Primary decomposition for graded modules

Prop: Let S be a Noetherian graded ring, M a graded S-module. Then

① Any associated prime $\mathfrak{p}$ of M is a graded ideal (or a homogeneous ideal, equivalently $\mathfrak{p}$ is generated by the homogeneous elements of $\mathfrak{p}$.) Further, for $\mathfrak{p} \in \mathrm{Ass}(M)$, $\exists\, x \in M_d$ for some d with $\mathfrak{p} = \mathrm{Ann}(x)$

② One can choose a $\mathfrak{p}$-primary graded submodule $Q(\mathfrak{p})$ for each $\mathfrak{p} \in \mathrm{Ass}(M)$ such that

$$(0) = \bigcap_{\mathfrak{p} \in \mathrm{Ass}(M)} Q(\mathfrak{p})$$

i.e., the primary decomposition of $(0) \subseteq M$ can be taken to be graded.

Proof: (1) Let $\mathfrak{p} \in \mathrm{Ass}(M)$, $\mathfrak{p} = \mathrm{Ann}(x)$ for some $x \in M$, say $x = x_{e'} + \dots + x_e$, $x_i \in M_i$, $e' \leq e$. Let $f = f_0 + \dots + f_r \in \mathfrak{p}$, $f_i \in S_i$. Will show each $f_i \in \mathfrak{p}$.

We have

$$0 = fx = f_r x_e + (f_{r-1} x_e + f_r x_{e-1}) + \dots + \underbrace{\sum_{i+j=k} f_i x_j}_{\text{degree } k \text{ term.}} + \dots$$

Thus ① $f_r x_e = 0$

② $f_{r-1} x_e + f_r x_{e-1} = 0$

③ $f_{r-2} x_e + f_{r-1} x_{e-1} + f_r x_{e-2} = 0$

Multiplying ② by f_r and using ①,

we see $f_r^2 x_{e-1} = 0$.

Multiply ③ by f_r^2 and we get

$$f_r^3 x_{e-2} = 0.$$

Continuing in this way, $\exists n$ such

that $f_r^n x_{e'} = 0$, and also then

$$f_r^n x_i = 0 \quad \forall i.$$

Thus $f_r^n x = 0$, so $f_r^n \in \mathrm{Ann}(x) = P$

so $f_r \in P$.

Thus also $f_0 + \cdots + f_{r-1} \in P$.

Continuing in this way, we see

$f_i \in \mathfrak{p} \quad \forall i$, and thus $\mathfrak{p}$ is graded.

We also see $\mathfrak{p} \subseteq \mathrm{Ann}(x_i)$, $\forall i$

and $\mathfrak{p} = \bigcap_{i=e'}^{e} \mathrm{Ann}(x_i)$.

Since $\mathfrak{p}$ is prime, $\mathfrak{p} = \mathrm{Ann}(x_i)$ for some i. (Result from first day handout).

(2) Claim: Let $\mathfrak{p} \subseteq S$ be a graded ideal, $Q \subseteq M$ a $\mathfrak{p}$-primary submodule.

Then the largest graded submodule $Q' \subseteq Q$ (i.e., take the submodule generated by homogeneous elements of Q.) is again $\mathfrak{p}$-primary.

Note: This is sufficient to prove the result: if $(0) = \bigcap_{\mathfrak{p}} Q(\mathfrak{p})$ is a primary decomposition, then we may replace each $Q(\mathfrak{p})$ with $Q(\mathfrak{p})'$.

<u>pf of claim</u>: Let $\mathfrak{p}' \in \mathrm{Ass}(M/Q')$.

We want to show $\mathfrak{p} = \mathfrak{p}'$.

$\mathfrak{p}$ is graded by assumption and $\mathfrak{p}'$ is graded by ①.

Thus we see $\mathfrak{p} = \mathfrak{p}' \iff \mathfrak{p} \cap H = \mathfrak{p}' \cap H$

where $H \subseteq S$ is the set of homogeneous elements of S, i.e., $H = \bigcup_{d=0}^{\infty} S_d$.

