1 Some commutative algebra

1.1 Integral ring extensions

All rings are assumed to be commutative and unitary. Consider a ring extension $A \subset B$.

Definition 1.1.1:

(a) An element $b \in B$ is called *integral over A* if there exists a monic $f \in A[X]$ with $f(b) = 0$.

(b) The ring B is called *integral over A* if every $b \in B$ is integral over A.

(c) The *integral closure of A in B* is the set $\tilde{A} := \{b \in B \mid b \text{ integral over } A\}$.

Definition-Example 1.1.2:

(a) An element $z \in \mathbb{C}$ is integral over $\mathbb{Q}$ if and only if z is an *algebraic number*.

(b) An element $z \in \mathbb{C}$ is integral over $\mathbb{Z}$ if and only if z is an *algebraic integer*.

Proposition 1.1.3: The following statements for an element $b \in B$ are equivalent:

(a) b is integral over A.

(b) The subring $A[b] \subset B$ is finitely generated as an A-module.

(c) b is contained in a subring of B which is finitely generated as an A-module.

Proof: (a) $\Rightarrow$ (b): Say $b^n + a_1 b^{n-1} + \ldots + a_n = 0$ with $a_i \in A$.

$\Rightarrow \forall m \geq n$: $b^m + a_1 b^{m-1} + \ldots + a_n b^{m-n} = 0$

Induction on $m \Rightarrow$ Each $b^m \in A b^{n-1} + \ldots + A$ $\Rightarrow A[b]$ gen. by $1, b, \ldots, b^{n-1}$.

(b) $\Rightarrow$ (c): $b \in A[b]$.

(c) $\Rightarrow$ (a): Say $b \in A'$ gen. by $b_1', \ldots, b_n'$ as A-module.

Write $b b_i' = \sum_{j=1}^n a_{ij} b_j'$ with $a_{ij} \in A$.

$M := (b \cdot \delta_{ij} - a_{ij})_{i,j}$ $\Rightarrow M \cdot \begin{pmatrix} b_1' \\ \vdots \\ b_n' \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$.

$\tilde{M}$:= adjunct of M $\Rightarrow \det(M) \cdot \begin{pmatrix} b_1' \\ \vdots \\ b_n' \end{pmatrix} = \tilde{M} \cdot M \cdot \begin{pmatrix} b_1' \\ \vdots \\ b_n' \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$

$\Rightarrow \det(M) \cdot 1 = 0$; $M = b \cdot \mathrm{Id}_n - N$

$\left.\begin{array}{l} \Rightarrow 0 = \det(M) = \det(b \cdot I_n - N) = \mathrm{char}_N(b) \\ \mathrm{char}_N(X) \in A[X] \text{ monic} \end{array}\right\} \Rightarrow$ (a).

q.e.d.

Proposition 1.1.4: (a) For any integral ring extensions $A \subset B$ and $B \subset C$ the ring extension $A \subset C$ is integral.

(b) The subset $\tilde{A}$ is a subring of B that contains A.

(c) The subring $\tilde{A}$ is its own integral closure in B.

Proof: (a) $\forall c \in C$: Choose $b_i \in B$ with $c^n + b_1 c^{n-1} + \ldots + b_n = 0$.

$\Rightarrow$ each $A[b_i]$ is fin. gen. as A-module, say by $1, b_i, \ldots, b_i^N$

$\Rightarrow$ $A[b_1, \ldots, b_n]$ - - - - - - - - - - - - by $\prod_{i=1} b_i^{\nu_i}$ with $\nu_i \leq N$.

$\Rightarrow$ $A[b_1, \ldots, b_n, c]$ - - - - - - - - - - - - these and c^μ for $\mu < n$.

$\Rightarrow$ c integral over A.

(b) $\forall a \in A$: $f(a) = 0$ for $f(X) = X - a \in A[X]$ $\Rightarrow$ $a \in \tilde{A}$.

$\Rightarrow$ $1 \in \tilde{A}$, $\forall b, b' \in \tilde{A}$: $A[b, b']$ fin. gen. as A-module

$b + b'$, $b \cdot b'$ $\Rightarrow$ $b + b'$, $b \cdot b' \in \tilde{A}$.

(c) If $b \in B$ is integral over $\tilde{A}$, with $b^n + \tilde{a}_1 b^{n-1} + \ldots + \tilde{a}_n = 0$ with $\tilde{a}_i \in \tilde{A}$.

