Commutative Algebra
Chapter 5: Integral Dependence and Valuations

Sichuan University, Fall 2022

Reminder

Let k be a field.

- An element x of some field extension of k is said to be *algebraic over* k if it is the root of some polynomial equation with coefficients in k, i.e.,

$$a_0x^n + a_1x^{n-1} + \cdots + a_n = 0, \qquad a_i \in k,\ a_n \neq 0.$$

- An *algebraic extension* of k is a field extension L of k in which every element is algebraic over k.
- We say that k is *algebraically closed* when the all the roots of every polynomial equation with coefficients in k are in k.
- Every field admits an algebraically closed extension.

Definition

Let $A \subseteq B$ be rings. We say that $x \in B$ is *integral over* A if it solution of a *monic* polynomial equation with coefficients in A, i.e., an equation of the form,

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0, \qquad a_i \in A.$$

Remark

Every $x \in A$ is integral over A.

Integral Dependence

Example

Let $A = \mathbb{Z}$ and $B = \mathbb{Q}$. Then $x \in \mathbb{Q}$ is integral over $\mathbb{Z}$ if and only if $x \in \mathbb{Z}$.

Proof.

- Let $x = p/q$ be integral over $\mathbb{Z}$ with p, q coprime:
$$(p/q)^n + a_1(p/q)^{n-1} + \cdots + a_n = 0, \qquad a_i \in \mathbb{Z}.$$
- Multiplying by q^n gives
$$p^n = -\left(a_1 q + \cdots + a_n q^n\right) = -\left(a_1 + \cdots + a_n q^{n-1}\right) q.$$
Thus, q divides p^n.
- As p and q are coprime this is possible only if $q = 1$, i.e., $x \in \mathbb{Z}$. □

Proposition (Proposition 5.1)

Let $A \subseteq B$ be rings and $x \in B$. TFAE:

(i) *x is integral over A.*

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

(iii) *$A[x]$ is contained in a subring C of B such that C is a finitely generated A-module.*

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

Reminder (Faithful module; see Chapter 2)

A module M over A is *faithful* when its annihilator is zero, i.e., if $a \in A$, then

$$ax = 0 \quad \forall x \in M \implies a = 0.$$

Reminder (Proposition 2.4; Cayley-Hamilton Theorem)

Let M be a finitely generated A-module and $\mathfrak{a}$ and ideal of A. Let $\phi : M \to M$ be an A-module endomorphism such that $\phi(M) \subseteq \mathfrak{a}M$. Then ϕ satisfies an equation of the form,

$$\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0, \qquad a_i \in \mathfrak{a}.$$

Proof of Proposition 5.1.

- If x is integral over A, then $x^n = -(a_1 x^{n-1} + \cdots + a_n)$. Thus,
$$x^{n+r} = -(a_1 x^{n+r-1} + \cdots + a_n x^r) \qquad \forall r \geq 0.$$
- By induction $x^{n+r} \in Ax^{n-1} + \cdots + A$ for all $r \geq 0$, and hence $A[x]$ is generated by $x^{n-1}, \ldots, 1$.
- In particular, $A[x]$ is finitely generated. Thus, (i) implies (ii).
- (ii)$\Rightarrow$ (iii): Take $C = A[x]$.
- (iii)$\Rightarrow$ (iv): Take $M = C$. Here C is a faithful module, since $yC = 0 \Rightarrow y1 = 0 \Rightarrow y = 0$.

$\square$

Proof of Proposition 5.1; Continued.

- Assume (iv). Apply Proposition 2.4 to M and $\mathfrak{a} = A$ and $\phi : M \rightarrow M$ given by the multiplication by x.
- Here $\phi(M) = xM \subseteq M = AM$, and so by Prop. 2.4 there are $a_1, \ldots, a_n \in A$ such that
$$\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0.$$
- That is, $(x^n + a_1x^{n-1} + \cdots + a_n)M = 0$, and hence $x^n + a_1x^{n-1} + \cdots + a_n = 0$, since M is faithful.
- This means that x integral over A, and hence (iv) implies (i).

The proof is complete. $\square$

Reminder (Proposition 2.16)

Let $A \subseteq B$ be rings. If M is a finitely generated B-module and B is finitely generated as an A-module, then M is finitely generated as an A-module.

Corollary (Corollary 5.2)

Let $x_1, \ldots, x_n$ be elements of B that are integral over A. Then the ring $A[x_1, \ldots, x_n]$ is a finitely generated A-module.

Proof.

We proceed by induction on n.