If $a \in \mathfrak{p} \cap H$, then a is locally nilpotent on M/Q (i.e., for each $x \in M/Q$, $\exists n > 0$ such that $a^n x = 0$ in M/Q.)

Thus a is also locally nilpotent

for M/Q', because if $x \in M$ is homogeneous, $a^n x \in Q$ for some n; so $a^n x \in Q'$ as $a^n x$ is homogeneous

Thus, with $P' = \mathrm{Ann}(x)$ for some $x \in M/Q'$, which by (1) can be taken to be homogeneous, we thus have $a^n \in P'$, so $a \in P' \cap H$.

$\therefore P \cap H \subseteq P' \cap H$.

Conversely, if $a \in H$, $a \notin P$, then for $x \in M$ satisfying $ax \in Q'$, $x = \sum x_i$, $x_i \in M_i$, we have $ax_i \in Q'$ for each i, so $x_i \in Q$ (because $a \notin P \Rightarrow a$ is not a 0-divisor for M/Q.)

Thus $x_i \in Q'$, $\forall i$, so $x \in Q'$

Thus a is not a 0-divisor for M/Q' and hence $a \notin \mathfrak{p}'$ (since every element of $\mathfrak{p}'$ is a 0-divisor for M/Q'.)

Thus $\mathfrak{p}' \cap H \subseteq \mathfrak{p} \cap H$. ∎

<u>Return to dimension theory</u>:

<u>Def</u>: we define $d(M)$ to be the degree of the polynomial function agreeing with $\chi(M, I; n) = \ell(M/I^n M)$ for large n.

<u>Claim</u>: $d(M)$ is independent of the ideal of definition I.

<u>Pf</u>: If I, J are two ideals of definition, then $\exists s$ such that $J^s \subseteq I$ (e.g., $m^\nu \subseteq I$ for some ν, so $J^\nu \subseteq I$.)

So $\chi(M, I; n) \leq \chi(M, J; sn)$

since $J^{sn} \subseteq I^n$ so

$\ell(M/I^nM) \leq \ell(M/J^{sn}M)$.

Thus if the corresponding polynomial functions are degree d, d' respectively, we see that $d \leq d'$.

Similarly $d' \leq d$, so $d = d'$. ☑

<u>Example</u>: Let $A = k[x_1, \ldots, x_d]_{(x_1, \ldots, x_d)}$ (k a field). Take $I = m = (x_1, \ldots, x_d)$.

Then I^n / I^{n+1} has a k-basis the set of monomials in $x_1, \ldots, x_d$ of degree n. [Exercise: check this!]

so the dimension is $\binom{d+n-1}{d-1}$

$$\Big[\ \overbrace{x_1\ x_1\ \underbrace{x_2 x_2 x_2\ t\ x_3 \cdots x_3}_{d-1}\ t\ x_4 \cdots x_4}^{d+n-1}\ \Big]$$

which is a degree $d-1$ polynomial in n, so $\chi(A, I; n)$ is a degree d polynomial in n.

<u>Goal</u>: $d(M) = \dim(M)$.

[Note: A monomial of degree n in $x_1, \ldots, x_d$ is an expression

$$\prod_{i=1}^{d} x_i^{n_i} \quad \text{with} \quad \sum n_i = n.$$

e.g. $k[x_1, x_2]$, $x_1^3 x_2^4$ is a monomial of degree 7.]

<u>Recall assumptions</u>: (A, m) a local ring, A Noetherian, M a f.g. A-module $m^\nu \subseteq I \subseteq m$ for some $\nu > 0$.

Lemma 0: If I is generated by r elements, then $d(M) \leq r$.

Pf: Since M is finitely generated, have a surjective map $A^p \longrightarrow M$ for some p, and then

$$\chi(A^p, I; n) \geq \chi(M, I; n)$$

So sufficient to show for A^p.

But $\chi(A^p, I; n) = p\,\chi(A, I; n)$,

$= e(A^p/I^n A^p) = e(A/I^n A)^p = p\,e(A/I^n A)$

so enough to show for $M = A$.

