

# Advanced Algebra II

## INTEGRAL EXTENSION, GOING UP AND GOING DOWN THEOREMS

In this section, we are going to explore more about the notion of integral extension. The goal is to show the going up and going down theorems.

Let  $A, B$  be rings. We say  $B$  is an extension over  $A$  if  $A \subset B$ . An element  $x \in B$  is said to be integral over  $A$  if it satisfies a *monic* polynomial in  $A[x]$ .  $B$  is integral over  $A$  if every element of  $B$  is integral over  $A$ .

The following Properties are more or less parallel to the theory of algebraic extensions. Proofs are similar. The reader should find no difficulty working them out.

**Proposition 0.1.** *Let  $A \subset B$  be an extension. The followings are equivalent:*

- (1)  $x \in B$  is integral over  $A$ .
- (2)  $A[x]$  is a finitely generated  $A$ -module.
- (3)  $A[x]$  is contained in a subring  $C \subset B$  such that  $C$  is a finitely generated  $A$ -module.

**Corollary 0.2.** *Let  $A \subset B$  be an extension. If  $x_i \in B$  is integral over  $A$  for  $i = 1, \dots, n$ . Then  $A[x_1, \dots, x_n]$  is a finitely generated  $A$ -module.*

**Corollary 0.3.** *Let  $A \subset B \subset C$  be extensions. If  $C$  is integral over  $B$  and  $B$  is integral over  $A$ , then  $C$  is integral over  $A$ .*

**Corollary 0.4.** *Let  $A \subset B$  be an extension. The integral closure of  $A$  in  $B$ , which is the set of elements in  $B$  integral over  $A$ , is a ring (subring of  $B$ ).*

Let  $A \subset B$  be an extension.  $A$  is said to be integrally closed in  $B$  if the integral closure of  $A$  is  $A$  itself.

**Corollary 0.5.** *Let  $A \subset B$  be an extension. And let  $C$  be the integral closure of  $A$  in  $B$ . Then  $C$  is integrally closed in  $B$ .*

**Proposition 0.6.** *Let  $A \subset B$  be an integral extension.*

- (1) If  $\mathfrak{b} \triangleleft B$  and  $\mathfrak{a} := \mathfrak{b} \cap A$ , then  $B/\mathfrak{b}$  is integral over  $A/\mathfrak{a}$ .
- (2) Let  $S$  be a multiplicative set of  $A$  (hence of  $B$ ), then  $S^{-1}B$  is integral over  $S^{-1}A$ .

*Proof.* (1) For  $\bar{b} \in B/\mathfrak{b}$ , one notices that  $b \in B$  and  $b^n + a_{n-1}b^{n-1} + \dots + a_0 = 0$  for some  $a_i \in A$ . It's clear that  $\bar{b}^n + \overline{a_{n-1}}\bar{b}^{n-1} + \dots + \overline{a_0} = 0 \in \bar{B} := B/\mathfrak{b}$ . And hence  $\bar{b}$  is integral over  $\bar{A} := A/\mathfrak{a}$ .

- (2) For  $\frac{b}{s} \in S^{-1}B$ . One notice that  $b^n + a_{n-1}b^{n-1} + \dots + a_0 = 0$  for some  $a_i \in A$ . Hence

$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s} \left(\frac{b}{s}\right)^{n-1} + \dots + \frac{a_0}{s^n} = 0.$$

And we are done. □

**Lemma 0.7.** *Let  $A \subset B$  be an integral extension and  $B$  is an domain. Then  $A$  is a field if and only if  $B$  is a field.*

*Proof.* Suppose that  $A$  is a field. For any  $b \neq 0 \in B$ ,  $b^n + a_{n-1}b^{n-1} + \dots + a_0 = 0$  for some  $a_i \in A$ . We may assume that  $a_0 \neq 0 \in A$  because  $B$  is a domain. Then

$$b(b^{n-1} + a_{n-1}b^{n-2} + \dots + a_1) = -a_0.$$

Therefore,  $b$  is invertible in  $B$  and so  $B$  is a field.

Conversely, let  $B$  be a field. For  $a \neq 0 \in A$ ,  $a^{-1} \in B$ . Thus  $(a^{-1})^n + a_{n-1}(a^{-1})^{n-1} + \dots + a_0 = 0$ . In particular,  $a^{-1} = -(a_{n-1} + \dots + a_0 a^{n-1}) \in A$ . □

Let  $A \subset B$  be an integral extension, and  $\mathfrak{q} \in \text{Spec}B$ ,  $\mathfrak{p} \in \text{Spec}A$ . We say that  $\mathfrak{q}$  is lying over  $\mathfrak{p}$  if  $\mathfrak{q} \cap A = \mathfrak{p}$ .

