Going-up and going-down theorem

陳宗震

June 2021

In this report, every ring is commutative.

0 Introduction and motivation

Since I haven't studied algebraic geometry, I can't realize the meaning of integral in algebraic geometry. Let's see how it is introduced in Atiyah-MacDonald.

> In classical algebraic geometry curves were frequently studied by projecting them onto a line and regarding the curve as a (ramified) covering of the line. This is quite analogous to the relationship between a number field and the rational field-or rather between their rings of integers-and the common algebraic feature is the notion of integral dependence.

In the first half of this report, we will focus on the property of integral extension and derive the going up and going down theorem. In the second half, we will give some application for integral and going up, going down theorem. Which includes Noether's normalization lemma and Zariski's lemma, and our ultimate goal is Hilbert's nullstellensatz.

1 Extension and contraction

Before going to introduce the concept of integral, let’ s first introduce a concept that we will often use later. Given a ring homomorphism $f : A \to B$. Notice that if $\mathfrak{a}$ is the ideal of A, then $f(\mathfrak{a})$ may not be the ideal of B. For example, $f : \mathbb{Z} \hookrightarrow \mathbb{Q}$ by $z \mapsto z/1$. Then $f(2\mathbb{Z})$ is not an ideal in $\mathbb{Q}$, since the only ideal in $\mathbb{Q}$ are 0 and $\mathbb{Q}$. But we can check that if $\mathfrak{b}$ is the ideal of B, then $f^{-1}(\mathfrak{b})$ is the ideal of A.

Definition 1.1. Let $f : A \to B$ be a ring homomorphism, $\mathfrak{a}, \mathfrak{b}$ be the ideal of A, B respectively. Define

- the **extension** $\mathfrak{a}^e$ of $\mathfrak{a}$ is the ideal $Bf(\mathfrak{a})$ which is generated by $f(\mathfrak{a})$ in B i.e.

$$\mathfrak{a}^e = \{\sum_{\text{finite}} b_i f(a_i) : a_i \in \mathfrak{a}, b_i \in B\}$$

- the **contraction** $\mathfrak{b}^c$ of $\mathfrak{b}$ is the ideal $f^{-1}(\mathfrak{b})$ i.e.

$$\mathfrak{b}^c = \{a \in A : f(a) \in \mathfrak{b}\}$$

Property 1.1.

- $\mathfrak{b} \in \operatorname{Spec} B \implies \mathfrak{b}^c \in \operatorname{Spec} A$. Conversely, $\mathfrak{a} \in \operatorname{Spec} A$ will not implies $\mathfrak{a}^e \in \operatorname{Spec} B$.
- $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$, $\mathfrak{b}^{ce} \subseteq \mathfrak{b}$
- $\mathfrak{a}^e = \mathfrak{a}^{ece}$, $\mathfrak{b}^c = \mathfrak{b}^{cec}$
- $(\mathfrak{a}_1 + \mathfrak{a}_2)^e = \mathfrak{a}_1^e + \mathfrak{a}_2^e$, $(\mathfrak{b}_1 + \mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c + \mathfrak{b}_2^c$
- $(\mathfrak{a}_1 \cap \mathfrak{a}_2)^e \subseteq \mathfrak{a}_1^e \cap \mathfrak{a}_2^e$, $(\mathfrak{b}_1 \cap \mathfrak{b}_2)^c = \mathfrak{b}_1^c \cap \mathfrak{b}_2^c$

Proof: By definition. □

Recall. Let $\rho : R \to S^{-1}R,\ x \mapsto \frac{x}{1}$ is natural canonical map

$$\begin{array}{ccc} \operatorname{Spec} S^{-1}R & \longleftrightarrow & \{\mathfrak{p} \in \operatorname{Spec} R : \mathfrak{p} \cap S = \varnothing\} \\ \mathfrak{q} & \longmapsto & \rho^{-1}(\mathfrak{q}) \\ S^{-1}\mathfrak{p} & \longleftarrow\!\shortmid & \mathfrak{p} \end{array}$$

So $\forall \mathfrak{p} \in \operatorname{Spec} R$ with $\mathfrak{p} \cap S = \varnothing$, $\mathfrak{p}^{ec} = \mathfrak{p}$.
If $\mathfrak{p}, \mathfrak{q} \in \operatorname{Spec} R$ and $\mathfrak{p} \cap S = \mathfrak{q} \cap S = \varnothing$, then $S^{-1}\mathfrak{p} = S^{-1}\mathfrak{q} \iff \mathfrak{p} = \mathfrak{q}$

Theorem 1.1. Let $A \to B$ be a ring homomorphism and let $\mathfrak{p} \in \operatorname{Spec} A$. Then $\mathfrak{p}$ is the contraction of a prime ideal of $B \iff \mathfrak{p}^{ec} = \mathfrak{p}$.

Proof:

- $(\Rightarrow)$: If $\mathfrak{p} = \mathfrak{q}^c$ for some $\mathfrak{q} \in \operatorname{Spec} B$. Then $\mathfrak{p}^{ec} = \mathfrak{q}^{cec} = \mathfrak{q}^c = \mathfrak{p}$.
- $(\Leftarrow)$: Let $S = f(A - \mathfrak{p})$ which is multiplicative closed subset of B. If $f(a) \in \mathfrak{p}^e \cap S$, then $a \in \mathfrak{p}^{ec} = \mathfrak{p}$, but $a \in A - \mathfrak{p}$ $(\to\leftarrow)$. So $\mathfrak{p}^e \cap S = \varnothing$ and thus the extension of $\mathfrak{p}^e$ in $S^{-1}B$ is a proper ideal $\mathfrak{n}$ in $S^{-1}B$. Say $\mathfrak{n} \subseteq \mathfrak{m}$ for some $\mathfrak{m} \in \operatorname{Max} S^{-1}B$. Let $\mathfrak{q}$ be the contraction of $\mathfrak{m}$ in B, then $\mathfrak{q} \in \operatorname{Spec} B$ and $\mathfrak{p}^e \subseteq \mathfrak{q}$. Notice that $\mathfrak{q} \cap S = \varnothing$ (otherwise $\mathfrak{m} = S^{-1}B$), then $\mathfrak{q}^c \cap (A - \mathfrak{p}) = \varnothing$. Combine with $\mathfrak{q}^c \supseteq \mathfrak{p}^{ec} = \mathfrak{p}$, we have $\mathfrak{q}^c = \mathfrak{p}$.

