The Going-Up and Going-Down Theorems

William Gao

July 30, 2025

1 Introduction

We assume familiarity with the basic definitions of commutative rings and modules. The requisite background may be found in the first three chapters of Atiyah and Macdonald's book [AM18].

Commutative algebra is the study of commutative rings and their ideals. The prototypical commutative ring is $\mathbb{Z}$, which contains an ideal $(m) := m\mathbb{Z}$ for every integer m consisting of all multiples of m. Multiplying each integer by 2 gives a ring homomorphism $\phi : \mathbb{Z} \to 2\mathbb{Z}$. This sends the ideal (m) of $\mathbb{Z}$ to the ideal $(2m)$ of $2\mathbb{Z}$. Going in the reverse direction we obtain, for each ideal $(2m)$ of $2\mathbb{Z}$, an ideal (m) of $\mathbb{Z}$ by undoing the multiplication by 2, or simply by dividing by 2.

Likewise, embedding $\mathbb{Z}$ as the constant polynomials in the polynomial ring $\mathbb{Z}[x]$ also gives a ring homomorphism. Yet the ideal (m) of $\mathbb{Z}$ considered as the subset $m\mathbb{Z}$ of $\mathbb{Z}[x]$ is not an ideal unless $m = 0$. Nevertheless, it is easy to generate from $m\mathbb{Z}$ an ideal $m\mathbb{Z}[x]$ of $\mathbb{Z}[x]$. Conversely, for each ideal of $\mathbb{Z}[x]$ we obtain an ideal of $\mathbb{Z}$ by undoing the embedding, which amounts to pulling out the constant term of each polynomial. We have thus illustrated that a ring homomorphism comes with a partial correspondence of ideals.

In these notes, we provide conditions under which this correspondence becomes complete.

2 Extension and Contraction

We begin by formalizing the correspondence of ideals under homomorphism suggested by the introduction. As a standing assumption, A and B will be commutative rings with unit.

Definition 2.1

Let $\phi : A \to B$ be a ring homomorphism. Let $\mathfrak{a}$ be an ideal of A and $\mathfrak{b}$ an ideal of B.

(1) The *extension* of $\mathfrak{a}$ under ϕ is $\mathfrak{a}^e_\phi := B\phi(\mathfrak{a})$.

(2) The *contraction* of $\mathfrak{b}$ under ϕ is $\mathfrak{b}^c_\phi := \phi^{-1}(\mathfrak{b})$.

We suppress the subscript when there is no ambiguity in the underlying map ϕ. The extension $\mathfrak{a}^e$ is clearly an ideal of B; in fact it is the ideal generated by $\phi(\mathfrak{a})$. Similarly, $\mathfrak{b}^c$ is an ideal of A: the fact that $\mathfrak{b}^c$ is an additive subgroup follows from the properties of $\mathfrak{b}$ and ϕ; if furthermore $x \in A$ and $y \in \mathfrak{b}^c$, then $\phi(y) \in \mathfrak{b}$ so $\phi(xy) = \phi(x)\phi(y) \in \mathfrak{b}$, hence $xy \in \mathfrak{b}^c$.

We hold a special interest in prime ideals, which behave nicely under contraction.

Lemma 2.2

Let $\phi : A \to B$ be a ring homomorphism and $\mathfrak{q}$ a prime ideal of B. Then its contraction $\mathfrak{q}^c$ is a prime ideal of A.

Proof. We already know $\mathfrak{q}^c$ is an ideal. To see that it is moreover prime, let $xy \in \phi^{-1}(\mathfrak{q})$, so that $\phi(xy) = \phi(x)\phi(y) \in \mathfrak{q}$. Since $\mathfrak{q}$ is a prime ideal, we must have $\phi(x) \in \mathfrak{q}$ or $\phi(y) \in \mathfrak{q}$. Thus $x \in \phi^{-1}(\mathfrak{q})$ or $y \in \phi^{-1}(\mathfrak{q})$. □

Example 2.3

Let $\phi : \mathbb{Z} \to \mathbb{Z}[x]$ be the inclusion and consider the prime ideal $2\mathbb{Z}[x]$ of $\mathbb{Z}[x]$. The contraction of $2\mathbb{Z}[x]$ is $2\mathbb{Z}[x] \cap \mathbb{Z} = (2)$, which is a prime ideal of $\mathbb{Z}$.