We are going to study the relation between prime ideals of integral extension.

**Proposition 0.8.** *Keep the notation as above with  $\mathfrak{q}$  is lying over  $\mathfrak{p}$ . Then  $\mathfrak{q}$  is maximal if and only if  $\mathfrak{p}$  is maximal.*

*Proof.*  $B/\mathfrak{q}$  is again integral over  $A/\mathfrak{p}$ . Since  $B/\mathfrak{q}$  is a field if and only if  $A/\mathfrak{p}$  is a field, we are done. □

An consequence is the following corollary which assert the "uniqueness in a chain of prime ideal":

**Corollary 0.9.** *Keep the notation as above. If  $\mathfrak{q}_1 \subset \mathfrak{q}_2$  are prime ideals lying over  $\mathfrak{p}$ . Then  $\mathfrak{q}_1 = \mathfrak{q}_2$ .*

*Proof.* Let  $S = A - \mathfrak{p}$ . (Note that  $\mathfrak{q}_i \cap S = \emptyset$  for  $i = 1, 2$ .) Then we have  $B_{\mathfrak{p}}$  integral over  $A_{\mathfrak{p}}$ . Moreover,  $\mathfrak{q}_1 B_{\mathfrak{p}} \subset \mathfrak{q}_2 B_{\mathfrak{p}}$ . Note that  $\mathfrak{q}_i B_{\mathfrak{p}} \cap A_{\mathfrak{p}} = (\mathfrak{q}_i \cap A)A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$  is maximal for  $i = 1, 2$ . Hence both  $\mathfrak{q}_1 B_{\mathfrak{p}} \subset \mathfrak{q}_2 B_{\mathfrak{p}}$  are maximal ideal lying over  $\mathfrak{p}A_{\mathfrak{p}}$ . We then have  $\mathfrak{q}_1 B_{\mathfrak{p}} = \mathfrak{q}_2 B_{\mathfrak{p}}$ . By the correspondence of prime ideals, we have  $\mathfrak{q}_1 \subset \mathfrak{q}_2$ . □

It's also desirable to have existence of prime ideal lying over a specific one.

**Proposition 0.10.** *Let  $A \subset B$  be an integral extension. Let  $\mathfrak{p} \in \text{Spec}(A)$ . Then there exist a  $\mathfrak{q} \in \text{Spec}(B)$  lying over  $\mathfrak{p}$ .*

*Proof.* Let  $S = A - \mathfrak{p}$ . We consider  $A_{\mathfrak{p}} \subset B_{\mathfrak{p}}$ . (This is injective since  $S^{-1}$  is exact.) Take a maximal ideal  $\mathfrak{m}$  of  $B_{\mathfrak{p}}$ . We claim that  $\mathfrak{q} := \mathfrak{m} \cap B$  is a prime ideal lying over  $\mathfrak{p}$ . To see this,

$$\mathfrak{q} \cap A = (\mathfrak{m} \cap B) \cap A = (\mathfrak{m} \cap A_{\mathfrak{p}}) \cap A = \mathfrak{p}A_{\mathfrak{p}} \cap A = \mathfrak{p}.$$

This is because  $\mathfrak{m}$  lying over a maximal ideal of  $A_{\mathfrak{p}}$  and the only maximal ideal of  $A_{\mathfrak{p}}$  is  $\mathfrak{p}A_{\mathfrak{p}}$ . □

**Theorem 0.11** (Going-up theorem). *Let  $B$  be an integral extension over  $A$ . Let  $\mathfrak{p}_1 \subset \mathfrak{p}_2 \in \text{Spec}(A)$  and  $\mathfrak{q}_1 \in \text{Spec}(B)$  lying over  $\mathfrak{p}_1$ . Then there is  $\mathfrak{q}_2 \in \text{Spec}(B)$  containing  $\mathfrak{q}_1$  lying over  $\mathfrak{p}_2$ .*

*Proof.* Let  $\bar{A} := A/\mathfrak{p}_1$  and  $\bar{B} := B/\mathfrak{q}_1$ . Then  $\bar{B}$  is integral over  $\bar{A}$ . There is a prime ideal  $\bar{\mathfrak{q}}_2$  lying over  $\bar{\mathfrak{p}}_2$ . Lift to  $B$ , then we are done.  $\square$

As we have seen, let  $B$  be an integral extension over  $A$ . Then every chain of distinct prime ideals of  $B$  restricts to a chain of distinct prime ideals of  $A$  and conversely, every chain of distinct prime ideals of  $A$  extends to a chain of distinct prime ideals of  $B$ . It follows that

$$\dim A = \dim B.$$

Before we going to dimension theory. We would like to investigate integral extension a little bit more which will be useful in Dedekind domain and DVRs.