□

2 Integral dependence

Definition 2.1. Let B be a ring and A is a subring of A. We say $x \in B$ is **integral** over A if

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

for some $a_i \in A$.

Example 2.1. $\mathbb{Z} \subseteq \mathbb{Q}$, if $t = r/s \in \mathbb{Q}$ is integral over $\mathbb{Z}$ with $\gcd(r, s) = 1$, then

$$\left(\frac{r}{s}\right)^n + a_1 \left(\frac{r}{s}\right)^{n-1} + \cdots + a_n = 0 \text{ with } a_i \in \mathbb{Z}$$

Multiply s^n in both side we have $s | r^n \implies s | 1$ i.e. $t \in \mathbb{Z}$.

Similar to algebraic over a field, we have some equivalent statement for integral and property similar to algebraic. But before the equivalent, we see the important lemma first.

Lemma 2.1. M : finitely generated A-module, $\mathfrak{a}$ be an ideal of A, $\phi \in \mathrm{End}_A(M)$ such that $\phi(M) \subseteq \mathfrak{a}M$. Then ϕ satisfies

$$\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0 \text{ for some } a_i \in \mathfrak{a}$$

Proof: Let $M = \langle x_1, ..., x_n \rangle_A$ and for all i, say $\phi(x_i) = \sum_{j=1}^{n} a_{ij}x_j$ for $a_{ij} \in \mathfrak{a}$. Then

$$\underbrace{\begin{pmatrix} \phi - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & \phi - a_{22} & & \\ \vdots & & \ddots & \\ -a_{n1} & & & \phi - a_{nn} \end{pmatrix}}_{:=N} \underbrace{\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}}_{:=\mathbf{x}} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Then $0 = \mathrm{adj}(N)N\mathbf{x} = \det(N)\mathbf{x} \implies \det(N)$ annihilates $x_1, ..., x_n$ i.e $\det N$ is zero endomorphism. Then $\det N = 0$ is polynomial of ϕ with coefficient in $\mathfrak{a}$ which is what we want. □

Proposition 2.1. TFAE

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

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

(3) $A[x]$ is containing in a subring C of B which is finitely generating A-module

(4) exists a faithful $A[x]$-module M is finite generated A-module

Proof:

- (1) ⇒ (2) : If x is a root of monic polynomial $f(t) \in A[t]$ with degree n, then $A[x] = \langle 1, x, ..., x^{n-1} \rangle_A$ which is finitely generated A-module.
- (2) ⇒ (3) : Choose $C = A[x]$.
- (3) ⇒ (4) : Choose $M = C$. If $y \in \mathrm{Ann}_{A[x]}(C)$, then $y \cdot 1 = 0$. Hence, C is faithful $A[x]$-module.
- (4) ⇒ (1) : Since $xM \subseteq M$. By Lemma 2.1 ($\phi : m \mapsto xm$ and $\mathfrak{a} = A$),

  $$f(\phi) = \phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$$

  for some $a_i \in A$. Then $f(x)M = f(\phi)M = 0$. Since M is faithful $A[x]$-module, $f(x) = 0$ i.e. x is integral over A.

□

Corollary 2.1. Let $x_1, ..., x_n \in B$ such that x_i is integral over A for all $i = 1, ..., n$. Then $A[x_1, ..., x_n]$ is finitely generated A-module.

Proof: By induction on n. Using Proposition 2.1 and the fact that x_i is integral over $A[x_1, ..., x_{i-1}]$. □

Corollary 2.2. Let $C = \{x \in B : x \text{ is integral over } A\}$ is a subring of B containing A.

Proof: If $x, y \in C$, then by Corollary 2.1, $A[x, y]$ is finitely generating A-module. Notice that $A[x \pm y], A[xy] \subseteq A[x, y] \subseteq B$, by Proposition 2.1, $x \pm y$, xy are integral over A. Clearly every element of A is integral over A. □

Definition 2.2.

- C in Corollary 2.2 is called the **integral closure** of A in B.
- If $C = A$, then we say A is **integrally closed** in B.
- If $C = B$, then we say B is **integral** over A.

Example 2.2. The integral closure of $\mathbb{Z}$ in $\mathbb{Q}[\sqrt{5}]$ is $\mathbb{Q}[\frac{1+\sqrt{5}}{2}]$:
If $z = a + b\sqrt{5}$ is integral over $\mathbb{Z}$, let $f(x) \in \mathbb{Z}[x]$ be the monic polynomial s.t. $f(z) = 0$. Notice that $(x - a)^2 - 5b^2 \in \mathbb{Q}[x]$ has root z. View f as the polynomial with coefficient Q, then $f(x) = ((x - a)^2 - 5b^2)g(x)$ for some monic polynomial g in $Q[x]$. By Guass lemma, f is reducible in $Z[x]$. So exists $c \in C$ s.t. $c((x - a)^2 - 5b^2), g(x)/c \in \mathbb{Z}[x]$. Consider the leading coefficient of two polynomial, $c = \pm 1$ i.e. $(x - a)^2 - 5b^2 \in \mathbb{Z}[x]$. Hence, $2a \in \mathbb{Z}$ and $a^2 - 5b^2 \in \mathbb{Z}$. Say $a = m/2$, $b = p/q$ with $\gcd(p, q) = 1$ and $q \in \mathbb{N}$.

$$a^2 - 5b^2 \in \mathbb{Z} \implies \frac{m^2q^2 - 20p^2}{4q^2} \in \mathbb{Z} \implies q^2 | 20p^2 \implies q|2$$

- If $q = 1$, then $a^2 \in \mathbb{Z} \implies a \in \mathbb{Z}$. Hence, $(x - a)^2 - 5b^2 \in \mathbb{Z}[x]$ has root z. And
$$a + b\sqrt{5} = (a + b)\frac{1 + \sqrt{5}}{2} + (a - b)\frac{2}{1 + \sqrt{5}} \in \mathbb{Q}\left(\frac{1 + \sqrt{5}}{2}\right) = \mathbb{Q}\left[\frac{1 + \sqrt{5}}{2}\right]$$
- If $q = 2$, say $a^2 - 5b^2 = k$ i.e. $m^2 - 5p^2 = 4k$. Then we can check that $m + p, m - p \in 2\mathbb{Z}$ and
$$a + b\sqrt{5} = \left(\frac{m + p}{2}\right)\frac{1 + \sqrt{5}}{2} + \left(\frac{m - p}{2}\right)\frac{2}{1 + \sqrt{5}} \in \mathbb{Q}\left(\frac{1 + \sqrt{5}}{2}\right) = \mathbb{Q}\left[\frac{1 + \sqrt{5}}{2}\right]$$

Remark 2.1. Let $f : A \to B$ be the ring homomorphism, so that B is A-algebra. Then f is said to be **integral**, and B is said to be an **integral** A-algebra, if B is integral over $f(A)$. We say f is **finite type** if B is finitely generated A-algebra and f is **finite** if B is finitely generated A-module. So finite type + integral = finite.