- For $n = 1$ this is is Proposition 5.1(ii) .
- Assume the result is true for $n - 1$. Set $A_r = A[x_1, \ldots, x_r]$.
- By assumption A_{n-1} is finitely generated over A.
- Here x_n is integral over A, and hence is integral over A_{n-1}.
- By Prop. 5.2(ii) $A_n = A_{n-1}[x_n]$ is finitely generated over A_{n-1}.
- By Proposition 2.16 A_n is finitely generated over A.

This gives the result. $\square$

Corollary (Corollary 5.3)

The set of all elements of B that are integral over A forms a sub-ring of B containing A.

Proof.

- Let $x, y \in B$ be integral over A.
- By Corollary 5.2 $A[x, y]$ is finitely generated over A.
- $A[x \pm y]$ and $A[xy]$ are contained in $A[x, y]$.
- Proposition 5.1(iii) then implies that $x \pm y$ and xy are integral over A.

This proves the result. $\square$

Definition (Integral closure)

The sub-ring of elements of B that are integral over A is called the *integral closure of* A in B and is denoted $B * A$ (Gaillard's notation).

Definition

- We say that A is *integrally closed* if $B * A = A$.
- We say that B is *integral over* A if $B * A = B$, i.e., every $x \in B$ is integral over A.

Remark

$B * A$ is integral over A.

Reminder (Finite and finite-type algebras; see Chapter 2)

Let B be an A-algebra.

- We say that the algebra B is *finite* if it is finitely generated as an A-module.
- We say that the algebra B has *finite type* if $B = A[x_1, \ldots, x_n]$ for some $x_i \in B$.

Remark

It follows from Corollary 5.2 that if an A-algebra B has finite type and is integral over A, then B is a finite A-algebra.

Corollary (Corollary 5.4)

Let $A \subseteq B \subseteq C$ be rings such that B is integral over A and C is integral over B. Then C is integral over A.

Proof.

- Let $x \in C$. Then x is integral over B, i.e.,

$$x^n + b_1 x^{n-1} + \cdots + b_n = 0, \qquad b_i \in B.$$

- By Prop. 5.2 $B' = A[b_1, \ldots, b_n]$ is finitely generated over A.
- As x is integral over B', Prop. 5.1 ensures that $B'[x]$ is finitely generated over B'.
- By Prop. 2.16 $B'[x]$ is finitely generated over A.
- By Prop. 5.1(iii) x is integral over A, and hence C is integral of A.

The proof is complete. □

Corollary (Corollary 5.5)

Let $A \subseteq B$ be rings. Then $B * A$ is integrally closed in B.

Proof.

- We have $A \subseteq B * A \subseteq B * (B * A)$.
- Here $B * A$ is integral over A, and $B * (B * A)$ is integral over $B * A$.
- By Corollary 5.4 $B * (B * A)$ is integral over A.
- This means that if $x \in B$ is integral over $B * A$, then x is integral over A, i.e., $x \in B^* A$.
- That is, $B * A$ is integrally closed in B.

The proof is complete. $\square$

Fact

Let $A \subseteq B$ be rings. Let $\mathfrak{b}$ an ideal of B with canonical homomorphism $f : B \to B/\mathfrak{b}$. Set $\mathfrak{a} = \mathfrak{b} \cap A$. Then f induces an exact sequence of A-modules,

$$0 \longrightarrow \mathfrak{a} \longrightarrow A \xrightarrow{f} f(A) \longrightarrow 0.$$

Thus,

$$f(A) \simeq A/\mathfrak{a}$$

Proposition (Proposition 5.6)

Let $A \subseteq B$ be rings such that B is integral over A.

(i) *If $\mathfrak{b}$ is an ideal of B and $\mathfrak{a} = \mathfrak{b}^c = \mathfrak{b} \cap A$, then $B/\mathfrak{b}$ is integral over $A/\mathfrak{a}$.*

(ii) *Let S be a multiplicatively closed subset of A. Then $S^{-1}B$ is integral over $S^{-1}A$.*

Proof of Proposition 5.6.

- Let $x \in B$. As x is integral over A,

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

- Let $\overline{x}$ be the image of x in $B/\mathfrak{b}$. Then:

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

  Thus, $\overline{x}$ is integral over $A/(A \cap \mathfrak{b}) = A/\mathfrak{a}$ (which is identified with the image of A in $B/\mathfrak{b}$).

- Let $s \in S$. Then:

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

  Thus, x/s is integral over $S^{-1}A$.

This gives the result. $\square$

The Going-Up Theorem

Reminder (Integral domains; see Chapter 1)

A ring A is called an *integral domain* if

$$xy = 0 \Longrightarrow x = 0 \text{ or } y = 0.$$

Proposition (Proposition 5.7)

Let $A \subseteq B$ be integral domains such that B is integral over A. Then

$$B \text{ is a field} \iff A \text{ is a field.}$$

Proof of Proposition 5.7.