Integral extension is very similar to algebraic extension.

**Definition 0.12.** *A domain  $A$  is said to be integrally closed if it is integrally closed in its quotient field.*

For the rest of this section, we are going to assume that  $B$  is a domain integral over  $A$  and  $A$  is integrally closed (i.e. in its quotient field  $K$ ). We remark that this setting is closely related to algebraic field extensions.

**Lemma 0.13.** *Let  $A \subset B$  be an extension and  $C$  is the integral closure of  $A$  in  $B$ . Let  $\mathfrak{a} \triangleleft A$  be an ideal. We say that  $b \in B$  is integral over  $\mathfrak{a}$  if  $b$  satisfies a polynomial with coefficient (except the leading term) in  $\mathfrak{a}$ . Then the integral closure of  $\mathfrak{a}$  in  $B$  is  $\sqrt{\mathfrak{a}C}$ .*

*Proof.* If  $b \in B$  is integral over  $\mathfrak{a}$ , then

$$b^n + a_{n-1}b^{n-1} + \dots + a_0 = 0.$$

Since  $b \in C$ , we have

$$b^n = -a_{n-1}b^{n-1} - \dots - a_0 \in \mathfrak{a}C.$$

Thus  $b \in \sqrt{\mathfrak{a}C}$ .

Conversely, let  $b \in \sqrt{\mathfrak{a}C}$ . Then  $b^n = \sum_{i=1}^r a_i x_i$ , with  $a_i \in \mathfrak{a}, x_i \in C$ . Then  $A[x_1, \dots, x_r]$  is a finite module over  $A$ . Since  $b^n A[x_1, \dots, x_r] \subset \mathfrak{a}A[x_1, \dots, x_r]$ . It follows that the multiplication by  $b^n$  behave like a matrix on  $A[x_1, \dots, x_r]$  with entries in  $\mathfrak{a}$ . Hence  $b^n$  satisfies the characteristic polynomial with coefficient in  $\mathfrak{a}$ . It follows that  $b$  is integral over  $\mathfrak{a}$ .  $\square$

**Remark 0.14.** *Keep the notation as above, let  $f(x)$  be an integral polynomial of  $b \in B$  and  $p(x)$  be its minimal polynomial over  $K$ . We remark that there is NO notion of "minimal integral polynomial" in general because the division algorithm doesn't holds in  $A$ .*

However, if  $A$  is UFD, then by Gauss lemma, we have  $p(x)|f(x)$  not only in  $K[x]$  but also in  $A[x]$ . Hence the minimal polynomial is integral.

**Lemma 0.15.** *Keep the notation as above, the minimal polynomial of  $b \in B$  is in  $A[x]$ . If  $b \in B$  is integral over  $\mathfrak{a} \triangleleft A$ , i.e. the integral polynomial has coefficients in  $\mathfrak{a}$ , then the minimal polynomial of  $b \in B$  is in  $\sqrt{\mathfrak{a}}[x]$ .*

*Proof.* Assume now  $b$  is integral over  $\mathfrak{a}$  with minimal polynomial  $p(x)$ . Take a splitting field of  $p(x)$ , say  $L/K$ . And let  $b = b_1, \dots, b_n$  be conjugates of  $b$ . Then they satisfy  $f(x)$  as well. Thus  $b_i$  is integral over  $\mathfrak{a}$ . It's not difficult to see that  $p(x) = \prod_{i=1}^n (x - b_i)^{m_i}$  for some  $m_i \geq 0$ . The coefficient are combination of  $b_i$  hence integral over  $\mathfrak{a}$ . Apply the above Lemma to the extension  $A \subset K$ , we have integral closure of  $\mathfrak{a}$  is  $\sqrt{\mathfrak{a}}$ . Hence minimal polynomial is in  $\sqrt{\mathfrak{a}}[x]$ .  $\square$

Let  $A$  be an integrally closed domain with quotient field  $K$ . Given an extension  $L/K$ , one can consider  $B$  to be the integral closure of  $A$  in  $L$ . (We may assume that  $L$  is algebraic over  $K$ , or even to be the splitting field of  $B$ .) Especially, in number theory, we usually consider a number field which is a finite extension over  $\mathbb{Q}$ . And let  $\mathcal{O}$  be the domain of algebraic integers. The extension  $\mathbb{Z} \subset \mathcal{O}$  justify our setup.