The corresponding statement for extension is false. For example, let $A = \mathbb{Z}$ and consider the prime ideal (2) of $\mathbb{Z}$. Let $B = \mathbb{Q}$ and let $\phi : \mathbb{Z} \to \mathbb{Q}$ be the inclusion. The extension of (2) is $\mathbb{Q}(2) = \mathbb{Q}$, which is not a prime ideal.

It follows from the set-theoretic properties $\mathfrak{a} \subseteq \phi^{-1}(\phi(\mathfrak{a}))$ and $\phi(\phi^{-1}(\mathfrak{b})) \subseteq \mathfrak{b}$ that $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$ and $\mathfrak{b}^{ce} \subseteq \mathfrak{b}$, respectively. From these inclusions, we get

$$\mathfrak{a}^e = \mathfrak{a}^{ece} \text{ and } \mathfrak{b}^c = \mathfrak{b}^{cec}. \tag{2.1}$$

When is a prime ideal of A necessarily the contraction of a prime ideal of B? This is the motivating question of our work, and we conclude this section with our first attempt at a satisfying answer.

Lemma 2.4

Let $\phi : A \to B$ be a ring homomorphism and let $\mathfrak{p}$ be a prime ideal of A. Then $\mathfrak{p}$ is the contraction of a prime ideal of B if and only if $\mathfrak{p}^{ec} = \mathfrak{p}$.

Proof. If there is a prime ideal $\mathfrak{q}$ of B such that $\mathfrak{q}^c = \mathfrak{p}$, then by eq. (2.1),

$$\mathfrak{p}^{ec} = \mathfrak{q}^{cec} = \mathfrak{q}^c = \mathfrak{p}.$$

Conversely, suppose $\mathfrak{p}^{ec} = \mathfrak{p}$. Define a multiplicatively closed subset of B by $S = \phi(A \setminus \mathfrak{p})$. Indeed generic elements of S take the form $\phi(x), \phi(y)$ where $x, y \in A \setminus \mathfrak{p}$. Since $\mathfrak{p}$ is a prime ideal this implies $xy \in A \setminus \mathfrak{p}$, and thus $\phi(x)\phi(y) = \phi(xy) \in S$. Hence we may consider the localization $S^{-1}B$ with canonical map $\psi : B \to S^{-1}B$ given by $x \mapsto \frac{x}{1}$. By assumption

$$A \setminus \mathfrak{p} = A \setminus \mathfrak{p}^{ec} = A \setminus \phi^{-1}(\mathfrak{p}^e) = \phi^{-1}(B \setminus \mathfrak{p}^e),$$

so $S = \phi(A \setminus p)$ does not intersect $\mathfrak{p}^e$. Thus $\psi(\mathfrak{p}^e)$ contains no units in $S^{-1}B$ and $(\mathfrak{p}^e)^e_\psi$ is a proper ideal of $S^{-1}B$. By Zorn's lemma, $(\mathfrak{p}^e)^e_\psi$ is contained in some maximal ideal $\mathfrak{m}$ of $S^{-1}B$.