- Suppose that A is a field. Let $y \in B$, $y \neq 0$. Then:
$$y^n + a_1 y^{n-1} + \cdots + a_n = 0, \qquad a_i \in A.$$
- We may assume the above equation to have minimal degree.
- In this case $a_n \neq 0$. Otherwise we would have
$$0 = y(y^{n-1} + a_1 y^{n-2} + \cdots + a_{n-1}),$$
and hence $y^{n-1} + a_1 y^{n-2} + \cdots + a_{n-1} = 0$, since B is an integral domain. This would contradict the minimality of n.
- As $a_n \neq 0$, it is invertible in A, and we have
$$\begin{aligned} 1 = a_n^{-1} a_n &= -a_n^{-1}(y^n + a_1 y^{n-1} + \cdots + a_{n-1} y) \\ &= -a_n^{-1}(y^{n-1} + a_1 y^{n-2} + \cdots + a_{n-1}) y, \end{aligned}$$
and hence y is invertible in B. Thus, B is a field.

$\square$

Proof of Proposition 5.7; Continued.

- Suppose that B is a field. Let $x \in A$, $x \neq 0$.
- $x^{-1} \in B$ is integral over A, i.e.,
$$x^{-m} + a_1' x^{-m+1} + \cdots + a_m' = 0, \qquad a_i' \in A.$$
- Thus,
$$\begin{aligned} x^{-1} = x^{m-1} x^{-m} &= -x^{m-1}(a_1' x^{-m+1} + \cdots + a_m') \\ &= -(a_1' + \cdots + a_m' x^{m-1}) \in A. \end{aligned}$$
- It follows that A is a field.

The proof is complete. $\square$

Reminder (Prime and maximal ideals; see Chapter 1)

Let $\mathfrak{p}$ be an ideal of a ring A. Then

$$\mathfrak{p} \text{ is prime} \Longleftrightarrow A/\mathfrak{p} \text{ is an integral domain},$$
$$\mathfrak{p} \text{ is maximal} \Longleftrightarrow A/\mathfrak{p} \text{ is a field},$$

Remark (Contractions of ideals; see Chapter 1)

Let $A \subseteq B$ be rings. The inclusion of A into B is a ring homomorphism. Thus, if $\mathfrak{b}$ is an ideal of B, then its contraction in A is $\mathfrak{b}^c = \mathfrak{b} \cap A$.

Corollary (Corollary 5.8)

Let $A \subseteq B$ be rings such that B is integral over A. Let $\mathfrak{q}$ be a prime ideal of B and set $\mathfrak{p} = \mathfrak{q}^c = \mathfrak{q} \cap A$. Then

$$\mathfrak{q} \text{ is maximal} \iff \mathfrak{p} \text{ is maximal.}$$

Proof.

- By Proposition 5.6 $B/\mathfrak{q}$ is integral over $A/\mathfrak{p}$.
- Here $\mathfrak{q}$ and $\mathfrak{p} = \mathfrak{q} \cap A$ are prime ideals, so $B/\mathfrak{q}$ and $A/\mathfrak{p}$ are integral domains.
- By Corollary 5.7 $B/\mathfrak{q}$ is a field if and only if $A/\mathfrak{p}$ is a field.
- That is, $\mathfrak{q}$ is maximal if and only if $\mathfrak{p}$ is maximal.

The result is proved. $\square$

The Going-Up Theorem

Reminder (Rings of fractions; Corollary 3.4 and Proposition 3.11)

Let S be a multiplicatively closed subset of a ring A.

- If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of A, then $S^{-1}(\mathfrak{a} \cap \mathfrak{b}) = S^{-1}(\mathfrak{a}) \cap S^{-1}(\mathfrak{b})$.
- There is a one-to-correspondence ($\mathfrak{p} \leftrightarrow S^{-1}\mathfrak{p}$) between the prime ideals of $S^{-1}A$ and the prime ideals of A that don't meet S.
- In particular, if $\mathfrak{p}$ and $\mathfrak{p}'$ are prime ideals of A that don't meet S, then $S^{-1}\mathfrak{p} = S^{-1}\mathfrak{p}' \Rightarrow \mathfrak{p} = \mathfrak{p}'$.
- If $S = A \setminus \mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of A, then $S^{-1}\mathfrak{p}$ is the maximal ideal of the local ring $A_{\mathfrak{p}} = S^{-1}A$.