Property 2.1. If $A \subseteq B \subseteq C$ are rings. B is integral over A and C is integral over B $\iff$ C is integral over A.

Proof:

- $(\Leftarrow)$: Trivial.
- $(\Rightarrow)$: For all $x \in C$, since x integral over B, say

$$x^n + b_1x^{n-1} + \cdots + b_n = 0 \text{ with } b_i \in B$$

Let $B' = A[b_1, ..., b_n]$ which is f.g. A-module, since b_i are integral over A. Since x is integral over B', $B'[x]$ is f.g B'-module. Hence, $B'[x]$ is f.g. A-module containing $A[x]$ and $B'[x] \subseteq C$. By Proposition 2.1, x is integral over A.

□

Property 2.2. Let $A \subseteq B$ are rings and C is integral closure of A in B. Then C is integrally closed in B.

Proof: If $x \in B$ is integral over C. By Property 2.1, x is integral over $A \implies x \in C$. □

Proposition 2.2. Let $A \subseteq B$ are rings and B is integral over A.

- If $\mathfrak{b}$ is an ideal of B and $\mathfrak{a} = \mathfrak{b}^c$ (i.e. $\mathfrak{a} = \mathfrak{b} \cap A$). Then $B/\mathfrak{b}$ is integral over $A/\mathfrak{a}$. (Note: $A/\mathfrak{a} = A/(A \cap \mathfrak{b}) \simeq (A + \mathfrak{b})/\mathfrak{b} \subseteq B/\mathfrak{b}$)
- If S is multiplicative closed subset of A, then $S^{-1}B$ is integral over $S^{-1}A$.

Proof:

- For all $x \in B$, say

$$x^n + a_1x^{n-1} + \cdots + a_n = 0 \text{ with } a_i \in A$$

Reduce the equation by mod $\mathfrak{b}$. Then $\overline{x}$ is integral over $(A + \mathfrak{b})/b \simeq A/\mathfrak{a}$.

- For all $x/s \in S^{-1}B$, then

$$\left(\frac{x}{s}\right)^{n-1} + \frac{a_1}{s}\left(\frac{x}{s}\right)^{n-1} + \cdots + \frac{a_n}{s^n} = 0$$

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

□

3 Going up theorem

Motivation: Given a ring extension $A \subseteq B$, we know if $\mathfrak{q} \in \operatorname{Spec} B$, then $\mathfrak{q} \cap A \in \operatorname{Spec} A$. So we have a map $\operatorname{Spec} B \to \operatorname{Spec} A$. Now, you may ask, will this map is surjuctive? The answer is no. But if we require for some property, then it may holds.

Proposition 3.1. Let $A \subseteq B$ be integral domains and B is integral over A. Then A is a field $\iff$ B is a field.

Proof:

- For all $0 \neq x \in B$, since x integral over A, choose the monic polynomial with smallest degree $n \geq 1$ such that exists $a_1, ..., a_n \in A$ s.t.

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

  Then $a_n \neq 0$, otherwise by B is integral domain, $x^{n-1} + a_1x^{n-2} + \cdots + a_{n-1} = 0$ contradict with the definition of n. So

  $$x^{-1} = a_n^{-1}(x^{n-1} + \cdots + a_2x + a_1) \in B$$

  i.e. B is a field.

- For all $0 \neq x \in A \subseteq B$, $x^{-1} \in B$, say

  $$x^{-m} + a_1x^{-m+1} + \cdots + a_m = 0 \text{ for some } m \geq 1$$

  Then $1 = x(-a_mx^{m-1} - \cdots - a_1) \implies x^{-1} = -(a_mx^{m-1} + \cdots + a_1) \in A$ i.e. A is a field.

□

Corollary 3.1. Let $A \subseteq B$ be rings and B is integral over A, $\mathfrak{q} \in \operatorname{Spec} B$ and $\mathfrak{p} = \mathfrak{q} \cap A$. Then $\mathfrak{p} \in \operatorname{Max} A \iff \mathfrak{q} \in \operatorname{Max} B$.

Proof: By Proposition 2.2, $B/\mathfrak{q}$ is integral over $A/\mathfrak{p}$ and $A/\mathfrak{p}$, $B/\mathfrak{q}$ are all integral domain. By Proposition 3.1, $B/\mathfrak{q}$ is a field $\iff$ $A/\mathfrak{p}$ is a field. Hence, $\mathfrak{q} \in \operatorname{Max} B \iff \mathfrak{p} \in \operatorname{Max} A$. □

Corollary 3.2. Let $A \subseteq B$ and B is integral over A, let $\mathfrak{q}, \mathfrak{q}' \in \operatorname{Spec} B$ such that $\mathfrak{q} \subseteq \mathfrak{q}'$ and $\mathfrak{q}^c = \mathfrak{q}'^c = \mathfrak{p}$. Then $\mathfrak{q} = \mathfrak{q}'$.

Proof: By Proposition 2.2, $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$. Let $\mathfrak{m} = \mathfrak{p}_\mathfrak{p}$ be the extension of $\mathfrak{p}$ and $\mathfrak{n}, \mathfrak{n}'$ is the extension of $\mathfrak{q}, \mathfrak{q}'$ in $B_\mathfrak{p}$ $\implies$ $\mathfrak{n}^c = \mathfrak{n}'^c = \mathfrak{m}$ and $\mathfrak{n} \subseteq \mathfrak{n}'$. Since $\mathfrak{m}$ is maximal in $A_\mathfrak{p}$, by Corollary 3.1, $\mathfrak{n}$ and $\mathfrak{n}'$ are maximal in $B_\mathfrak{p}$ $\implies$ $\mathfrak{n} = \mathfrak{n}'$ and thus $\mathfrak{q} = \mathfrak{q}'$ □

Theorem 3.1. Let $A \subseteq B$ be rings and B is integral over A, $\mathfrak{p} \in \operatorname{Spec} A$, then $\exists \mathfrak{q} \in \operatorname{Spec} B$ such that $\mathfrak{q} \cap A = \mathfrak{p}$.