We have a surjection

$$S = \left(\frac{A}{I}\right)[X_1, \ldots, X_r] \longrightarrow A^* = \bigoplus_{n=0}^{\infty} I^n/I^{n+1}$$

$$X_i \longmapsto a_i \in I/I^2$$

where $a_1, \ldots, a_r$ are generators of I.

So enough to show for the ring S.

But this is the calculation we already did (replacing k with the finite length module A/I),

and so f_s is of degree $r-1$.

and thus $\chi(A, I; n)$ is degree $\leq r$. ∎

<u>Lemma 1</u>: $(A, \mathfrak{m})$, I as usual.

Suppose $0 \to M_1 \to M_2 \to M_3 \to 0$ is an exact sequence of f.g. A-modules.

Then $d(M_2) = \max\{d(M_1), d(M_3)\}$.

Also $\chi(M_2, I; n) - \chi(M_1, I; n) - \chi(M_3, I; n)$ is a polynomial of degree $< d(M_2)$ for $n \gg 0$.

pf: $\ell(M_3/I^n M_3) = \ell(M_2/(M_1+I^n M_2))$

$$\le \ell(M_2/I^n M_2)$$

so $\chi(M_3, I; n) \le \chi(M_2, I; n)$,

Thus $d(M_3) \le d(M_2)$.

Also

$\chi(M_2, I; n) - \chi(M_3, I; n)$

$= \ell(M_2/I^n M_2) - \ell(M_2/(M_1+I^n M_2))$

$$= \ell\left(\frac{M_1+I^n M_2}{I^n M_2}\right) \underset{\uparrow}{=} \ell\left(\frac{M_1}{M_1 \cap I^n M_2}\right)$$

Noether's third isomorphism theorem

[From exact sequence

$$0 \to \frac{M_1+I^n M_2}{I^n M_2} \to \frac{M_2}{I^n M_2} \to \frac{M_2}{M_1+I^n M_2} \to 0$$

By Artin-Rees, there exists some $r \ge 0$

such that $M_1 \cap I^n M_2 \subseteq I^{n-r} M_1$

Thus

$$\ell(M_1/I^n M_1) \geq \ell(M_1/(M_1 \cap I^n M_2))$$

(since $I^n M_1 \subseteq M_1 \cap I^n M_2$)

$$\geq \ell(M_1/I^{n-r} M_1).$$

Thus

$$\chi(M_1, I; n) \geq \chi(M_2, I; n) - \chi(M_3, I; n)$$

$$\geq \chi(M_1, I; n-r).$$

So the conclusion is that

$\chi(M_1, I; n)$ has the same degree

as $\chi(M_2, I; n) - \chi(M_3, I; n)$

and the same leading term.

Thus the degree of

$\chi(M_2) - \chi(M_3) - \chi(M_1)$

is less than the degree of $\chi(M_2)$,

and $d(M_2) = \max\{d(M_1), d(M_3)\}$. $\blacksquare$

<u>Lemma 2</u>: (A, m) as usual. Then

$d(A) \geq \dim A$.

<u>Pf</u>: Induction on $d(A)$.

<u>Base</u>: $d(A) = 0$. Then $\chi(A, m; n)$

is eventually constant, so

$$m^{\nu} = m^{\nu+1} = \cdots \quad \text{for some } \nu > 0.$$

By Krull's theorem, $\bigcap_{n=0}^{\infty} m^n = 0$,

so $m^{\nu} = (0)$. Thus $\ell(A) < \infty$,

so $\dim A = 0$.

<u>Induction step</u>: Now suppose $d(A) > 0$,

and assume result for rings B with

$d(B) < d(A)$.

If $\dim A = 0$, result is obvious, so assume $\dim A > 0$.

Let $$\mathfrak{p}_0 \supsetneq \cdots \supsetneq \mathfrak{p}_e = \mathfrak{p}$$

be a chain of primes of A of length $e > 0$.

Take $x \in \mathfrak{p}_{e-1} \setminus \mathfrak{p}$. Then

$$\dim\big(A/((x)+\mathfrak{p})\big) \geq e-1, \quad \text{since}$$

$$\mathfrak{p}_0 \supsetneq \cdots \supsetneq \mathfrak{p}_{e-1} \supseteq (x) + \mathfrak{p}_e$$

yields a chain of primes of length $e-1$ in $A/((x)+\mathfrak{p})$.