Corollary (Corollary 5.9)

Let $A \subseteq B$ be rings such that B is integral over A. Let $\mathfrak{q}$ and $\mathfrak{q}'$ be prime ideals of B such that $\mathfrak{q} \subseteq \mathfrak{q}'$ and $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$. Then $\mathfrak{q} = \mathfrak{q}'$.

Proof of Corollary 5.9.

- By Proposition 5.6 $B_{\mathfrak{p}}$ is integral over $A_{\mathfrak{p}}$.
- Let $\mathfrak{m}$ be the extension of $\mathfrak{p}$ in $A_{\mathfrak{p}}$. This is the unique maximal ideal of the local ring $A_{\mathfrak{p}}$.
- Let $\mathfrak{n}$ and $\mathfrak{n}'$ be the extensions of $\mathfrak{q}$ and $\mathfrak{q}'$ in $B_{\mathfrak{p}}$. Then $\mathfrak{n} \subseteq \mathfrak{n}'$.
- $\mathfrak{n} \cap A_{\mathfrak{p}}$ is the extension of $\mathfrak{q} \cap A = \mathfrak{p}$ in $A_{\mathfrak{p}}$, and hence is equal to $\mathfrak{m}$.
- In particular $\mathfrak{n} \cap A_{\mathfrak{p}}$ is maximal, and hence $\mathfrak{n}$ is maximal by Corollary 5.8.
- Likewise $\mathfrak{n}'$ is maximal. As $\mathfrak{n} \subseteq \mathfrak{n}'$ it follows that $\mathfrak{n} = \mathfrak{n}'$.
- By Proposition 3.11 the contractions in A of $\mathfrak{n}$ and $\mathfrak{n}'$ are $\mathfrak{q}$ and $\mathfrak{q}'$, respectively, so we see that $\mathfrak{q} = \mathfrak{q}'$.

The proof is complete. $\square$

The Going-Up Theorem

Theorem (Theorem 5.10)

Let $A \subseteq B$ be rings such that B is integral over A. Then, for any prime ideal $\mathfrak{p}$ of A, there is a prime ideal $\mathfrak{q}$ of B such that $\mathfrak{q} \cap A = \mathfrak{p}$.

Proof of Theorem 5.10.

- By Proposition 5.6 $B_{\mathfrak{p}}$ is integral over $A_{\mathfrak{p}}$.
- We also have a commutative diagram,

$$\begin{tikzcd} A \arrow[r, hook, "\iota"] \arrow[d, "\alpha"'] & B \arrow[d, "\beta"] \\ A_{\mathfrak{p}} \arrow[r, hook, "\iota_{\mathfrak{p}}"] & B_{\mathfrak{p}} \end{tikzcd}$$

- Let $\mathfrak{n}$ be a maximal ideal of $B_{\mathfrak{p}}$. By Proposition 5.8 $\mathfrak{m} = \mathfrak{n} \cap A_{\mathfrak{p}}$ is maximal.
- Thus, $\mathfrak{m} = \alpha(\mathfrak{p})$, since $\alpha(\mathfrak{p})$ is the unique maximal ideal of $A_{\mathfrak{p}}$. Hence $\mathfrak{p} = \alpha^{-1}(\mathfrak{m})$.
- Set $\mathfrak{q} = \beta^{-1}(\mathfrak{n})$. This is a prime ideal. As the diagram above is commutative, we have

$$\mathfrak{q} \cap A = \iota^{-1}\left(\beta^{-1}(\mathfrak{n})\right) = \alpha^{-1}\left(\iota_{\mathfrak{p}}^{-1}(\mathfrak{n})\right) = \alpha^{-1}(\mathfrak{n} \cap A_{\mathfrak{p}}) = \alpha^{-1}(\mathfrak{m}) = \mathfrak{p}.$$

This proves the result. $\square$

The Going-Up Theorem

Theorem (Going-Up Theorem; Theorem 5.11)

Let $A \subseteq B$ be rings such that B is integral over A. Suppose we are given the following:

- *A chain $\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$ of prime ideals of A.*
- *A chain $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$ of prime ideals of B with $m < n$ such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for $i = 1, \ldots, m$.*

Then the latter chain extends to a chain $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_n$ of ideals of B such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for $i = 1, \ldots, n$.

Proof of Theorem 5.11.