Proof: By Proposition 2.2, $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$ and the diagram commute.

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

Let $\mathfrak{m}$ be the maximal ideal in $B_{\mathfrak{p}}$, then the contraction of $\mathfrak{m}$ in $A_{\mathfrak{p}}$ is also maximal. Notice that $(A_{\mathfrak{p}}, \mathfrak{p}_{\mathfrak{p}})$ is local ring, so $\mathfrak{m} \cap A_{\mathfrak{p}} = \mathfrak{p}_{\mathfrak{p}}$. Let $\mathfrak{q} = \beta^{-1}(\mathfrak{m})$, then $\mathfrak{q} \in \operatorname{Spec} B$ and $\mathfrak{m} = \mathfrak{q}_{\mathfrak{p}}, \mathfrak{q} \cap (A - \mathfrak{p}) = \varnothing \implies \mathfrak{p}_{\mathfrak{p}} = \mathfrak{q}_{\mathfrak{p}} \cap A_{\mathfrak{p}} = (\mathfrak{q} \cap A)_{\mathfrak{p}}$. Since $\mathfrak{q} \cap A, \mathfrak{p} \in \operatorname{Spec} A$ and $(\mathfrak{q} \cap A) \cap (A - \mathfrak{p}), \mathfrak{p} \cap (A - \mathfrak{p}) = \varnothing \implies \mathfrak{p} = \mathfrak{q} \cap A$. □

Theorem 3.2. [Going-up theorem] Let $A \subseteq B$ be rings and B integral over A. Let $\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$ be a chain of prime ideals of A and $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$ $(m < n)$ be a chain of primes ideals of B such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for $1 \leq i \leq m$. Then we can extended $\{\mathfrak{q}_i\}_{i=1}^{m}$ to $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_n$ such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for $1 \leq i \leq n$.

Proof: By induction, we only need to do the case for $m = 1$ and $n = 2$. By Proposition 2.2, $B/\mathfrak{q}_1$ is integral over $A/\mathfrak{p}_1$. By Theorem 3.1, $\exists \overline{q}_2 \in \operatorname{Spec} B/\mathfrak{q}_1$ s.t. $\overline{q}_2 \cap A/\mathfrak{p}_1 = \mathfrak{p}_2/\mathfrak{p}_1$. Lift back $\overline{q}_2$ to B, we get a prime ideal $\mathfrak{q}_2$ in B s.t. $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$ and $\mathfrak{q}_2 \supseteq \mathfrak{q}_1$. □

4 Integrally closed integral domains and going down theorem

First, we can do more in Property 2.2 :

Property 4.1. Let $A \subseteq B$ be rings and C is integral closure of A in B, S is multiplicative closed subset of A. Then $S^{-1}C$ is integral closure of $S^{-1}A$ in $S^{-1}B$.

Proof: Since C is integral over A, by Proposition 2.2, $S^{-1}C$ is integral over $S^{-1}A$. If $x/s \in S^{-1}B$ is integral over $S^{-1}A$, say

$$(x/s)^n + (a_1/s_1)(x/s)^{n-1} + \cdots + (a_n/s_n) = 0$$

for some $a_i \in A, s_i \in S$. Let $t = s_1 s_2 \cdots s_n \in S$ and rewrite as

$$\frac{tx^n + a_1' x^{n-1} + \cdots + a_n'}{ts^n} = 0 \text{ in } S^{-1}A$$

Then exists $u \in S$ such that $utx^n + ua_1' x^{n-1} + \cdots + ta_n' = 0$. Multiply $(ut)^{n-1}$, then it becomes an equation of integral dependence for utx over A i.e. $utx \in C$. Then $x/s = (utx)/(uts) \in S^{-1}C$. □

Definition 4.1. An integral domain is said to be **integrally closed** if it is integrally closed in its field of fractions.
(Note : Since A is integral domain, $A \setminus \{0\}$ is multiplicative closed set and thus field of fractions exists.)

Example 4.1. As we discuss in Example 2.1, every UFD is integrally closed. In particular, if k is a field. By Gauss lemma $k[x_1, ..., x_n]$ is UFD and thus is integrally closed.

Proposition 4.1. (local property) Let A be an integral domain. TFAE

(1) A is integrally closed

(2) $A_{\mathfrak{p}}$ is integrally closed $\forall \mathfrak{p} \in \operatorname{Spec} A$

(3) $A_{\mathfrak{m}}$ is integrally closed $\forall \mathfrak{m} \in \operatorname{Max} A$

Proof: Let C be the integral closure of A in field of fraction of A and $f : A \to C$ be inclusion. A is integrally closed $\iff$ f is surjective $\iff$ $f_{\mathfrak{p}}$ (resp. $f_{\mathfrak{m}}$) is surjective $\forall \mathfrak{p} \in \operatorname{Spec} A$ (resp. $\forall \mathfrak{m} \in \operatorname{Max} A$) $\iff$ $A_{\mathfrak{p}}$ (resp. $A_{\mathfrak{m}}$) is integrally closed $\forall \mathfrak{p} \in \operatorname{Spec} A$ (resp. $\forall \mathfrak{m} \in \operatorname{Max} A$). □

Now, we generalize the definition of integral.

Definition 4.2. Let $A \subseteq B$ be rings and let $\mathfrak{a}$ be an ideal of A. $x \in B$ is said to be **integral** over $\mathfrak{a}$ if

$$x^n + a_1 x^{n-1} + \cdots + a_n x^n = 0 \text{ for some } a_i \in \mathfrak{a}$$

The **integral closure** of $\mathfrak{a}$ in B is

$$\{b \in B : b \text{ is integral over } \mathfrak{a}\}$$

Lemma 4.1. Let C be the integral closure of A in B and let a^e denote the extension of $\mathfrak{a}$ in C. Then the integral closure of $\mathfrak{a}$ in B is the radical of $\mathfrak{a}^e$. Therefore, $\mathfrak{a}$ is closed under addition and multiplication.