**Proposition 0.16.** *Let  $A$  be an integrally closed domain with quotient field  $K$ . Given a normal extension  $L/K$ , one can consider  $B$  to be the integral closure of  $A$  in  $L$ . Let  $\mathfrak{p} \in \text{Spec}A$ , then prime ideals in  $B$  lying over  $\mathfrak{p}$  are conjugate. That is, for  $\mathfrak{q}_1, \mathfrak{q}_2 \in \text{Spec}B$  lying over  $\mathfrak{p}$ , there is  $\sigma \in \text{Gal}_K L$  such that  $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$ .*

*Proof.* We will only prove this under the assumption that  $B$  is finitely generated over  $A$ . (Then we may assume that  $[L : K]$  is finite).

If  $\mathfrak{q}_2 \neq \sigma_j(\mathfrak{q}_1)$  for all  $j$  then  $\mathfrak{q}_2 \not\subset \sigma_j(\mathfrak{q}_1)$  for all  $j$ .

**claim.** there is  $x \in \mathfrak{q}_2$  such that  $x \notin \sigma_j(\mathfrak{q}_1)$  for all  $j$ . We leave this claim as an exercise.

Let  $y = \prod_{\sigma_j \in \text{Gal}_K L} \sigma_j(x)$ . Then  $y$  is invariant under  $\text{Gal}_K L$ . We may assume that  $y^{p^l}$  is separable over  $K$  for some  $l \geq 0$ . (If  $\text{char}(K)=0$ , then  $l=0$ .) Let  $S$  be the separable closure of  $K$  in  $L$ . Then  $S$  is Galois over  $K$  with  $\text{Gal}_K S = \text{Gal}_K L$  (cf. Thm. 12 of lecture 1). Hence  $y^{p^l} \in K$ . One notice that  $B \cap K = A$ . It follows that  $y^{p^l} \in A$ . And then  $y \in K$  is integral over  $A$ . Therefore,  $y \in A$ . We Clearly,  $y = x \frac{y}{x} \in \mathfrak{q}_2$ . Hence  $y \in A \cap \mathfrak{q}_2 = \mathfrak{p} \subset \mathfrak{q}_1$ . Hence  $\sigma_j(x) \in \mathfrak{q}_1$  for some  $j$ . This leads to a contradiction.  $\square$

**Corollary 0.17.** *Keep the notation as above. Assume furthermore that  $B$  is finitely generated over  $A$ . Then for  $\mathfrak{p} \in \text{Spec}A$ , there are only finitely many prime ideal in  $B$  lying over  $\mathfrak{p}$ . And any two of them are "conjugate" to each other.*

*Proof.* Let  $L$  be the splitting field of  $B$  over  $K$ . One sees that  $L/K$  is finite. Let  $C$  be the integral closure of  $A$  in  $L$ . Clearly,  $A \subset B \subset C$ . We know that prime ideal in  $C$  lying over  $\mathfrak{p}$  is conjugate to each other. Since the Galois group is finite. There are only finitely many prime ideals. Restrict to  $B$ , then there are only finitely many prime ideals in  $B$  lying over  $\mathfrak{p}$ .  $\square$

**Theorem 0.18** (Going down theorem). *Keep the notation as above, i.e.  $B$  is an domain integral over an integrally closed domain  $A$ . If there are  $\mathfrak{p}_2 \subset \mathfrak{p}_1 \in \text{Spec}A$  and  $\mathfrak{q}_1$  in  $B$  lying over  $\mathfrak{p}_1$ . Then there is  $\mathfrak{q}_2 \subset \mathfrak{q}_1 \in \text{Spec}B$  lying over  $\mathfrak{p}_2$*

*Proof.* Let  $L$  be the normal closure of  $B$  over  $K$  and  $C$  be the integral closure of  $A$  in  $L$ . It's clear that  $C$  is integral over  $B$ . There is a prime ideal  $\mathfrak{r}_1$  in  $C$  lying over  $\mathfrak{q}_1$ . And there is a prime ideal  $\mathfrak{r}_2$  in  $C$  lying over  $\mathfrak{p}_2$ . By Going up theorem, there is a prime ideal  $\mathfrak{r}'_1 \supset \mathfrak{r}_2$  in  $C$  lying over  $\mathfrak{p}_1$ . Therefore, there is  $\sigma \in \text{Gal}_K L$  such that  $\sigma(\mathfrak{r}_1) = \mathfrak{r}'_1$ . Then  $\sigma^{-1}(\mathfrak{r}_2) \subset \mathfrak{r}_1$ . Let  $\mathfrak{q}_2 := \sigma^{-1}(\mathfrak{r}_2) \cap B$ . Then we are done.  $\square$