(I_m - A)g = 0$. Since $A \in I^{m \times m}$, we have $\det(I_m - A) = 1 - r$ for some $r \in I$. Thus $(1-r)S' = 0$, which implies $1 - r = 0$. Thus $1 \in I$, that is, $I = R$. □

Lemma 4 (Cohen-Seidenberg Going Up Lemma) *Let $R \subseteq S$ be an integral ring extension and let $\mathfrak{p}$ be a prime ideal of R. Then there exists a prime ideal $\mathfrak{q}$ of S such that $\mathfrak{q} \cap R = \mathfrak{p}$.*

Proof: Since $R \subseteq S$ is integral, $R_{\mathfrak{p}} \subseteq S_{\mathfrak{p}}$ is also integral. By the previous lemma, $\mathfrak{p}_{\mathfrak{p}} S_{\mathfrak{p}}$ is a proper ideal of $S_{\mathfrak{p}}$. Thus it is contained in a maximal ideal $\mathfrak{m}$ of $S_{\mathfrak{p}}$. Then

$$\mathfrak{p}_{\mathfrak{p}} \subseteq \mathfrak{p}_{\mathfrak{p}} S_{\mathfrak{p}} \cap R_{\mathfrak{p}} \subseteq \mathfrak{m} \cap R_{\mathfrak{p}} \subsetneq R_{\mathfrak{p}}.$$

Since $\mathfrak{p}_{\mathfrak{p}}$ is the maximal ideal in $R_{\mathfrak{p}}$, we conclude that $\mathfrak{p}_{\mathfrak{p}} = \mathfrak{m} \cap R_{\mathfrak{p}}$. The commutative diagram

$$\begin{array}{ccc} R & \hookrightarrow & S \\ \phi \downarrow & & \downarrow \psi \\ R_{\mathfrak{p}} & \hookrightarrow & S_{\mathfrak{p}} \end{array}$$

yields $\phi^{-1}(\mathfrak{p}_{\mathfrak{p}}) = \psi^{-1}(\mathfrak{m}) \cap R$. However, $\phi^{-1}(\mathfrak{p}_{\mathfrak{p}}) = \mathfrak{p}$ since $\mathfrak{p}$ is prime, and $\psi^{-1}(\mathfrak{m})$ is prime since $\mathfrak{m}$ is prime. $\square$

If $R \subseteq S$ is an arbitrary ring extension, then the Krull dimension of R can be either greater or less than the Krull dimension of S.

Theorem 3 *Let $R \subseteq S$ be an integral ring extension. Then R and S have the same Krull dimension.*

Proof: Let $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_l$ be a prime ideal chain in R. By the Going Up Lemma, there exists a prime ideal $\mathfrak{q}_0$ such that $\mathfrak{q}_0 \cap R = \mathfrak{p}_0$. Now $S/\mathfrak{q}_0$ is integral over $R/\mathfrak{p}_0$ and $\mathfrak{p}_1/\mathfrak{p}_0$ is a prime ideal of $R/\mathfrak{p}_0$. Again by the Going Up Lemma, there exists a prime ideal $\bar{\mathfrak{q}}_1$ of $S/\mathfrak{q}_0$ such that $\bar{\mathfrak{q}}_1 \cap R/\mathfrak{p}_0 = \mathfrak{p}_1/\mathfrak{p}_0$. This ideal must have the form $\bar{\mathfrak{q}}_1 = \mathfrak{q}_1/\mathfrak{q}_0$ for some prime ideal $\mathfrak{q}_1 \supseteq \mathfrak{q}_0$ of S. If equality would hold, we'd obtain $\mathfrak{p}_1 = \mathfrak{p}_0$, a contradiction. Thus $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1$. Moreover, $\mathfrak{q}_1 \cap R = \mathfrak{p}_1$. Proceeding like this, we can produce a prime ideal chain in S of length l. Thus we have shown that Krull-dim$(R) \leq$ Krull-dim(S).

For the converse, let $\mathfrak{q}_0 \subsetneq \ldots \subsetneq \mathfrak{q}_l$ be a prime ideal chain in S. Set $\mathfrak{p}_i := \mathfrak{q}_i \cap R$. Then $\mathfrak{p}_0 \subseteq \ldots \subseteq \mathfrak{p}_l$ is a prime ideal chain in R. If all inclusions are strict, we have shown that Krull-dim$(R) \geq$ Krull-dim(S) as desired. Suppose conversely that $\mathfrak{p}_i = \mathfrak{p}_{i+1}$. It suffices to show that this implies $\mathfrak{q}_i \supseteq \mathfrak{q}_{i+1}$. Let $s \in \mathfrak{q}_{i+1}$. Since $S/\mathfrak{q}_i$ is integral over $R/\mathfrak{p}_i$, we have an equation $\bar{s}^n + \bar{r}_{n-1}\bar{s}^{n-1} + \ldots + \bar{r}_1\bar{s} + \bar{r}_0 = 0$, where we may assume that n is minimal with this property. Then we have $\bar{r}_0 \in R/\mathfrak{p}_i = R/\mathfrak{p}_{i+1}$ on the one hand and $\bar{r}_0 \in \mathfrak{q}_{i+1}/\mathfrak{q}_i$ on the other. This implies that $\bar{r}_0 = 0$. Then $\bar{s}(\bar{s}^{n-1} + \ldots + \bar{r}_1) = 0$ holds in the domain $S/\mathfrak{q}_i$. Due to the minimality of n, we may conclude that $\bar{s} = 0$, that is, $s \in \mathfrak{q}_i$. $\square$