Proof: If $x \in B$ is integral over $\mathfrak{a}$, say

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0 \text{ for some } a_i \in \mathfrak{a}$$

Then $x^n \in \mathfrak{a}^e$ i.e. $x \in \sqrt{\mathfrak{a}^e}$. Conversely, if $x \in \sqrt{\mathfrak{a}^e}$, say $x^n = \sum\limits_{i=1}^{m} a_i x_i$ for some $n > 0$, $a_i \in \mathfrak{a}$ and $x_i \in C$. Since x_i are integral over A, by Corollary 2.1, $M = A[x_1, ..., x_m]$ is f.g. A-module. Then we have $x^n M \subseteq \mathfrak{a} M$. By Lemma 2.1 and $1 \in M$, x^n is integral over $\mathfrak{a}$ and thus x is integral over $\mathfrak{a}$. □

Proposition 4.2. Let $A \subseteq B$ be integral domains and A integrally closed. Let $x \in B$ is integral over an ideal $\mathfrak{a}$ of A. Then x is algebraic over the field of fraction K of A, and the minimal polynomial of x over K is form

$$t^n + a_1 t^{n-1} + \cdots + a_n$$

with $a_1, ..., a_n \in \sqrt{\mathfrak{a}}$ in K.

Proof: It's clear that x algebraic over K. Let monic polynomial $f(t) \in A[t]$ s.t. $f(x) = 0$ and $\overline{f}(t) \in K[x]$ with is f with coefficient in K. Let $x_1, ..., x_n$ be all roots of $m_{x,K}(t)$. Since $m_{x,K}(t) | \overline{f}(t)$, $\overline{f}(x_i) = 0$ for all i. Then exists $u_i \in A \setminus \{0\}$ such that $u_i f(x_i) = 0$. Since A is domain, $f(x_i) = 0$ i.e. x_i integral over $\mathfrak{a}$. Notice that the coefficient a_i of $m_{x,K}$ is symmetric polynomial of $x_1, ..., x_n$ which is also integral over A and $a_i \in K$. By A is integrally closed and Lemma 4.1 ($C = A$, $\mathfrak{a}^e = \mathfrak{a}$), $a_i \in \sqrt{\mathfrak{a}}$ w.r.t. K. □

Theorem 4.1. [Going-down theorem] Let $A \subseteq B$ be integral domains and A integrally closed, B integral over A. Let $\mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$ be chain of primes ideals of A, and let $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$ $(m < n)$ be chain of prime ideals of B such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ $(1 \leq i \leq m)$. Then the chain $\{\mathfrak{q}_i\}_{i=1}^m$ can be extended to a chain $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_n$ such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for $1 \leq i \leq n$.

Proof: By induction, we only need to prove the case for $m = 1$ and $n = 2$. Consider $A \to B \to B_{\mathfrak{q}_1}$, if we find a prime ideal $(\mathfrak{q}_2)_{\mathfrak{q}_1}$ in $B_{\mathfrak{q}_1}$ such that the contraction of $(\mathfrak{q}_2)_{\mathfrak{q}_1}$ is $\mathfrak{p}_2$. Then $\mathfrak{q}_2 \subseteq \mathfrak{q}_1$ and $\mathfrak{q}_2$ is contraction of $(\mathfrak{q}_2)_{\mathfrak{q}_1}$ in B, $\mathfrak{q}_2 \cap A$ is contraction of $\mathfrak{q}_2$ in $A \implies \mathfrak{q}_2 \cap A = \mathfrak{p}_2$ and thus $\mathfrak{q}_2$ as required. By Theorem 1.1, it is suffices to show that $\mathfrak{p}_2^{ec} = \mathfrak{p}_2$ i.e. $B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A = \mathfrak{p}_2$.

- For all $y/s \in B_{\mathfrak{q}_1}\mathfrak{p}_2$ with $y \in B\mathfrak{p}_2$ and $s \in B \backslash \mathfrak{q}_1$. Since $y \in B\mathfrak{p}_2 = \mathfrak{p}_2^e \subseteq \sqrt{\mathfrak{p}_2^e}$ (where extension w.r.t. B) and by Lemma 4.1, y is integral over $\mathfrak{p}_2$. By Proposition 4.2, the minimal polynomial of y is form

$$t^n + u_1 t^{n-1} + \cdots + u_n$$

  with $a_i \in \sqrt{\mathfrak{p}_2} = \mathfrak{p}_2$ (since $\mathfrak{p}_2$ is primes ideal).

- If $x \in B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A$, write $x = y/s$ and thus $sx = y$ (by B is integral domain). Rewrite $s = yx^{-1}$ with $x^{-1} \in K$. Then the minimal polynomial of s over K is

$$t^n + \frac{u_1}{x}t^{n-1} + \cdots + \frac{u_n}{x^n} \tag{1}$$

  Let $v_i = u_i/x^i$, then $x^i v_i = u_i \in \mathfrak{p}_2$. Since $s \in B$ is integral over A. By Proposition 4.2, $v_i \in \sqrt{A} = A$. Suppose that $x \notin \mathfrak{p}_2$, then $v_i \in \mathfrak{p}_2$ $\forall i = 1, ..., n$. By (2), $s^n \in B\mathfrak{p}_2 \subseteq B\mathfrak{p}_1 \subseteq \mathfrak{q}_1 \implies s \in \mathfrak{q}_1$ which is contradict to $s \in B \setminus \mathfrak{q}_1 s$. Hence, $x \in \mathfrak{p}_2$ and thus $B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A = \mathfrak{p}_2$ as required.

□

Proposition 4.3. Let A be an integrally closed domain and K is field of fraction. Let L/K : Galois, B is the integral closure of A in L. Then there exists a basis $v_1, ..., v_n$ of L over K such that $B \subseteq \sum\limits_{j=1}^{n} Av_j$.