Let $\mathfrak{q} \coloneqq \mathfrak{m}^c_\psi$. Lemma 2.2 shows that $\mathfrak{q}$ is a prime ideal of B. Moreover $(\mathfrak{p}^e)^e_\psi \subseteq \mathfrak{m}$ implies

$$\mathfrak{p}^e \subseteq (\mathfrak{p}^e)^{ec}_\psi \subseteq \mathfrak{m}^c = \mathfrak{q}$$

and thus $\mathfrak{p} = \mathfrak{p}^{ec} \subseteq \mathfrak{q}^c$. We also know that $\mathfrak{q}$ does not intersect S, otherwise $\mathfrak{m}$ would contain a unit in $S^{-1}B$. Therefore $\mathfrak{q}^c$ does not intersect $A \setminus \mathfrak{p}$; that is $\mathfrak{q}^c \subseteq \mathfrak{p}$. □

3 The Cayley-Hamilton Theorem

The Cayley-Hamilton theorem is a fundamental result in linear algebra which states that a linear operator satisfies its own characteristic polynomial. We provide a generalization to finitely-generated modules. Its significance will become apparent in the next section, when we study polynomial dependence in more detail.

Theorem 3.1 (Cayley-Hamilton)
Let M be a finitely-generated A-module, $\mathfrak{a}$ an ideal of A, and $\phi : M \to M$ an A-module homomorphism such that $\phi(M) \subseteq \mathfrak{a}M$. Then there exist $a_1, \ldots, a_n \in \mathfrak{a}$ such that

$$\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0.$$

Proof. Let $x_1, \ldots, x_n$ generate M. For $1 \leq i \leq n$ we have $\phi(x_i) \in \phi(M) \subseteq \mathfrak{a}M$, so we may write

$$\phi(x_i) = \sum_{j=1}^{n} a_{ij}x_j$$

for $a_{ij} \in \mathfrak{a}$. In other words if δ_{ij} is the Kronecker delta, then

$$\sum_{j=1}^{n} (\delta_{ij}\phi - a_{ij})x_j = 0.$$

If $A = (a_{ij})$, I is the identity matrix, and $x = (x_1, \ldots, x_n)$, we can write this as $(I\phi - A)x = 0$. Now multiplying on the left by the adjugate matrix of $I\phi - A$,

$$\det(I\phi - A)x = \operatorname{adj}(I\phi - A)(I\phi - A)x = 0.$$

Hence $\det(I\phi - A) = 0$, and we obtain the desired equation by expanding the determinant. □

4 Integral Dependence

A classical goal of field theory was to determine, given a base field K, which polynomials in $K[x]$ (i.e. with coefficients in K) have roots in K, and to determine, for those polynomials with no roots in K, over which field extension of K we may find its roots. More formally, let L be a field extension of K. We say $\alpha \in L$ is *algebraic* over K if it is the root of some polynomial in $K[x]$.

The analogue of algebraic dependence in the commutative ring setting is integral dependence. In this case we impose the further requirement that the polynomial be monic.

Definition 4.1
Let A be a subring of B. An element $x \in B$ is *integral* over A if it is the root of a monic polynomial in $A[x]$; that is, there exist $a_1, \ldots, a_n \in A$ such that

$$x^n + a_1x^{n-1} + \cdots + a_n = 0. \tag{4.1}$$

Every $x \in A$ is integral over A by $x - x = 0$. The requirement that the polynomial in eq. (4.1) be monic is nontrivial. For example, every rational number $\frac{r}{s} \in \mathbb{Q}$ is algebraic over $\mathbb{Z}$ since $s \cdot \frac{r}{s} - r = 0$,

but only integers are integral over $\mathbb{Z}$: if $\frac{r}{s}$ is in lowest terms, we have

$$(\tfrac{r}{s})^n + a_1(\tfrac{r}{s})^{n-1} + \cdots + a_{n-1} = 0,$$

and then

$$r^n + sa_1r^{n-1} + \cdots + s^n a_{n-1} = 0,$$

so s divides r^n. Hence $s = \pm 1$, thus $\frac{r}{s} \in \mathbb{Z}$.

Henceforth, A will be a subring of B. The following characterization of integral elements will be useful, and notably features our first deployment of the Cayley-Hamilton theorem.

Theorem 4.2

The following are equivalent:

(1) $x \in B$ is integral over A.

(2) $A[x]$ is a finitely-generated A-module.