- We may assume $m = 1$. By induction we may further assume that $n = m + 1 = 2$.
- Set $\overline{A} = A/\mathfrak{p}_1$ and $\overline{B} = B/\mathfrak{q}_1$. Then $\overline{A} \subseteq \overline{B}$, and $\overline{B}$ is integral of over $\overline{A}$ by Proposition 5.6.
- Let $\overline{\mathfrak{p}}_2$ be the image of $\mathfrak{p}_2$ in $\overline{A}$. As $\mathfrak{p}_2 \supseteq \mathfrak{p}_1$ this is a prime ideal of $\overline{A}$ by Proposition 1.1*.
- By Theorem 5.10 there is a prime ideal $\overline{\mathfrak{q}}_2$ of $\overline{B}$ such that $\overline{\mathfrak{q}}_2 \cap \overline{A} = \overline{\mathfrak{p}}_2$.
- Let $\mathfrak{q}_2$ be the contraction of $\overline{\mathfrak{q}}_2$ in B. This is a prime of ideal of B containing $\mathfrak{q}_1$ by Proposition 1.1*.
- Moreover,

$$\mathfrak{q}_2 \cap A = (\overline{\mathfrak{q}}_2)^c \cap \overline{A}^c = \left(\overline{\mathfrak{q}}_2 \cap \overline{A}\right)^c = (\overline{\mathfrak{p}}_2)^c = \mathfrak{p}_2.$$

  Thus $\mathfrak{q}_2$ has the required properties.

The proof is complete. $\square$

Reminder (Fraction Field; slides on Chapter 3)

If A is an integral domain, its *field of fraction*, denoted $\operatorname{Frac}(A)$, is $S^{-1}A$ with $S = A \setminus 0$.

Facts

Let A be a integral domain and let $S \subset A \setminus 0$ be multiplicatively closed. Set $K = \mathrm{Frac}(A)$.

(i) $S^{-1}A$ is a subring of K, and hence is an integral domain.

(ii) The natural homomorphism $A \to S^{-1}A$, $a \to a/1$, is injective.

(iii) $\mathrm{Frac}(S^{-1}A) = K$.

Proof.

(i) The homomorphism $S^{-1}A \ni a/s \to a/s \in K$ is injective.

(ii) Follows from (i). It actually holds for any arbitrary ring provided S does not contain any zero-divisor.

(iii) The homomorphism $\mathrm{Frac}(S^{-1}A) \ni (a/s)/(b/t) \to (at)/(bs) \in K$ is injective and surjective, and hence is an isomorphism. □

Integrally Closed Domains. Going-Down Theorem

Proposition (Proposition 5.12)

Let $A \subseteq B$ be rings, A integral domain, and let $S \subseteq A \setminus 0$ be multiplicatively closed. Then $S^{-1}(B * A)$ is the integral closure of $S^{-1}A$ in $S^{-1}B$, i.e.,

$$(S^{-1}B) * (S^{-1}A) = S^{-1}(B * A).$$

Remarks

1. This result holds for arbitrary rings provided S does not contain any zero-divisor.
2. In Atiyah-MacDonald's book this assumption on S is missing. The result fails without it.

Proof of Proposition 5.12.

- As $B * A$ is integral over A, Proposition 5.6(ii) ensures that $S^{-1}(B * A) \subseteq (S^{-1}B) * (S^{-1}A)$.
- Let $b/s \in (S^{-1}B) * (S^{-1}A)$ with $b \in B$ and $s \in S$. Then:

$$(b/s)^n + (a_1/s_1)(b/s)^{n-1} + \cdots + (a_n/s_n) = 0, \quad a_i \in A,\ s_i \in S.$$

- Set $t = s_1 \cdots s_n$. Multiplying by $(st)^n$ gives

$$\begin{aligned} 0 &= (bt)^n/1 + a_1 s(t/s_1)(bt)^{n-1} + \cdots + a_n s^n t^{n-1}(t/s_n) \\ &= \left((bt)^n + a_1'(bt)^{n-1} + \cdots + a_n'\right)/1, \end{aligned}$$

  where we have set $a_i' = a_i s^i t^{i-1} s_1 \cdots s_{i-1} s_{i+1} \cdots s_n \in A$.
- As the homomorphism $a \to a/1$ is injective, this gives $(bt)^n + a_1'(bt)^{n-1} + \cdots + a_n' = 0$, and hence $bt \in B * A$.
- Thus $b/s = (bt)/(ts) \in S^{-1}(B * A)$, and hence $(S^{-1}B) * (S^{-1}A) \subseteq S^{-1}(B * A)$.

This proves the result. □

Definition

A say that an integral domain A is *integrally closed* when it is integrally closed in its fraction ring $\mathrm{Frac}(A)$.

Example

The ring $A = \mathbb{Z}$ is an integral domain with fraction field $\mathbb{Q}$ and it is integrally closed in $\mathbb{Q}$ (see slide 3). Thus, $\mathbb{Z}$ is an integrally closed integral domain.