Lemma 5 *Let $R \subseteq S$ be an arbitrary ring extension and let $\mathfrak{p}$ be a prime ideal of R. Then there exists a prime ideal $\mathfrak{q}$ of S such that $\mathfrak{q} \cap R = \mathfrak{p}$ if and only if $\mathfrak{p} = \mathfrak{p}S \cap R$.*

Proof: If $\mathfrak{p} = \mathfrak{q} \cap R$ for some $\mathfrak{q}$, then $\mathfrak{p}S \cap R = (\mathfrak{q} \cap R)S \cap R \subseteq \mathfrak{q} \cap R = \mathfrak{p}$ and the other inclusion holds anyhow. Conversely, let $\mathfrak{p} = \mathfrak{p}S \cap R$. Consider the ideal $\mathfrak{p}_\mathfrak{p} S_\mathfrak{p}$ in $S_\mathfrak{p}$. Since $\mathfrak{p}S \cap (R \setminus \mathfrak{p}) = \emptyset$, this is a proper ideal and hence contained in a maximal ideal $\mathfrak{m}$ of $S_\mathfrak{p}$. The rest of the argument is analogous to the proof of the Going Up Lemma. $\square$

If $R \subseteq S$ is a ring extension and I is an ideal of R, then $s \in S$ is said to be integral over I if it satisfies a relation $s^n = \sum_{i=0}^{n-1} r_i s^i$ with $r_i \in I$. Let $\bar{I} = \{s \in S \mid s \text{ is integral over } I\}$.

Lemma 6 *Let $R \subseteq S$ be an arbitrary ring extension and let $\bar{R}$ be the integral closure of R in S. Let I be an ideal of R. Then $\bar{I} = \mathrm{Rad}(I\bar{R})$. In particular, $\bar{I}$ is closed under addition and multiplication.*

Proof: Let s be integral over I, then $s^n = \sum_{i=0}^{n-1} r_i s^i$ with $r_i \in I$ and $s \in \bar{R}$. Thus $s^n \in I\bar{R}$ and hence $s \in \mathrm{Rad}(I\bar{R})$.

Conversely, let $s \in \mathrm{Rad}(I\bar{R})$. Then $s^n = \sum_{i=0}^{n-1} r_i s_i$ with $r_i \in I$ and $s_i \in \bar{R}$. Since each s_i is integral over R, the ring $R[s_1, \ldots, s_n]$ is finitely generated as an R-module, say, by $g_1, \ldots, g_m$. Then $s^n g_i = \sum r_j s_j g_i = \sum r_j \sum r_{ijk} g_k$ for all i, which yields a matrix equation $s^n g = Ag$ with $A \in I^{m \times m}$. This implies that $\det(s^n I_m - A) = 0$, which shows that $s^{nm} = \sum_{i=0}^{nm-1} a_i s^i$ for some $a_i \in I$. Thus $s \in \bar{I}$. $\square$

Lemma 7 *Let $R \subseteq S$ be an arbitrary ring extension, where R, S are domains and R is normal. Let I be an ideal of R. Let $s \in S$ be integral over I. Then s is algebraic over $K := \mathrm{Quot}(R)$ and if $s^m = \sum_{i=0}^{m-1} k_i s^i$ with $k_i \in K$ is its minimal equation (i.e., m is minimal), then $k_i \in \mathrm{Rad}(I)$.*

Proof: Let $s^n = \sum_{i=0}^{n-1} r_i s^i$, where $r_i \in I$. Since s is integral over R, it is clearly algebraic over K. Let L be an extension field of K that contains s and over which $f = x^n - \sum_{i=0}^{n-1} r_i x^i \in R[x]$ splits into linear factors, that is, $f = \prod_{i=1}^{n}(x - l_i)$ for some $l_i \in L$, where we may assume that $l_1 = s$. Let $g \in K[x]$ be the minimal polynomial of $s \in L$. Then g is a divisor of f and we may assume that $g = \prod_{i=1}^{m}(x - l_i)$ for some $m \leq n$ without loss of generality. Expanding $g = x^m - \sum_{i=0}^{m-1} k_i x^i$, the coefficients $k_i \in K$ are in $R[l_1, \ldots, l_m]$. Since each l_i is integral over R, the k_i are also integral over R. Since R is normal, we must have $k_i \in R$.