Proof:

- For all $v \in L$ which is algebraic over K, then it must satisfy the condition form

$$a_0 v^r + a_1 v^{r-1} + \cdots + a_n = 0 \text{ for some } a_i \in A$$

  Multiply a_0^{r-1}, then $a_0 v$ is integral over A. Thus, given basis $\{v_1, ..., v_n\}$ for L over K, there exists a_i s.t. $u_i := a_i v_i \in B$

- Let T denote the trace form L to K. Since L/K is separable, the bilinear form $(x, y) \mapsto T(xy)$ is nondegenerate, and thus we have the dual basis $w_1, ..., w_n$ define by $T(w_i u_j) = \delta_{ij}$. Given $x \in B$, say $x = \sum\limits_{j=1}^{n} x_j v_j$ for some $x_j \in K$. Then $xu_i \in B$

(since $u_i \in B$). By Proposition 4.2, $T(xu_i) \in A$ since the trace of element y is the coefficient of $x^{\deg m_{y,K}-1}$ in $m_{y,K}$and multiply (-1). Combine with

$$T(xu_i) = \sum_{j=1}^{n} T(x_i u_i v_j) = \sum_{j=1}^{n} x_j T(u_i v_j) = \sum_{j=1}^{n} x_j \delta_{ij} = x_i$$

we have $x_i \in A$. Hence, $B \subseteq \sum\limits_{j=1}^{n} A v_j$.

□

5 Application

In this section, we will prove based on what we have learned above. Ultimately we will derive Hilbert's nullstellensatz theorem from these.

5.1 Krull dimension & Noether's normalization lemma

Definition 5.1. Let A be a ring. Define **Krull dimension** of A to be the supremum of the lengths of all chains of prime ideals in A and denoted by $\dim A$. We allow $\dim A = \infty$.

Example 5.1.

- If k is a field, them $\dim k = 0$.
- If A is a PID and not a field, then $\dim A = 1$.

  Since if $I \neq 0$, then $I \in \operatorname{Spec} A \iff I \in \operatorname{Max} A$.
- If A is Noetherian, then $\dim A[x] = \dim A + 1$.

  In particular, if k is a field, then $\dim k[x_1, ..., x_n] = n$.
- Notice that every proper ideal in nontrivial ring A will contain in a maximal ideal, so $\dim A = 0 \iff \operatorname{Max} A = \operatorname{Spec} A$. Hence, A : Artinian $\iff$ A : Noetherian $+ \dim A = 0$.

Property 5.1. If $A \subseteq B$ be rings and B is integral over A, then $\dim A = \dim B$.

Proof: By Corollary 3.2 and going-up theorem. □

Theorem 5.1 (Noether's normalization lemma). Let k be a field and let $A \neq 0$ be a finitely generated k-algebra. Then there exists $y_1, ..., y_r \in A$ which are algebraically independent over k and such that A is integral over $k[y_1, ..., y_r]$.

Proof: We induct on the number of generators m of A over k. If $m = 0$ i.e. $A = k$, then done! If $m > 0$, let $x_1, ..., x_m$ be the generators of A over k. If $x_1, ..., x_m$ are algebraically independent over k. Since A is integral over $A = k[x_1, ..., x_m]$, and done! Otherwise, there exists $f \in k[t_1, ..., t_m]$ such that

$$f(x_1, ..., x_m) = 0$$

Let $r > \deg f$ and $z_1 = x_1$, $z_i = x_i - x_1^{r^{i-1}}$ for all $i = 2, ..., m$. Notice that $z_1, ..., z_m$ also generators of A over k and satisfies

$$f(x_1, z_2 + x_1^r, ..., z_m + x_1^{r^{m-1}}) = 0. \tag{1}$$

Since $r > \deg f$, there exists unique term $\prod_{i=1}^{m} t_i^{\alpha_i}$ in $f(t_1, ..., t_m)$ has maximum of $\sum_{i=1}^{m} \alpha_i r^{i-1}$ among all terms in f. So, after expand (1), it is the polynomial of x_1 with coefficient in $k[z_2, ..., z_m]$ and leading coefficient in k. Hence, x_1 is integral over $k[z_2, ..., z_m]$. Since $z_2, ..., z_m$ also integral over $k[z_2, ..., z_m]$, A is integral over $k[z_2, ..., z_m]$. By induction hypothesis, $k[z_2, ..., z_m]$ integral over $k[y_1, ..., y_r]$ for some $y_1, ..., y_r \in A$ are algebraically independent over k. Hence, A integral over $k[y_1, ..., y_r]$ as required. □

Corollary 5.1 (Zariski's lemma)**.** Let k be a field and K is finitely generated k-algebra. Suppose that K is a field, then K/k is finite extension.

Proof: By Noether's normalization lemma, K is integral over $k[y_1, ..., y_r]$ for some $y_1, ..., y_r \in B$ are algebraically independent over k. Since K is a field, $\dim K = 0$. By Property 5.1, $\dim k[y_1, ..., y_r] = 0$. Since $y_1, ..., y_r$ are algebraically independent, $\dim k[y_1, ..., y_r] = r \implies r = 0$. Hence, K is integral over k and thus K/k is finite extension. □

5.2 Hilbert's nullstellensatz

Definition 5.2. Let k be an algebraically closed field, $A = k[t_1, ..., t_n]$ be the polynomial ring and S is a subset of A. Define **zero locus** of S be the set

$$Z(S) = \{x \in k^n : f(x) = 0 \ \forall f \in S\}$$

If a subset $X \subseteq k^n$ has the form $V = Z(S)$ for some S, then X is called **affine algebraic variety**. Define **ideal of variety** X by

$$I(X) = \{g(x) \in k[t_1, ..., t_n] : g(\mathbf{x}) = 0 \ \forall \mathbf{x} \in X\}$$

Theorem 5.2. [weak Hilbert's nullstellensatz] Let k be the algebraically closed field and $\mathfrak{a}$ be the ideal in the polynomial ring $A = k[x_1, ..., x_n]$. Then $\mathfrak{a} \neq A \iff Z(\mathfrak{a}) \neq \varnothing$.

Proof: Let $\mathfrak{a} \subsetneq k[x_1, ..., x_n]$ and $\mathfrak{a}$ contains in $\mathfrak{m} \in \operatorname{Max} A$. Then $A/\mathfrak{m}$ is a field with generator $\bar{t}_1, ..., \bar{t}_n$ as k-algebra. By Zariski's lemma, $A/\mathfrak{m}$ is finite extension of k i.e.