(3) $A[x] \subseteq C$ for some subring C of B which is a finitely-generated A-module.

(4) There exists a faithful $A[x]$-module M which is finitely-generated as an A-module.

Proof. (1) $\implies$ (2). Since $x \in B$ is integral over A we have

$$x^n + a_1x^{n-1} + \cdots + a_n = 0$$

for some $a_i \in A$. We claim that $1, x, \ldots, x^{n-1}$ generates $A[x]$ as an A-module. For each $r \geq 0$, we have

$$x^{n+r} = -(a_1x^{n+r-1} + \cdots + a_nx^r).$$

By induction on r, each power of x is in the A-module generated by $1, x, \ldots, x^{n-1}$, as desired.

(2) $\implies$ (3). Let $C \coloneqq A[x]$. This is a subring of B and a finitely-generated A-module by assumption.

(3) $\implies$ (4). Let $M \coloneqq C$. This is a faithful $A[x]$-module because if $yM = 0$ then in particular $y1 = 0$, and a finitely-generated A-module by assumption.

(4) $\implies$ (1). We use Theorem 3.1 (Cayley-Hamilton) with ϕ being multiplication by x and $\mathfrak{a} = A$. ϕ is an A-module homomorphism such that $xM \subseteq M$ since M is an $A[x]$-module. We conclude that there exist $a_1, \ldots, a_n \in A$ such that

$$x^n + a_1x^{n-1} + \cdots + a_n$$

annihilates M; since M is faithful it must be zero. □

As a corollary of the equivalence of (1) and (2), if $x, y \in B$ are integral over A, then $A[x]$ is a finitely-generated A-module. Furthermore y is integral over $A[x]$, so $A[x, y] = A[x][y]$ is a finitely-generated $A[x]$-module, thus a finitely-generated A-module. Now $x + y \in A[x, y]$ so $A[x + y] \subseteq A[x, y]$, where $A[x, y]$ is a subring of B and a finitely-generated A-module. By the equivalence of (3) and (1), $x + y \in B$ is integral over A. Similarly $xy \in A[x, y]$ so $xy \in B$ is integral over A. This justifies the following definition.

Definition 4.3
The *integral closure* of A in B is the subring $\overline{A}$ of elements in B which are integral over A.

If $A = \overline{A}$ we say A is integrally closed in B, if $\overline{A} = B$ we say B is integral over A. The latter is a property that is preserved under quotients and localizations.

Lemma 4.4
Let B be integral over A. Let $\iota : A \hookrightarrow B$ be the inclusion map.

(1) Let $\mathfrak{b}$ be an ideal of B and $\mathfrak{a} := \mathfrak{b}_\iota^c = A \cap \mathfrak{b}$ its contraction under the inclusion. Then $B/\mathfrak{b}$ is integral over $A/\mathfrak{a}$.

(2) Let S is a multiplicatively closed subset of A, and thus B. Then $S^{-1}B$ is integral over $S^{-1}A$.

Proof. (1) Given $\overline{x} \in B/\mathfrak{b}$, since $x \in B$ and B is integral over A we have

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

for some $a_i \in A$. Reducing modulo $\mathfrak{b}$,

$$\overline{x}^n + \overline{a}_1 \overline{x}^{n-1} + \cdots + \overline{a}_n = \overline{0},$$

where $\overline{a}_i \in A/(A \cap \mathfrak{b}) = A/\mathfrak{a}$.

(2) Given $\frac{x}{s} \in S^{-1}B$, since $x \in B$ and B is integral over A we have

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

for some $a_i \in A$. Then

$$(\tfrac{x}{s})^n + (\tfrac{a_1}{s})(\tfrac{x}{s})^{n-1} + \cdots + \tfrac{a_n}{s^n} = 0,$$

where $\frac{a_i}{s} \in S^{-1}A$.

□

Recall that a ring is an integral domain if it has no zero divisors. This strengthens the notion of integral dependence to provide the following dependence of fields.