Now apply lemma $\underline{1}$ to the exact sequence

$$0 \to A/\mathfrak{p} \xrightarrow{\cdot x} A/\mathfrak{p} \to A/((x)+\mathfrak{p}) \to 0.$$

injective since $A/\mathfrak{p}$ is an integral domain to get

$$\chi(A/\mathfrak{p}, I; n) - \chi(A/\mathfrak{p}, I; n)$$
$$- \chi(A/((x)+\mathfrak{p}), I; n)$$

has degree $<$ $\deg \chi(A/\mathfrak{p}, I; n)$

so
$$d(A/((x)+\mathfrak{p})) < d(A/\mathfrak{p}) \leq d(A)$$

Thus by induction hypothesis, we have

$$e - 1 \leq \dim A/((x)+\mathfrak{p}) \leq d(A/((x)+\mathfrak{p})) < d(A)$$

Thus $e \leq d(A)$, so $\dim A \leq d(A)$. ∎

__Remark:__ This shows $\dim A$ is finite for A a Noetherian local ring.

When A is any Noetherian ring, $\mathfrak{p} \subseteq A$ prime, $\dim A_{\mathfrak{p}} = ht(\mathfrak{p})$, so $ht(\mathfrak{p})$ is finite.

Not true that the dimension of

any Noetherian ring is finite.

<u>Lemma 3</u>: (A, m), M as usual, $x \in m \subseteq A$. Then

$$d(M) \geq d(M/xM) \geq d(M) - 1.$$

<u>pf</u>: Let I be an ideal of def'n containing x (e.g. $I = m$). Then

$$\chi(M/xM, I; n) = \ell(M / (xM + I^n M))$$
$$= \ell(M/I^n M)$$
$$- \ell((xM + I^n M)/I^n M)$$

and $\frac{xM + I^n M}{I^n M} \cong \frac{xM}{xM \cap I^n M} \cong \frac{M}{\underbrace{\{m \in M \mid xm \in I^n M\}}_{(I^n M : x)}}$

$x \cdot m \longleftarrow m$

and $I^{n-1} M \subseteq (I^n M : x)$ as $x \in I$.

Thus $\chi(M/xM, I; n)$

$$\geq \ell(M/I^n M) - \ell(M/I^{n-1}M)$$

$$= \chi(M, I; n) - \chi(M, I; n-1).$$

Thus $d(M) \geq d(M/xM) \geq d(M) - 1$. ▨

Lemma 0

<u>Lemma 4</u>: (A, m), M as usual.

$\dim M = r$. Then there exists

$x_1, \ldots, x_r \in m \subseteq A$ such that

$$\ell(M/(x_1M + \cdots + x_rM)) < \infty.$$

<u>Pf</u>: Let I be an ideal of definition,

When $r=0$, we already know $\ell(M) < \infty$.

Now suppose $r > 0$, and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_e$

be the minimal primes of $\sqrt{\mathrm{Ann}(M)}$

such that $\dim(A/\mathfrak{p}_i) = r$

(Such exists because there is

a chain of primes in $A/\mathrm{Ann}(M)$ of length r.)

None of these are maximal ideals since $r>0$, so $m \notin P_i$ for any i. Thus $m \not\subseteq \bigcup_{i=1}^{e} P_i$.

Thus $\exists\, x_1 \in m$ with $x_1 \notin P_i$ for any i.

Then $\dim(M/x_1 M) \leq r-1$,

as $\mathrm{Ann}\, M + (x_1) \subseteq \mathrm{Ann}(M/x_1 M)$

Now proceed by induction. ☒

<u>Theorem</u>: (A, m) local Noetherian, M a f.g. A-module. Then

$d(M) = \dim M$

= smallest r such that $\exists$ $x_1, \dots, x_r \in m$ with

$$\ell(M/(x_1M+\cdots+x_rM))<\infty.$$

<u>Proof</u>: If $\ell(M/(x_1M+\cdots+x_rM))<\infty$

then by Lemma 3, $d(M)\le r$.