$k \subseteq A/\mathfrak{m} \subseteq \overline{k} = k$. Hence, $A/\mathfrak{m} \simeq k$ as k-algebra. Consider $\varphi : A/\mathfrak{m} \xrightarrow{\sim} k$ and let $a_i = \varphi(\overline{t}_i)$, then for all $f \in \mathfrak{m}$ we have

$$f(a_1, ..., a_n) = f(\varphi(\overline{t}_1), ..., \varphi(\overline{t}_n)) = \varphi(f(\overline{t}_1, ..., \overline{t}_n)) = 0$$

i.e. $(a_1, ..., a_n) \in Z(\mathfrak{m}) \subseteq Z(\mathfrak{a})$. If $\mathfrak{a} = A$, then consider the root of x_1 and $x_1 + 1 \implies Z(\mathfrak{a}) = \varnothing$. □

Corollary 5.2. Let k be algebraic closed field, then every maximal ideal in $k[x_1, ..., x_n]$ is form $\mathfrak{m} = (x_1 - a_1, ..., x_n - a_n)$.

Proof: For all $a = (a_1, ..., a_n) \in F^n$, consider the evaluation map

$$\begin{array}{rccc} ev_a : & k[x_1, x_2, ..., x_n] & \longrightarrow & k \\ & f(x_1, ..., x_n) & \longmapsto & f(a) \end{array}$$

is k-algebra epimorphism and let $\mathfrak{m}_a = \ker ev_a$. Then $k[x_1, ..., x_n]/\mathfrak{m}_a \simeq k \implies \mathfrak{m}_a$ is maximal. Conversely, $\forall \mathfrak{m} \in \operatorname{Max} k[x_1, ..., x_n]$. Let $\varphi : A/\mathfrak{m} \to k$ and $a = (a_1, ..., a_n)$ defined in Theorem 5.2. Then $\forall f \in \mathfrak{m}_a$,

$$\varphi(\overline{f}(x_1, ..., x_n)) = f(a_1, ..., a_n) = 0 \implies \overline{f}(x_1, ..., x_n) = 0 \text{ in } k[x_1, ..., x_n]/\mathfrak{m}$$

Hence, $\mathfrak{m}_a \subseteq \mathfrak{m}$. Since $\mathfrak{m}_a$ is maximal and $\mathfrak{m} \neq k[x_1, ..., x_n]$, $\mathfrak{m} = \mathfrak{m}_a$ as required. □

Lemma 5.1. Let k be a field, B be a finitely generated k-algebra and $\mathfrak{b}$ be an ideal in B. Then

$$\sqrt{\mathfrak{b}} = \bigcap_{\mathfrak{b} \subseteq \mathfrak{m} \in \operatorname{Max} B} \mathfrak{m}$$

Proof: Notice that

$$\left(\bigcap_{\mathfrak{b} \subseteq \mathfrak{m} \in \operatorname{Max} B} \mathfrak{m} \right) \Big/ \mathfrak{b} = \bigcap_{\mathfrak{m} \subseteq \mathfrak{m} \in \operatorname{Max} B} \mathfrak{m}/\mathfrak{b} = \bigcap_{\mathfrak{m}/\mathfrak{b} \in \operatorname{Max} B/\mathfrak{b}} \mathfrak{m}/\mathfrak{b}$$

and

$$\left(\bigcap_{\mathfrak{b} \subseteq \mathfrak{m} \in \operatorname{Spec} B} \mathfrak{m} \right) \Big/ \mathfrak{b} = \bigcap_{\mathfrak{m} \subseteq \mathfrak{m} \in \operatorname{Spec} B} \mathfrak{m}/\mathfrak{b} = \bigcap_{\mathfrak{m}/\mathfrak{b} \in \operatorname{Spec} B/\mathfrak{b}} \mathfrak{m}/\mathfrak{b}$$

So we only need to proof the cases for $b = 0$ i.e. nilradical of B equal to Jacobson radical of B. Let $f \in B$ s.t. $f \notin \sqrt{0}$. Let $S = \{f^n : n \in \mathbb{Z}_{\geq 0}\}$ which is multiplicative closed set in B and $S^{-1}B$ is a non-trivial k-algebra, hence it has a maximal ideal $\mathfrak{m}$. Consider $\phi : B \to S^{-1}B$. Since B is f.g k-algebra, the field $S^{-1}B/\mathfrak{m}$ is also f.g. k-algebra. By Zariski's lemma, $S^{-1}B/\mathfrak{m}$ is a finite extension over k and notice that $k \subseteq B/\phi^{-1}(\mathfrak{m}) \subseteq S^{-1}B/\mathfrak{m} \implies B/\phi^{-1}(\mathfrak{m})$ is integral over k. Since $\phi^{-1}(\mathfrak{m}) \in \operatorname{Spec} B \implies B/\phi^{-1}(\mathfrak{m})$ is integral domain. By Proposition 3.1, k is a field $\implies B/\phi^{-1}(\mathfrak{m})$ is a also a field i.e. $\phi^{-1}(\mathfrak{m}) \in \operatorname{Max} B$. Notice that if $f \in \phi^{-1}(\mathfrak{m})$, then $f/1 \in \mathfrak{m}$ and thus $1 = 1/f \cdot f/1 \in \mathfrak{m}$ $(\rightarrow\leftarrow)$. Hence, $f \notin \phi^{-1}(\mathfrak{m}) \in \operatorname{Max} B$ i.e. $f \notin J_B$. Which means $\mathfrak{N}_B = J_B$. □

Theorem 5.3 (Hilbert's nullstellensatz)**.** Let k be an algebraically closed field, A be the polynomial ring $A = k[t_1, ..., t_n]$ and $\mathfrak{a}$ be an ideal of A. Then

$$I(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}}$$

Proof: We continue to use the notation in above. Observe that if $a \in Z(\mathfrak{a}) \iff \mathfrak{a} \subseteq \mathfrak{m}_a$ and $f \in I(V) \iff f(a) = 0 \ \forall a \in V \iff f \in \bigcap\limits_{a\in V} \mathfrak{m}_a$. Hence,

$$I(Z(\mathfrak{a})) = \bigcap_{a\in Z\mathfrak{a}} \mathfrak{m}_a = \bigcap_{\mathfrak{a}\subseteq\mathfrak{m}_a} \mathfrak{m}_a$$

By Corollary 5.2, every maximal ideal in A is form $\mathfrak{m}_a$ for some $a \in k^n$. Hence,

$$\bigcap_{\mathfrak{a}\subseteq\mathfrak{m}_a} \mathfrak{m}_a = \bigcap_{\mathfrak{a}\subseteq\mathfrak{m}} \mathfrak{m} = \sqrt{\mathfrak{a}} \qquad \text{(By Lemma 5.1)}$$

□

5.3 Extend the ring homomorphism when integral

Recall that we learn in field theory. Let $\sigma : F \to L$ is homomorphism and $F(\alpha)/F$ is algebraic. Then $\exists \tau : F(\alpha) \to L$ s.t. $\sigma|_F = f \iff m^{\sigma}_{\alpha,F}(\beta) = 0$ for some $\beta \in L$. Then we have similar property for integral extension.