Lemma 4.5
Let $A \subseteq B$ be integral domains, and let B be integral over A. Then B is a field if and only if A is a field.

Proof. ($\Longrightarrow$) Suppose B is a field. Let $x \in A$ be nonzero. Then $x^{-1} \in B$, so it is integral over A; that is,

$$x^{-m} + a_1 x^{-m+1} + \cdots + a_m = 0$$

for some $a_i \in A$. Multiplying by x^{m-1},

$$x^{-1} = -(a_1 + a_2 x + \cdots + a_m x^{m-1}) \in A.$$

($\Longleftarrow$) Suppose A is a field. Let $y \in B$ be nonzero. Since y is integral over A, we have

$$y^n + a_1' y^{n-1} + \cdots + a_n' = 0 \tag{4.2}$$

for $a_i' \in A$. We may assume that this has minimal degree among all equations of integral dependence, so that $a_n' \neq 0$. Otherwise, the equation eq. (4.2) could be written as

$$y(y^{n-1} + a_1' y^{n-2} + \cdots + a_{n-1}') = 0.$$

Then since B is an integral domain, $y^{n-1} + a_1' y^{n-2} + \cdots + a_{n-1}' = 0$, contradicting minimality in eq. (4.2). We conclude that

$$y^{-1} = -(a_n')^{-1}(y^{n-1} + a_1' y^{n-2} + \cdots + a_{n-1}) \in B.$$

□

Along with the natural behaviour of quotients, the previous statement about fields unsurprisingly yields a statement about maximal ideals.

Lemma 4.6

Let B be integral over A. Let $\mathfrak{q}$ be a prime ideal of B and let $\mathfrak{p} \coloneqq \mathfrak{q}^c = \mathfrak{q} \cap A$ be its contraction under the inclusion $A \hookrightarrow B$. Then $\mathfrak{q}$ is maximal if and only if $\mathfrak{p}$ is maximal.

Proof. We know that $\mathfrak{q}$ is a prime ideal of B and $\mathfrak{p} = \mathfrak{q} \cap A$ is a prime ideal of A and, so $B/\mathfrak{q}$ and $A/\mathfrak{p}$ are integral domains with $A/\mathfrak{q} \subseteq B/\mathfrak{q}$. By Lemma 4.4, $B/\mathfrak{q}$ is integral over $A/\mathfrak{p}$. By Lemma 4.5, $B/\mathfrak{q}$ is a field if and only if $A/\mathfrak{p}$ is a field, or equivalently $\mathfrak{q}$ is a maximal ideal of B if and only if $\mathfrak{p}$ is a maximal ideal of A. □

We can make the definition of integral dependence without A being a subring. The only other case we are interested in is integral dependence over an ideal, which is completely characterized by the following lemma.

Lemma 4.7

Let $\mathfrak{a}$ be an ideal of A, let $A \subseteq B$, and let $\iota : A \hookrightarrow \overline{A}$ be the inclusion map. Then the integral closure of $\mathfrak{a}$ in B is $\sqrt{\mathfrak{a}_\iota^e}$.

Proof. If $x \in B$ is integral over $\mathfrak{a}$, then there exist $a_1, \ldots, a_n \in \mathfrak{a}$ such that

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0.$$

In particular $a_1, \ldots, a_n \in A$ implies $x \in \overline{A}$, so $x^n = -(a_1 x^{n-1} + \cdots + a_n) \in \overline{A}\mathfrak{a} = \mathfrak{a}_\iota^e$ implies $x \in \sqrt{\mathfrak{a}_\iota^e}$.