$\Rightarrow$ $A[\tilde{a}_1, \ldots, \tilde{a}_n]$ fin. gen. as A-module

$\Rightarrow$ $A[\tilde{a}_1, \ldots, \tilde{a}_n, b]$ - - - - - - - - .

$\Rightarrow$ b integral over A $\Rightarrow$ $b \in \tilde{A}$.

qed.

1.2 Prime ideals

Consider an integral ring extension $A \subset B$.

Proposition 1.2.1: For every prime ideal $\mathfrak{q} \subset B$ the intersection $\mathfrak{q} \cap A$ is a prime ideal of A.

Proof: $A/\mathfrak{q}\cap A \hookrightarrow B/\mathfrak{q}$ = integral domain.

$\Rightarrow$ integral domain. qed

$$\begin{array}{ccc} \mathfrak{q} & \subset & B \\ | & & | \\ \mathfrak{q}\cap A = \mathfrak{p} & \subset & A \end{array}$$

Definition 1.2.2: We say that $\mathfrak{q}$ *lies over* $\mathfrak{q} \cap A$.

Theorem 1.2.3: For any prime ideals $\mathfrak{q} \subset \mathfrak{q}' \subset B$ $\underbrace{\text{over the same } \mathfrak{p}}_{}$ we have $\mathfrak{q} = \mathfrak{q}'$.

$\mathfrak{q}\cap A = \mathfrak{q}'\cap A$ $\Updownarrow$

Proof: Suppose $\mathfrak{q} \neq \mathfrak{q}'$. Pick $b \in \mathfrak{q}' \setminus \mathfrak{q}$. $\Rightarrow \exists f \in A[X]$ monic with $f(b) = 0$. In particular there exists $f \in A[X]$ monic with $f(b) \in \mathfrak{q}$. Among all these choose one with $\deg(f)$ minimal. $\Rightarrow$ $f(b) = \underbrace{b^n + a_1 b^{n-1} + \dots + a_{n-1} \cdot b}_{\in \mathfrak{q}'} + \underbrace{a_n}_{} \in \mathfrak{q} \subset \mathfrak{q}'$.

$\Rightarrow a_n \in \mathfrak{q}'$. $\Rightarrow a_n \in \mathfrak{q}' \cap A = \mathfrak{q} \cap A \Rightarrow a_n \in \mathfrak{q}$.

$\Rightarrow \underbrace{b}_{\notin \mathfrak{q}} \cdot \underbrace{(b^{n-1} + a_1 b^{n-2} + \dots + a_{n-1})}_{} \in \mathfrak{q}$.

$\mathfrak{q}$ prime $\Rightarrow$ $\in \mathfrak{q}$ $\Rightarrow$ contradiction to the minimality of $\deg(f)$.

qed.

Theorem 1.2.4: For every prime ideal $\underline{\mathfrak{p} \subset A}$ there exists a prime ideal $\underline{\mathfrak{q} \subset B}$ over $\mathfrak{p}$.

$\Updownarrow$

$\mathfrak{q} \cap A = \mathfrak{p}$.

Proof: $\mathfrak{p}$ prime $\Rightarrow A \setminus \mathfrak{p}$ multiplicative

$0 \in \mathfrak{p} \Rightarrow 0 \notin A \setminus \mathfrak{p}$.

Let $\mathcal{I}$ be the set of all ideals $\mathfrak{b} < B$

with $\mathfrak{b} \cap (A \setminus \mathfrak{p}) = \emptyset$.

$\Leftrightarrow \underline{\mathfrak{b} \cap A < \mathfrak{p}}$.

Lemma: $\mathcal{I}$ possesses a max. element,

and every such element is prime.

Proof: $(0) \in \mathcal{I}$. For any chain $\emptyset \neq \mathcal{K} \subset \mathcal{I}$

take $\mathfrak{b} := \bigcup \mathcal{K}$. $\Rightarrow \mathfrak{b} < B$ ideal in $\mathcal{I}$.

Zorn's lemma $\Rightarrow \mathcal{I}$ possesses a max. element $\mathfrak{q}$.

If $1 \in \mathfrak{q}$ then $1 \in \mathfrak{p} \Rightarrow$ Contradiction $\Rightarrow \mathfrak{q} \neq B$.