If r is as small as possible,

we have $r\le \dim M$ by Lemma 4.

Thus enough to show $\dim(M)\le d(M)$,

so $d(M)\le r\le \dim M\le d(M)$.

Consider a chain of submodules

$$M=M_1\supsetneq M_2\supsetneq\cdots\supsetneq M_{k+1}=(0)$$

with $M_i/M_{i+1}\cong A/P_i$

[We showed such a chain exists when discussing primary decomposition]

Then $P_i\supseteq \mathrm{Ann}\, M \quad \forall i$

~~and $\operatorname{Ass}(M) \subseteq \{ p_1, \dots, p_k \}$~~

and all minimal primes over $\operatorname{Ann}(M)$ are associated primes.

Thus $d(M) = \max \{ d(A/p_i) \mid 1 \le i \le k \}$

by Lemma 1.

$\geq \max \{ \dim(A/p_i) \mid 1 \le i \le k \}$

by Lemma 2

$= \dim A/\operatorname{Ann}(M)$

$= \dim M.$

$\therefore \; d(M) \geq \dim M.$ $\boxtimes$

<u>Theorem</u>: Let A be a Noetherian ring, $I = (a_1, \dots, a_r) \subseteq A$ an ideal. Then any prime ideal minimal over I (i.e., a minimal

element of $V(I)$) has height $\leq r$. In particular $ht(I) \leq r$.

pf: Let $\mathfrak{p} \in V(I)$ be minimal. Then $\mathfrak{p}A_{\mathfrak{p}}$ is the only prime ideal of $A_{\mathfrak{p}}$ containing $IA_{\mathfrak{p}}$, so we have

$$A_{\mathfrak{p}}/IA_{\mathfrak{p}} = A_{\mathfrak{p}}/(a_1 A_{\mathfrak{p}} + \cdots + a_r A_{\mathfrak{p}})$$

is Artinian, (since $\dim A_{\mathfrak{p}}/IA_{\mathfrak{p}} = 0$)

Thus $\dim A_{\mathfrak{p}} \leq r$, and

$$ht\, \mathfrak{p} = \dim A_{\mathfrak{p}}. \quad \square$$

Remark: If (A, m) is local Noetherian, $\dim A = d$, we know from the dimension theorem that every ideal of definition is generated by at least d elements and there exists an ideal of definition generated by d elements.

<u>Def</u>: If $\dim A = d$ and $x_1, \dots, x_d$ generate an ideal of definition, we call $x_1, \dots, x_d$ a <u>system of parameters</u> for A.

If there exists a system of parameters generating $m \subseteq A$ the maximal ideal, we say A is a <u>regular local ring</u>.

Note by Nakayama's lemma, $\dim_{A/m} m/m^2$ is the minimal number of generators necessary to generate m. Thus

(A, m) is a regular local ring $\Leftrightarrow \dim_{A/m} m/m^2 = \dim A$.

In general, $\dim_{A/m} m/m^2 \geq \dim A$.

<u>Remark for algebraic geometers:</u>

The local ring $\mathcal{O}_{X,p}$ of a variety X at point $p \in X$ is regular if and only if p is a non-singular point of X.

<u>Remark</u>: We don't yet know even what $\dim A[x]$ is in terms of $\dim A$. But if A is Noetherian, we will show $\dim A[x] = \dim A + 1$, so in particular $\dim k[x_1, \dots, x_n] = n$ for k a field.

<u>Lemma</u>: Let B be a flat A-algebra. [i.e., given a ring hom. $\varphi: A \to B$] Then the following are equivalent:

① $I = I^{ec}$ for $I \subseteq A$ an ideal

② $\operatorname{Spec} B \to \operatorname{Spec} A$ is surjective.

③ For every maximal ideal $m \subseteq A$, $m^e \neq B$.

④ If M is a non-zero A-module,

then $M_B := M \otimes_A B$ is non-zero

(5) For every A-module M, the map $M \to M_B$, $m \mapsto m \otimes 1$ is injective.

<u>Proof:</u> (1) $\Rightarrow$ (2) Let $\mathfrak{p} \in \operatorname{Spec} A$.