Moreover, the k_i can be written as sums and products of the l_i. Since $l_i \in \bar{I}$ for all i, this implies that $k_i \in \bar{I}$ by Lemma 6. Thus we have representations $k_i^{n_i} = \sum_{j=0}^{n_i-1} r_{ij} k_i^j$ for some $r_{ij} \in I$. Since $k_i \in R$, this implies that $k_i \in \mathrm{Rad}(I)$. $\square$

Theorem 4 (Cohen-Seidenberg Going Down Theorem) *Let $R \subseteq S$ be an integral ring extension, where R, S are domains and R is normal. Let $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1$ be prime ideals of R. Let $\mathfrak{q}_1$ be a prime ideal of S such that $\mathfrak{q}_1 \cap R = \mathfrak{p}_1$. Then there exists prime ideal $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1$ of S such that $\mathfrak{q}_0 \cap R = \mathfrak{p}_0$.*

Proof: It suffices to show that there exists $\mathfrak{q}_0 \subseteq \mathfrak{q}_1$ with the desired property. If equality would hold, we'd obtain $\mathfrak{p}_0 = \mathfrak{p}_1$, a contradiction. Consider $R \subseteq S \subseteq S_{\mathfrak{q}_1}$. The prime ideals of $S_{\mathfrak{q}_1}$ have the form $\mathfrak{q}_{\mathfrak{q}_1}$ where $\mathfrak{q}$ is a prime ideal of S that is contained in $\mathfrak{q}_1$. Therefore it suffices to show that $\mathfrak{p}_0$ is the contraction to R of some prime ideal in $S_{\mathfrak{q}_1}$. According to Lemma 5, we need to show that $\mathfrak{p}_0 = \mathfrak{p}_0 S_{\mathfrak{q}_1} \cap R$.

Let $r \in R$ be such that $r = \frac{a}{b}$ with $a \in \mathfrak{p}_0 S$ and $b \in S \setminus \mathfrak{q}_1$. We need to show that $r \in \mathfrak{p}_0$. Without loss of generality, let $r \neq 0$. Since $a \in \mathfrak{p}_0 S$, and $S = \bar{R}$, we have $a \in \bar{\mathfrak{p}}_0$ according to Lemma 6. By Lemma 7, the minimal equation of a over $K := \mathrm{Quot}(R)$ has the form

$$a^k = \sum_{i=0}^{k-1} c_i a^i \tag{1}$$

with $c_i \in \mathfrak{p}_0$. Since $b = \frac{a}{r}$ and $\frac{1}{r}$ is a unit in K, the minimal equation for b over K is obtained by dividing (1) by r^k, which yields

$$b^k = \sum_{i=0}^{k-1} \frac{c_i}{r^{k-i}} b^i. \tag{2}$$

Set $d_i := \frac{c_i}{r^{k-i}}$. Since b is integral over R, we have $d_i \in R$, again by Lemma 7. Suppose that $r \notin \mathfrak{p}_0$. Then $r^{k-i} d_i = c_i \in \mathfrak{p}_0$ implies that $d_i \in \mathfrak{p}_0$. Then (2) implies that $b^k \in \mathfrak{p}_0 S \subseteq \mathfrak{p}_1 S \subseteq \mathfrak{q}_1$, a contradiction. $\square$

Corollary 1 *In the situation of the Going Down Theorem, we have* $\mathrm{ht}(\mathfrak{q}) = \mathrm{ht}(\mathfrak{q} \cap R)$ *for every prime ideal $\mathfrak{q}$ of S.*

Proof: Let $\mathfrak{q}_0 \subsetneq \ldots \subsetneq \mathfrak{q}_l = \mathfrak{q}$ be a prime ideal chain in S. As in the proof of Theorem 3, one can show that $\mathfrak{q}_0 \cap R \subsetneq \ldots \subsetneq \mathfrak{q}_l \cap R = \mathfrak{q} \cap R$ is a prime ideal chain in R. Thus $\mathrm{ht}(\mathfrak{q}) \leq \mathrm{ht}(\mathfrak{q} \cap R)$. (This part of the proof works for arbitrary integral extensions, the Going Down Theorem was not used.)

Conversely, let $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_l = \mathfrak{q} \cap R$ be a prime ideal chain in R. Applying the Going Down Theorem repeatedly, we obtain a prime ideal chain $\mathfrak{q}_0 \subsetneq \ldots \subsetneq \mathfrak{q}_l = \mathfrak{q}$. Thus $\mathrm{ht}(\mathfrak{q}) \geq \mathrm{ht}(\mathfrak{q} \cap R)$. $\square$