Take $b, b' \in B \setminus \mathfrak{q}$ such that $\underline{bb' \in \mathfrak{q}}$.

Then $\mathfrak{q} + (b) \supsetneq \mathfrak{q} \overset{\text{max.}}{\Longrightarrow} \mathfrak{q} + (b) \notin \mathcal{I}$. $\Rightarrow \exists\, q \in \mathfrak{q}\ \exists\, y \in B: q + by = a \in A \setminus \mathfrak{p}$.

and - - - - - - - - - - - - $\exists\, q' \in \mathfrak{q}\ \exists\, y' \in B: q' + b'y' = a' \in A \setminus \mathfrak{p}$.

$\Rightarrow (q+by)(q'+b'y') = aa' \in A \setminus \mathfrak{p}$.

$qq' + qb'y' + byq' + bb'yy'$ <- - - all summands in $\mathfrak{q}$. $\Rightarrow aa' \in \mathfrak{q}$.

$\Rightarrow a' \in (A \setminus \mathfrak{p}) \cap \mathfrak{q} = \emptyset$ because $\mathfrak{q} \in \mathcal{J}$. $\Rightarrow$ Contradiction! qed.

~~**Theorem 1.2.4:** For every prime ideal $\mathfrak{p} \subset A$ there exists a prime ideal $\mathfrak{q} \subset B$ over $\mathfrak{p}$.~~

Take $\mathfrak{q} \in \mathcal{J}$ maximal $\Rightarrow \mathfrak{q} \subset B$ prime.

Suppose $\mathfrak{q} \cap A \subsetneq \mathfrak{p}$. Take $b \in \mathfrak{p} \setminus \mathfrak{q}$. $\Rightarrow \mathfrak{q} + (b) \supsetneq \mathfrak{q}$

$\Rightarrow (\mathfrak{q} + (b)) \cap (A \setminus \mathfrak{p}) \neq \emptyset$. Choose $a \in (A \setminus \mathfrak{p}) \cap (\mathfrak{q} + (b))$

$a = q + bc$ with $q \in \mathfrak{q}$, $c \in B$.

$\Rightarrow c$ integral over A. With $c^n + a_1 c^{n-1} + \dots + a_n = 0$ with $a_i \in A$.

$$\Rightarrow (bc)^n + a_1 b (bc)^{n-1} + \dots + b^n a_n = 0.$$

$$\Rightarrow (a-q)^n + a_1 b (a-q)^{n-1} + \dots + b^n a_n = 0.$$

Note $q \in \mathfrak{q}$, $a, a_i, b \in A$

$$\Rightarrow \underbrace{a^n + a_1 b a^{n-1} + \dots + b^n a_n}_{\text{all terms } \in A} \in \mathfrak{q}.$$

$$\in \mathfrak{q} \cap A \subset \mathfrak{p}.$$

$b \in \mathfrak{p}$. $\Rightarrow a^n \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$. Contradiction!

$\Rightarrow \mathfrak{q} \cap A = \mathfrak{p}$. qed.

See Hungerford: Algebra.

1.4 Localization

Definition 1.4.1: A subset $S \subset A \smallsetminus \{0\}$ is called *multiplicative* if it contains 1 and is closed under multiplication.

Definition-Proposition 1.4.2: For any multiplicative subset $S \subset A$ the subset

$$\boxed{S^{-1}A := \left\{\tfrac{a}{s} \,\middle|\, a \in A,\ s \in S\right\}}$$

is a subring of K that contains A and is called the *localization of A with respect to S.*

Example 1.4.3: For every prime ideal $\mathfrak{p} \subset A$ the subset $A \smallsetminus \mathfrak{p}$ is multiplicative. The ring $A_{\mathfrak{p}} := (A \smallsetminus \mathfrak{p})^{-1}A$ is called the *localization of A at $\mathfrak{p}$*.

$\mathfrak{p} \neq A \Rightarrow 1 \in A \smallsetminus \mathfrak{p}$.

$\forall a, b \in A \smallsetminus \mathfrak{p} : ab \notin \mathfrak{p} \Rightarrow ab \in A \smallsetminus \mathfrak{p}$.

Proposition 1.4.4: For every multiplicative subset $S \subset A$ we have:

(a) $S^{-1}\tilde{A} = \widetilde{S^{-1}A}$.

(b) If A is normal, then so is $S^{-1}A$.