So $\mathfrak{p} = \mathfrak{p}^{ec}$ by (1). Then $S = \varphi(A \setminus \mathfrak{p})$ is disjoint from $\mathfrak{p}^e$, so the extension of $\mathfrak{p}^e$ in $S^{-1}B$ is a proper ideal of $S^{-1}B$ [$I \subseteq B$ has $I^e \neq S^{-1}B$ iff $I \cap S = \emptyset$]

Thus there is a maximal ideal $\mathfrak{m}$ of $S^{-1}B$ containing the extension of $\mathfrak{p}^e \subseteq S^{-1}B$.

Now let $q \subseteq B$ be the contraction of this maximal ideal.

$$\begin{array}{ccccc}
 & & q = m^c & & m \\
 & & \rotatebox[origin=c]{90}{$\subseteq$} & & \rotatebox[origin=c]{90}{$\subseteq$} \\
p & & p^e & & (p^e)^e \\
A & \longrightarrow & B & \longrightarrow & S^{-1}B
\end{array}$$

Note q is prime and $q \supseteq p^e$. and $q \cap S = \phi$. Thus $q^c \subseteq A$ is a prime ideal, and $q^c = p$.

Thus $\varphi^{-1}(q) = p$, or $\varphi^*(q) = p$, showing surjectivity.

② $\Rightarrow$ ③ Suppose $\varphi^* : \operatorname{Spec} B \to \operatorname{Spec} A$ is surjective, $m \subseteq A$ maximal. Then there exists a prime $q \subseteq B$ with $q^c = m$. Then

$$m^e = q^{ce} \subseteq q \neq B.$$

(3) $\Rightarrow$ (4) Let $x \in M$, $x \neq 0$,

$I = \text{Ann}(x)$. So $I \neq A$. Thus

$I^e \neq B$ since $I \subseteq m \subseteq A$ with

m maximal

and $I^e \subseteq m^e \neq B$.

Now $0 \neq B/I^e = B/IB \cong B \otimes_A (A/I)$

$\cong B \otimes_A Ax$

where $Ax \subseteq M$ is the submodule of M

generated by x.

We have an inclusion $Ax \hookrightarrow M$,

and hence, since B is flat,

$B \otimes_A Ax \longrightarrow B \otimes_A M$ is

injective. Thus $M_B = B \otimes_A M$

is non-zero.

(4) $\Rightarrow$ (5) Let M be an A-module and $M' = \ker(M \longrightarrow B \otimes_A M)$

$$m \longmapsto 1 \otimes m$$

So $0 \to M' \to M \to M_B$

so after tensoring with B, we get

$$0 \to M'_B \to M_B \to (M_B)_B$$

is exact by flatness of B as an A-module.

But the latter map is

$$m \otimes b \longmapsto (m \otimes 1) \otimes b$$

$$g : M \otimes_A B \longrightarrow (M \otimes_A B) \otimes_A B$$

and I claim this map is injective.

Define a map

$$p : (M \otimes_A B) \otimes_A B \longrightarrow M \otimes_A B$$

by $p((m \otimes b) \otimes b') = m \otimes b'$

Note $p \circ g(m \otimes b) = p((m \otimes 1) \otimes b)$

$= m \otimes b$,

so $p \circ g : M_B \to M_B$ is the identity,

so in particular g is injective,

Thus $M'_B = 0$, and so $M' = 0$

because we are assuming (4).

(5) $\Rightarrow$ (1) Look at the injective map

$$A/I \longrightarrow (A/I)_B = B/I^e$$

Thus $I \subseteq I^{ec} \subseteq I$ by injectivity

so $I = I^{ec}$. ☐

Note: $M \otimes_A B \to (M \otimes_A B) \otimes_A B$

will not in general be an isomorphism,

e.g. $A = k$, $B = k[x]$, $M = k$

$$M_B = k[x]$$

$$(M_B)_B = k[x] \otimes_k k[x] \cong k[x, y].$$

Remark on Lemma 0:

Question re details of calculation of Hilbert function of the graded ring $S = \left(\frac{A}{I}\right)[x_1, \ldots, x_r]$