Conversely if $x \in \sqrt{\mathfrak{a}_\iota^e}$ then we may write

$$x^k = \sum_{i=1}^{m} c_i x_i \tag{4.3}$$

for some k, $c_i \in \mathfrak{a}$ and $x_i \in \overline{A}$. Since each x_i is integral over A, the A-module $M \coloneqq A[x_1, \ldots, x_m]$ is finitely-generated, and eq. (4.3) shows that $x^k M \subseteq \mathfrak{a}M$. By taking ϕ to be multiplication by x^k in Theorem 3.1, there exist $a_1, \ldots, a_n \in \mathfrak{a}$ such that

$$(x^k)^n + a_1 (x^k)^{n-1} + \cdots + a_n = 0.$$

Thus x is integral over $\mathfrak{a}$. □

Now looking at integral elements over an ideal, we can characterize its minimal polynomial.

Lemma 4.8
Let $A \subseteq B$ be integral domains, let A be integrally closed in its field of fractions $K(A)$, let $\mathfrak{a}$ be an ideal of A, and let $x \in B$ be integral over $\mathfrak{a}$. Then x is algebraic over $K(A)$, and if its minimal polynomial over $K(A)$ is $t^m + b_1 t^{m-1} + \cdots + b_m$, then $b_1, \ldots, b_m \in \sqrt{\mathfrak{a}}$.

Proof. Since x is integral over $\mathfrak{a}$, it satisfies an equation of integral dependence

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0, \tag{4.4}$$

where $a_1, \ldots, a_n \in \mathfrak{a}$. Since $\mathfrak{a} \subseteq A \subseteq K(A)$, x is certainly algebraic over $K(A)$. Let

$$t^m + b_1 t^{m-1} + \cdots + b_m \tag{4.5}$$

be the minimal polynomial of x over $K(A)$. In particular eq. (4.5) divides the left side of eq. (4.4). Let L be the algebraic closure of $K(A)$, so that L contains all the roots $x_1, \ldots, x_n$ of eq. (4.5). Then each x_i satisfies eq. (4.4), so each x_i is integral over $\mathfrak{a}$. If $\overline{A}_L$ is the integral closure of A in L and $\iota : A \hookrightarrow \overline{A}_L$ is the inclusion map, then by Lemma 4.7, $x_i \in \sqrt{\mathfrak{a}^e_\iota}$.

By Vieta's formulas, the coefficients $b_1, \ldots, b_m$ of eq. (4.5) are polynomials in the x_i, so they also lie in $\sqrt{\mathfrak{a}^e_\iota}$ and thus are integral over $\mathfrak{a}$. Since A is integrally closed in $K(A)$, Lemma 4.7 states that the integral closure of $\mathfrak{a}$ in $K(A)$ is simply $\sqrt{\mathfrak{a}}$. Therefore $b_1, \ldots, b_m \in \sqrt{\mathfrak{a}}$. □

5 Lying-Over, Going-Up, and Going-Down

The three procedures of interest are introduced in the following definition.

Definition 5.1
Let $\phi : A \to B$ be a ring homomorphism.

(1) Let $\mathfrak{p}$ be a prime ideal of A. A prime ideal $\mathfrak{q}$ of B *lies over* $\mathfrak{p}$ if $\mathfrak{p} = \mathfrak{q}^c$.

(2) ϕ has the *going-up property* if given any chain $\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$ of prime ideals of A and any chain $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$ of prime ideals of B such that $m < n$ and $\mathfrak{q}_j$ lies over $\mathfrak{p}_j$ for $1 \leq j \leq m$, the latter chain may be extended to a chain $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_n$ such that each $\mathfrak{q}_j$ lies over $\mathfrak{p}_j$.

(3) ϕ has the *going-down property* if given any chain $\mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$ of prime ideals of A and any chain $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$ of prime ideals of B such that $m < n$ and each $\mathfrak{q}_j$ lies over $\mathfrak{p}_j$, the latter chain may be extended to a chain $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_n$ such that each $\mathfrak{q}_j$ lies over $\mathfrak{p}_j$.

From now on, we will implicitly extend and contract ideals under the inclusion $A \hookrightarrow B$, meaning $\mathfrak{a}^e = B\mathfrak{a}$ and $\mathfrak{b}^c = \mathfrak{b} \cap A$.