Theorem 5.4. Let A be a subring of a ring B such that B is integral over A, and let $f : A \mapsto \Omega$ be a homomorphism of A into an algebraically closed field Ω. Show that f can be extended to a homomorphism of B into Ω.

Proof:

- Notice that Ω is integral domain, so 0 is prime ideal and thus $\ker f = f^{-1}(0)$ is also prime ideal in A. By Theorem 3.1, there exists $\mathfrak{q} \in \operatorname{Spec} B$ s.t. $\mathfrak{q} \cap A = \ker f$. By Proposition 2.2, $B/\mathfrak{q}$ is integral over $A/\ker f$. By 1st isomorphism, $\exists \overline{f} : A/\ker f \hookrightarrow \Omega$. So it is suffices to show the cases for $A \subseteq B$ be integral domain and f is $1-1$.

- Define $\mathcal{S} = \{(C, \sigma) : A \subseteq C \subseteq B, \sigma : C \hookrightarrow \Omega \text{ and } \sigma|_A = f\}$ and partial order $(C, \sigma) \leq (C', \sigma') \iff C \subseteq C'$ and $\sigma'|_C = \sigma$. By the routine argument of Zorn' s lemma, $\exists$ a maximal element (C, σ) in $\mathcal{S}$. We claim that $C = B$ and thus $\exists \sigma : B \to \Omega$ and $\sigma|_A = f$.

- If not, $\exists b \in B \setminus C$. Notice that b is integral over C and C is also integral domain. Notice that we can find at least one polynomial $m(x)$ with least degree in $C[x]$ s.t. $m(b) = 0$, say $\deg m = d$ and m_0 be the leading coefficient. We claim that for all $g(x) \in C[x]$ with $g(b) = 0$, there exists $0 \neq c \in C$ and $h(x) \in C[x]$ s.t.

  $$cg(x) = h(x)m(x)$$

  We induct on $\deg g = n$. If $n = d$, let the leading coefficient of $g(x)$ is g_0, then

  $$m_0 g(b) - g_0 m(b) = 0 \text{ and } \deg(m_0 g(x) - g_0 m(x)) < \deg m(x)$$

By definition of $m(x)$, $m_0g(x) - g_0m(x) = 0$ i.e. $m_0g(x) = g_0m(x)$. For $n > d$, let the leading coefficient of $g(x)$ is g_0, then

$$m_0g(b) - g_0b^{n-d}m(b) = 0 \text{ and } d' := \deg(m_0g(x) - g_0x^{n-d}m(x)) < n$$

Case1. $d' < d$: Then $m_0g(x) = g_0x^{n-d}m(x)$.

Case2. $d' \geq d$: By induction hypothesis, $\exists 0 \neq c \in C, h(x) \in C[x]$ s.t.

$$c(m_0g(x) - g_0x^{n-d}m(x)) = h(x)m(x) \implies cm_0g(x) = (h(x) + cg_0x^{n-d})m(x)$$

Since C is integral domain, $cm_0 \neq 0$. By induction, our claim holds.

- Since $\Omega = \overline{\Omega}$, let β be the arbitrary root of $m^\sigma(x) = 0$. Now, define $\tau : C[b] \to \Omega$ by $f(b) \mapsto f^\sigma(\beta)$. Then $\tau(c) = \sigma(c)$ for all $c \in C$.

  - well-defined : If $g(b) = 0$. By claim, $\exists 0 \neq c \in C$ and $h(x) \in C[x]$ s.t. $cg(x) = h(x)m(x)$ and thus $\tau(c)g^\sigma(\beta) = h^\sigma(\beta)m^\sigma(\beta) = 0$. Since $\tau(c) = \sigma(c) \neq 0$ by σ is injective, $g^\sigma(\beta) = 0$

  - τ is $1-1$: Notice that $\sigma(C)$ is also integral domain. Let $g(x) \in \sigma(C)[x]$ (say $g(x) = p^\sigma(x)$) has least degree s.t. $g(\beta) = 0$. By same argument, $\sigma(c)m^\sigma(x) = h^\sigma(x)g(x)$ for some $0 \neq c \in C$, $h(x) \in C[x]$. Then $cm(x) = h(x)p(x)$ by σ is $1-1 \implies h(b)p(b) = cm(b) = 0 \implies p(b) = 0$ or $h(b) = 0$.

    - If $p(b) = 0$, combine $\deg p \leq \deg m \implies m_0p(x) = p_0m(x) \implies p(b) = 0$.
    - If $h(b) = 0 \implies \deg h = \deg m \implies p(x) = c'$ for some $c' \in C$ $(\rightarrow\leftarrow)$.

    Now, $q(b) \in \ker\tau \iff q^\sigma(\beta) = 0 \iff f(c)q^\sigma = r^\sigma(x)g(x)$ for some $c \neq 0$, $r(x) \in C[x] \implies cq(x) = r(x)p(x) \implies cq(b) = r(b)p(b) = 0 \implies q(b) = 0$. Hence, τ is $1-1$.

Hence, $(C, \sigma) \lneq (C[b], \tau) \in \mathcal{S}$ $(\rightarrow\leftarrow)$. Which means $C = B$.

□

References

[1] Ian G. Macdonald Michael Atiyah. “Introduction to Commutative Algebra”. In: Westview Press, 1994. Chap. 5.

[2] Torgeir Aambø. *On Hilbert’s nullstellensatz*. URL: `https://wiki.math.ntnu.no/_media/ma8202/2020v/on_hilbert_s_nullstellensatz.pdf`.