S_d = free $\frac{A}{I}$-module generated by monomials of degree d in r variables: there $\binom{d+r-1}{r-1} = N$ such monomials.

polynomial of degree $r-1$.

$$S_d = \left(\frac{A}{I}\right)^N$$

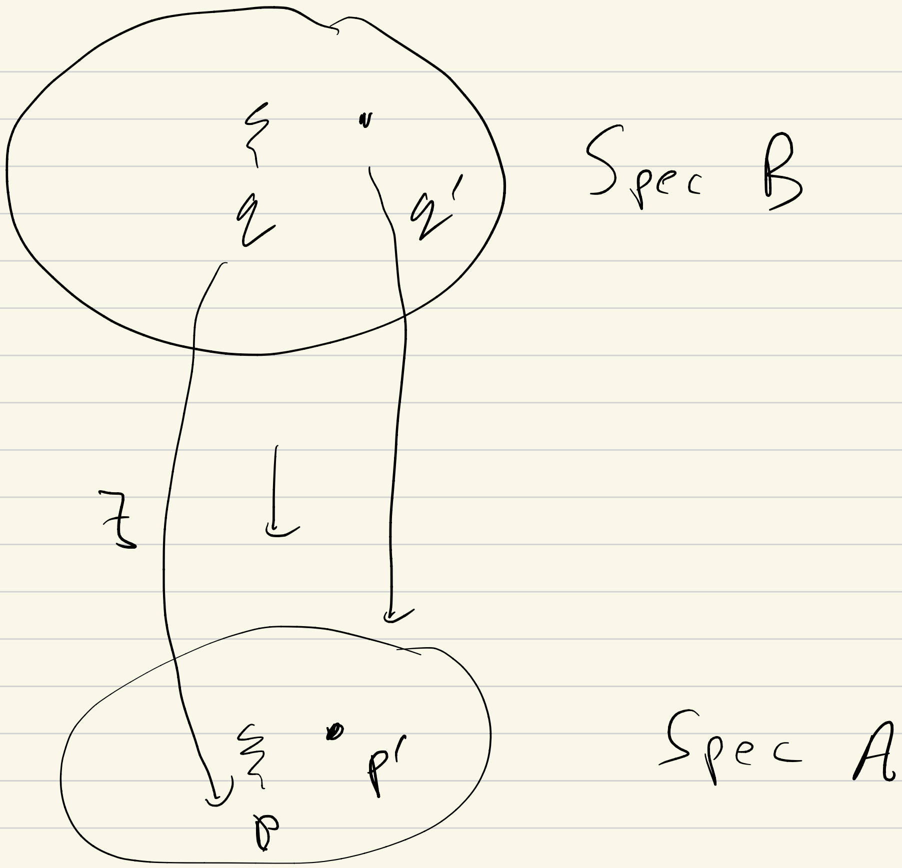
$$\ell_{A/I}(S_d) = N \cdot \ell(A/I)$$
$$= N \cdot \text{constant}.$$

<u>Definition</u>: Let $\varphi : A \to B$ be a homomorphism. We say the <u>going-down theorem</u> holds for φ if for every $\mathfrak{p} \subseteq \mathfrak{p}'$, $\mathfrak{p}, \mathfrak{p}' \in \operatorname{Spec} A$

$q' \in (\varphi^*)^{-1}(\mathfrak{p}')$ (i.e., $\varphi^{-1}(q') = \mathfrak{p}'$)

Then $\exists\ q \subseteq q'$ with $q \in (\varphi^*)^{-1}(\mathfrak{p})$

i.e., $\mathfrak{p} = \varphi^{-1}(q)$.



e.g.
$B = A[x]$

Theorem: Suppose $\varphi : A \to B$ makes B a flat A-algebra. Then the going-down theorem holds for φ.

Proof: Let $\mathfrak{p} \subseteq \mathfrak{p}'$ be primes in A,
$\mathfrak{q}' \in (\varphi^*)^{-1}(\mathfrak{p}')$

Claim: $B_{\mathfrak{q}'}$ is a flat $A_{\mathfrak{p}'}$-algebra.