More generally, any principal domain with the unique factorization property is integrally closed. In particular, we have:

Example

Any polynomial ring $A = k[x_1, \ldots, x_n]$ over a field k is integrally closed.

Reminder (Surjectivity is a local property; Proposition 3.9)

Let $\phi : M \to N$ be an A-module homomorphism between A-modules. Then TFAE:

1. ϕ is surjective.
2. $\phi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is surjective for every prime ideal $\mathfrak{p}$ of A.
3. $\phi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is surjective for every maximal ideal $\mathfrak{m}$ of A.

Integral closedness is a local property:

Proposition (Proposition 5.13)

Let A be an integral domain. Then TFAE:

(i) *A is integrally closed.*

(ii) *$A_{\mathfrak{p}}$ is integrally closed for every prime ideal $\mathfrak{p}$.*

(iii) *$A_{\mathfrak{m}}$ is integrally closed for every maximal ideal $\mathfrak{m}$.*

Proof of Proposition 5.13.

- Set $K = \mathrm{Frac}(A)$. Let $f : A \to K * A$ be the inclusion. Then:

$$(A \text{ integrally closed}) \Longleftrightarrow A = K * A \Longleftrightarrow (f \text{ surjective}).$$

- By the facts on Slide 30 $\mathrm{Frac}(A_{\mathfrak{p}}) = K$.
- If $\mathfrak{p}$ is prime, then by Proposition 5.12 $K * A_{\mathfrak{p}} = K_{\mathfrak{p}} * A_{\mathfrak{p}} = (K * A)_{\mathfrak{p}}$.
- Under these equalities the inclusion of $A_{\mathfrak{p}}$ into $K * A_{\mathfrak{p}}$ is $f_{\mathfrak{p}} : A_{\mathfrak{p}} \to (K * A)_{\mathfrak{p}}$.
- Thus,

$$(A_{\mathfrak{p}} \text{ is integrally closed}) \Longleftrightarrow (f_{\mathfrak{p}} \text{ is surjective}).$$

- Combining this with Proposition 3.9 gives the result.

The proof is complete. □

Definition

Let $A \subseteq B$ be rings and $\mathfrak{a}$ an ideal of A.

- An element $x \in B$ is said to be integral over $\mathfrak{a}$ if it is solution of monic equation with coefficients in $\mathfrak{a}$, i.e.,

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0, \qquad a_i \in \mathfrak{a}.$$

- The set of all such elements is called the *integral closure of* $\mathfrak{a}$ *in* B and is denoted $B * \mathfrak{a}$ (Gaillard's notation).

Remark (Contractions of ideals; see Chapter 1)

Let $A \subseteq B$ be rings. The inclusion of A into B is a ring homomorphism. Therefore:

- If $\mathfrak{a}$ is an ideal of A, then its extension in B is $\mathfrak{a}^e = B\mathfrak{a}$, i.e., it consists all finite sums $\sum b_i a_i$ with $b_i \in B$ and $a_i \in \mathfrak{a}$.
- If $\mathfrak{b}$ is an ideal of B, then its contraction in A is $\mathfrak{b}^c = \mathfrak{b} \cap A$.

Lemma (Lemma 5.14)

Let $A \subseteq B$ be rings and $\mathfrak{a}$ an ideal of A. Then the integral closure of $\mathfrak{a}$ in B is the radical of its extension in $B * A$. That is,

$$B * \mathfrak{a} = r\left((B * A)\mathfrak{a}\right).$$

In particular, $B * \mathfrak{a}$ is an ideal of B.

Proof of Lemma 5.14.

- If $x \in B * \mathfrak{a}$, then $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ with $a_i \in \mathfrak{a}$. In particular, $x \in B * A$.
- Thus, $x^n = -(a_1 x^{n-1} + \cdots + a_n) \in (B * A)\mathfrak{a}$, and hence $x \in r((B * A)\mathfrak{a})$.
- Conversely, let $x \in r((B * A)\mathfrak{a})$. Then $x^n = \sum_{i=1}^m a_i x_i$ with $a_i \in \mathfrak{a}$ and $x_i \in B * A$.
- By Proposition 5.2 $M = A[x_1, \ldots, x_m]$ is a finitely generated A-module. Moreover $x^n M \subseteq \mathfrak{a} M$.
- Let $\phi : M \to M$ be the multiplication by x^n. As $\phi(M) \subseteq \mathfrak{a} M$, by the Cayley-Hamilton theorem (Proposition 2.4),
$$\phi^p + a_1 \phi^{p-1} + \cdots + a_p = 0, \qquad a_i \in \mathfrak{a}.$$
- Evaluating at 1 gives $x^{pn} + a_1 x^{n(p-1)} + \cdots + a_n = 0$, and hence $x \in B * \mathfrak{a}$.