Theorem 5.2 (Lying-over)
Let B be integral over A and $\mathfrak{p}$ a prime ideal of A. Then there exists a prime ideal $\mathfrak{q}$ of B that lies over $\mathfrak{p}$.

Proof. The following diagram commutes:

$$\begin{array}{ccc} A & \hookrightarrow & B \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ A_{\mathfrak{p}} & \hookrightarrow & B_{\mathfrak{p}} \end{array} \tag{5.1}$$

By Lemma 4.4, $B_{\mathfrak{p}}$ is integral over $A_{\mathfrak{p}}$. Let $\mathfrak{n}$ be a maximal ideal of $B_{\mathfrak{p}}$. Then $\mathfrak{m} \coloneqq \mathfrak{n}^c = \mathfrak{n} \cap A_{\mathfrak{p}}$ is a maximal ideal of $A_{\mathfrak{p}}$ by Lemma 4.6. In fact $A_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{m} = \mathfrak{p}_\alpha^e \coloneqq \mathfrak{p}A_{\mathfrak{p}}$, since every element not contained in $\mathfrak{p}A_{\mathfrak{p}}$ is a unit. Let $\mathfrak{q} \coloneqq \mathfrak{n}_\beta^c = \beta^{-1}(\mathfrak{n})$. Then $\mathfrak{q}$ is a prime ideal of B and we claim that

$$\mathfrak{q} \cap A = \alpha^{-1}(\mathfrak{m}) = \alpha^{-1}(\mathfrak{p}A_{\mathfrak{p}}) = \mathfrak{p}.$$

We have $x \in \mathfrak{q} \cap A$ if and only if $x \in A$ and $\beta(x) \in \mathfrak{n}$. Since eq. (5.1) commutes, this is equivalent to $\alpha(x) \in \mathfrak{m}$, hence $\mathfrak{q} \cap A = \alpha^{-1}(\mathfrak{m}) = \alpha^{-1}(\mathfrak{p}A_{\mathfrak{p}})$. Now $x \in \alpha^{-1}(\mathfrak{p}A_{\mathfrak{p}})$ if and only if $\frac{x}{1} \in \mathfrak{p}A_{\mathfrak{p}}$, or $x \in A\mathfrak{p} = \mathfrak{p}$. Therefore $\mathfrak{q}$ lies over $\mathfrak{p}$. □

The going-up property is now a direct consequence of the lying-over theorem.

Theorem 5.3 (Going-up)
Let B be integral over A. Then $A \hookrightarrow B$ has the going-up property.

Proof. By induction, it suffices to show that given prime ideals $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ of A and a prime ideal $\mathfrak{q}_1$ of B lying over $\mathfrak{p}_1$, there exists a prime ideal $\mathfrak{q}_2$ of B that lies over $\mathfrak{p}_2$.

We know that $A/\mathfrak{p}_1 \subseteq B/\mathfrak{q}_2$ are rings, $B/\mathfrak{q}_2$ is integral over $A/\mathfrak{p}_1$ by Lemma 4.4, and $\mathfrak{p}_2/\mathfrak{p}_1$ is a prime ideal of $A/\mathfrak{p}_1$. By Theorem 5.2, there exists a prime ideal of $B/\mathfrak{q}_1$ that lies over $\mathfrak{p}_2/\mathfrak{p}_1$. By the fourth isomorphism theorem this prime ideal takes the form $\mathfrak{q}_2/\mathfrak{q}_1$ for some prime ideal $\mathfrak{q}_2$ of B. In particular $(\mathfrak{q}_2/\mathfrak{q}_1) \cap (A/\mathfrak{p}_1) = \mathfrak{p}_2/\mathfrak{p}_1$, hence $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$ meaning $\mathfrak{q}_2$ lies over $\mathfrak{p}_2$. □

With stronger assumptions and a more delicate proof, we pick up the going-down property as well.

Theorem 5.4 (Going-down)
Let $A \subseteq B$ be integral domains, A integrally closed in its field of fractions $K(A)$, and B integral over A. Then $A \hookrightarrow B$ has the going-down property.