This proves the result. □

Proposition (Proposition 5.15)

Let $A \subseteq B$ be integral domains such that A is integrally closed. Let $x \in B$ be integral over an ideal $\mathfrak{a}$ of A. Then:

1. *x is algebraic over the fraction field $K = \mathrm{Frac}(A)$.*
2. *Let $\mu(t) = t^n + a_1 t^{n-1} + \cdots + a_n$ be the minimal polynomial of x over K. Then all the coefficients $a_1, \ldots, a_n$ lie in $r(\mathfrak{a})$.*

Reminder (Contracted ideals; see Proposition 1.17(iii))

Let $f : A \rightarrow B$ be a ring homomorphism.

- An ideal $\mathfrak{a}$ of A is a the contraction of an ideal of B if and only if $\mathfrak{a}^{ec} = \mathfrak{a}$.
- In particular, if $A \subseteq B$ and f is the inclusion map, then the above condition amounts to

$$(B\mathfrak{a}) \cap A = \mathfrak{a}.$$

Reminder (Corollary 3.13)

Let A be a ring and $\mathfrak{p}$ a prime ideal. Then we have a one-to-one correspondence between prime ideals of $A_{\mathfrak{p}}$ and prime ideals of A contained in $\mathfrak{p}$.

Integrally Closed Domains. Going-Down Theorem

Theorem (Going-Down Theorem; Theorem 5.16)

Let $A \subseteq B$ be integral domains such that A is integrally closed and B is integral over A, i.e., $K * A = A$ and $B * A = B$, where $K = \mathrm{Frac}(A)$. Assume we are given the following:

- *A chain $\mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$ of prime ideals of A.*
- *A chain $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$ of prime ideals of B with $m < n$ such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for $i = 1, \ldots, m$.*

Then the latter chain extends to a chain $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_n$ of ideals of B such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for $i = 1, \ldots, n$.

Valuation Rings

Definition

We say that a ring B is a *valuation ring* of a field K if K contains B as a sub-ring and

$$x \in K \setminus 0 \implies x \in B \text{ or } x^{-1} \in B.$$

Remarks

1. Any sub-ring of a field is automatically an integral domain, and so any valuation ring is an integral domain.
2. If B is a valuation ring for a field K, then K is the fraction field of B. (An isomorphism from $\mathrm{Frac}(B)$ to K is $x/y \to xy^{-1}$.)

Valuation Rings

Reminder (Characterization of local rings; see Proposition 1.6(i))

Let A be a ring and $\mathfrak{m}$ a proper ideal that contains all non-units of A. Then $\mathfrak{m}$ is the unique maximal ideal of A, and hence A is a local ring.

Proposition (Proposition 5.18)

Let B a valuation ring in a field K.

(i) *B is a local ring.*

(ii) *Any sub-ring of K containing B is a valuation ring of K.*

(iii) *B is integrally closed in K.*

Proof of Proposition 5.18(i).

- Let $\mathfrak{m}$ be the set of non-units of B. Thus, if $x \in B$, then

$$x \in \mathfrak{m} \Longleftrightarrow \left(x = 0 \quad \text{or} \quad x^{-1} \notin B\right).$$

- If $a \in B$ and $x \in \mathfrak{m}$, then $ax \in \mathfrak{m}$. Otherwise, $(ax)^{-1} \in B$ and $x^{-1} = a(ax)^{-1} \in B$ (not possible).
- Let $x, y \in \mathfrak{m} \setminus 0$. Then $xy^{-1} \in B$ or $yx^{-1} \in B$.
- If $xy^{-1} \in B$, then $x + y = (1 + xy^{-1})y \in \mathfrak{m}$.
- Likewise, if $yx^{-1} \in B$, then $x + y \in \mathfrak{m}$.
- This shows that $\mathfrak{m}$ is an ideal of B.
- As $\mathfrak{m}$ contains all the non-units of B, Proposition 1.6(i) ensures that $\mathfrak{m}$ is the unique maximal ideal of B, and hence B is a local ring. $\square$

Proof of Proposition 5.18(iii).

- Let $x \in K * B$. Then:
$$x^n + b_1 x^{n-1} + \cdots + b_n = 0, \qquad b_i \in B.$$
- Suppose that $x \notin B$. Then $x^{-1} \in B$, and hence
$$\begin{aligned} x = x^{-n+1} x^n &= -x^{-n+1}\left(b_1 x^{n-1} + \cdots + b_n\right) \\ &= -b_1 - b_2 x^{-1} - \cdots - b_n (x^{-1})^{n-1} \in B. \end{aligned}$$
  This is a contradiction, so $x \in B$, and hence $K * B = B$.
- That is, B is integrally closed in K.