Proof. As in the proof of going-up, it suffices to show that given prime ideals $\mathfrak{p}_1 \supseteq \mathfrak{p}_2$ of A and a prime ideal $\mathfrak{q}_1$ of B lying over $\mathfrak{p}_1$, $\mathfrak{p}_2$ is the contraction of a prime ideal $\mathfrak{q}_2 \subseteq \mathfrak{q}_1$. Note that $\mathfrak{q}_2 \subseteq \mathfrak{q}_1$ if and only if $\mathfrak{q}_2$ is a prime ideal in $B_{\mathfrak{q}_1}$. Let $\beta : A \to B_{\mathfrak{q}_1}$ be the restriction of the canonical homomorphism $x \mapsto \frac{x}{1}$ to A. By Lemma 2.4, $\mathfrak{p}_2$ is the contraction of a prime ideal of $B_{\mathfrak{q}_1}$ if and only if

$$\mathfrak{p}_2 = ((\mathfrak{p}_2)_\beta^e)_\beta^c = (B_{\mathfrak{q}_1}\mathfrak{p}_2)_\beta^c = B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A.$$

The $\subseteq$ inclusion is immediate since $1 \in B_{\mathfrak{q}_1}$. It remains to show that $B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A \subseteq \mathfrak{p}_2$. Every element of $B_{\mathfrak{q}_1}\mathfrak{p}_2$ may be written as $\frac{y}{s}$, where $y \in B\mathfrak{p}_2$ and $s \in B \setminus \mathfrak{q}_1$. In particular $y \in \mathfrak{p}_2^e \subseteq \sqrt{\mathfrak{p}_2^e}$, where the extension is under the inclusion $A \hookrightarrow B$ as usual. Since B is precisely the integral closure of A in B, Lemma 4.7 shows that y is integral over $\mathfrak{p}_2$. Now applying Lemma 4.8, y is algebraic over $K(A)$ and its minimal equation over $K(A)$ takes the form

$$y^r + u_1 y^{r-1} + \cdots + u_r = 0, \tag{5.2}$$

where $u_1, \dots, u_r \in \mathfrak{p}_2$. Let $x = \frac{y}{s} \in B_{\mathfrak{p}_1}\mathfrak{p}_2 \cap A$, so that $s = yx^{-1}$ for $x^{-1} \in K(A)$. Then the minimal equation for s over $K(A)$ is obtained by multiplying eq. (5.2) by x^{-r}, yielding

$$s^r + v_1 s^{r-1} + \cdots + v_r = 0 \tag{5.3}$$

where $v_i = u_i x^{-i}$. Hence $x^i v_i = u_i \in \mathfrak{p}_2$ for $1 \leq i \leq r$. But $s \in B$ is integral over A, so by applying Lemma 4.8 with A itself as the ideal, $v_i \in A$ for $1 \leq i \leq r$.

If we had $x \notin \mathfrak{p}_2$, then as $\mathfrak{p}_2$ is a prime ideal of A and $x^i v_i \in \mathfrak{p}_2$, we would have $v_i \in \mathfrak{p}_2$. Then

$$s^r = -(v_1 s^{r-1} + \cdots + v_r) \in B\mathfrak{p}_2 \subseteq B\mathfrak{p}_1 \subseteq \mathfrak{q}_1,$$

where the last containment holds because $B\mathfrak{p}_1 \subseteq B\mathfrak{q}_1 = \mathfrak{q}_1$. Since $\mathfrak{q}_1$ is a prime ideal of B, this implies $s \in \mathfrak{q}_1$, which is a contradiction. Therefore $x \in \mathfrak{p}_2$, and $B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A = \mathfrak{p}_2$, as desired. □

References

[AM18] M. F. Atiyah and I. G. Macdonald. *Introduction to Commutative Algebra*. CRC Press, Taylor & Francis Group, 2018. Reprint of the 1969 edition.