The proof is complete. $\square$

Valuation Rings

Facts

Let K be a field and Ω an algebraically closed field.

- Define Σ to be the set of pairs (A, f), where A is a sub-ring of K and $f : A \to \Omega$ is a ring homomorphism.
- Σ is a partially ordered set:

$$(A, f) \leq (A', f') \iff A \subseteq A' \text{ and } f'_{|A} = f.$$

- By Zorn's lemma Σ admits a maximal element.

Theorem (Theorem 5.21; see Atiyah-MacDonald)

If (B, g) is a maximal element of Σ, then the ring B is a valuation ring of K.

Corollary

Let A be a sub-ring of a field K and $f : A \to \Omega$ a ring homomorphism, where Ω is an algebraically closed field. Then f can be extended to a ring homomorphism $g : B \to \Omega$, where B is a valuation ring B for K.

Corollary (Corollary 5.22)

Let A be a sub-ring of a field K. Then the integral closure $K * A$ is the intersections of all the valuation rings of K that contain A.

Proof.

- If $B \supseteq A$ is a valuation ring for K, then by Proposition 5.18 B is integrally closed in K, and hence $B = K * B \supseteq K * A$.
- Conversely, let $x \notin K * A$. Then x is not in the ring $A' = A[x^{-1}]$. Otherwise $x = a_0 + \cdots + a_n x^{-n}$, $a_i \in A$. Thus,
$$x^{n+1} - (a_0 x^n + \cdots a_n) = 0,$$
and hence $x \in K * A$ (not possible).
- In particular, x^{-1} is a unit of A', and so there is a maximal ideal $\mathfrak{m}'$ of A' containing x^{-1}.

□

Proof of Corollary 5.22; Continued.

- Let Ω be the algebraic closure of the field $k' = A'/\mathfrak{m}'$ and $f : A' \to k' \subseteq \Omega$ the canonical homorphism.
- By Theorem 5.21 f can be extended to a ring homomorphism $g : B \to \Omega$, where B is a valuation ring of K.
- Here $x^{-1} \in A' \subseteq B$. If $x \in B$, then x^{-1} is a unit of B, and so $g(x^{-1})$ is a unit of Ω, i.e., $g(x^{-1}) \neq 0$.
- However, as $x^{-1} \in \mathfrak{m}' \subseteq A'$, we have $g(x^{-1}) = f(x^{-1}) = 0$ (contradiction). Thus, $x \notin B$.
- By contraposition, if x is contained in all the valuation rings containing A, then $x \in K * A$.

The proof is complete. $\square$

Proposition (Proposition 5.23)

Let $A \subseteq B$ be integral domains such that B is finitely generated over A. Let $v \in B \setminus 0$. Then there is $u \in A \setminus 0$ with the following property: any homomorphism f of A into an algebraically closed field Ω such that $f(u) \neq 0$ extends to a homomorphism $g : B \to \Omega$ such that $g(v) \neq 0$.

Corollary (Corollary 5.24)

Let k be a field and B a finitely generated k-algebra. If B is a field, then it is a finite algebraic extension of k.

Remark

Let Ω be the algebraic closure of k.

- A field L/k is an algebraic extension if and only if L embeds into Ω.
- A homomorphism $g : L \to \Omega$ is injective if and only if $g(1) \neq 0$ (since $x \neq 0$ and $g(x) = 0$ implies $g(1) = g(x)g(x^{-1}) = 0$).
- Thus, L/k is an algebraic extension if and only if there is a homomorphism $g : L \to \Omega$ such that $g(1) \neq 0$.

Proof of Corollary 5.24.

- Apply Proposition 5.23 to $v = 1$ and the inclusion $f : k \hookrightarrow \Omega$.
- We get a homomorphism $g : B \to \Omega$ such that $g(1) \neq 0$.
- By the previous remark B/k is an algebraic extension.

The result is proved. $\square$

Corollary (Weak Nullstellensatz; Corollary 7.10)

Let k be a field, A a finitely generated k-algebra, and $\mathfrak{m}$ a maximal ideal of A. Then the field $A/\mathfrak{m}$ is a finite algebraic extension of k. In particular, if k is algebraically closed, then $A/\mathfrak{m} \simeq k$.

Proof.

- As A is a finitely generated k-algebra, so is $A/\mathfrak{m}$.
- Corollary 5.24 then ensures that $A/\mathfrak{m}$ is a finite algebraic extension of k.

The result is proved. $\square$