Pf: First we observe that

$$B_{\mathfrak{p}'} = (\varphi(A \setminus \mathfrak{p}'))^{-1} B$$

is a flat $A_{\mathfrak{p}'}$-module.

Indeed, if $N \to M$ is an injective map of $A_{\mathfrak{p}'}$-module homomorphisms, note

$$N \otimes_{A_{\mathfrak{p}'}} B_{\mathfrak{p}'} = N \otimes_{A_{\mathfrak{p}'}} (A_{\mathfrak{p}'} \otimes_A B)$$

$$\cong N \otimes_A B$$ (identity given in Example Sheet II).

Thus $N \otimes_{A_{\mathfrak{p}'}} B_{\mathfrak{p}'} \to M \otimes_{A_{\mathfrak{p}'}} B_{\mathfrak{p}'}$

coincides with $N \otimes_A B \longrightarrow M \otimes_A B$

which is injective since B is flat over A.

Next, note $B_{q'}$ is a localization of $B_{p'}$, as $B \setminus q' \supseteq \varphi(A \setminus p')$

[Indeed, if $\varphi(a) \in q'$, then $a \in \varphi^{-1}(q') = p'$.]

But $B_{q'}$ is flat as a $B_{p'}$-module

[In general, $S^{-1}A$ is a flat A-module.] A similar argument as above then shows $B_{q'}$ is a flat $A_{p'}$-module

[Special case of: if $A \xrightarrow{\varphi} B \xrightarrow{\psi} C$ given with B a flat A-algebra and C a flat B-algebra, then C is a flat A-algebra.] $\boxtimes$

Now $A_{p'}$ has a unique maximal ideal whose extension in $B_{q'}$ is contained in $q' B_{q'}$, since $\varphi(p') \subseteq q'$ (since $\varphi^{-1}(q') = p'$).

Thus item (3) of the previous lemma holds, and $\varphi^*: \operatorname{Spec} B_{q'} \to \operatorname{Spec} A_{p'}$ is surjective.

Let $q^* \in \operatorname{Spec} B_{q'}$ be a prime lying over $p A_{p'}$, i.e.,

$\varphi^*(q^*) = p A_{p'}$. Let

$q = q^* \cap B$: this is a prime ideal in B contained in q'.

Finally, $\varphi^*(q) = p$ or $\varphi^{-1}(q) = p$:

We have the commutative diagram

q

$$\begin{tikzcd} B \arrow[r] & B_{q'} \supseteq q^* \\ A \arrow[u, "\varphi"] \arrow[r] & A_{p'} \arrow[u, "\varphi"'] \end{tikzcd}$$

$\varphi^{-1}(q) = \varphi^*(q)$

$\varphi^{-1}(q^*) = pA_{p'}$

p

hence $\varphi^*(q) = p$ by commutativity.

Hence going-down holds. $\boxtimes$

<u>Theorem</u>: Let $\varphi: A \to B$ be a homomorphism of Noetherian rings, $q \in \operatorname{Spec} B$, $p = \varphi^{-1}(q) = \varphi^*(q)$.

Then

① $ht(q) \leq ht(p) + ht(q/pe)$

computed in B/pe

or equivalently,

$$\dim B_q \le \dim A_p + \dim (B_q \otimes_{A_p} k(p))$$

where $k(p) = A_p / p A_p$.

(2) The inequality of (1) is an equality if going-down holds for φ (e.g., if B is a flat A-algebra)

(3) If $\varphi^* : \operatorname{Spec} B \to \operatorname{Spec} A$ is surjective and going-down holds for φ, then $\dim B \ge \dim A$, and $ht(I) = ht(I^e)$ for $I \subseteq A$ any ideal.

Pf: (1) We first check the equivalence of the two inequalities

We have $ht(q) = \dim B_q$

and $ht(p) = \dim A_p$

We need to check that $ht(q/p^e)$

$= \dim (B_q \otimes_{A_p} k(p))$. Note

primes of B/p^e contained in q/p^e

are in 1-1 correspondence with primes

$q' \subseteq B$ with $p^e \subseteq q' \subseteq q$, and

note that if $q' \subseteq q$, $p^e \subseteq q' \Leftrightarrow \varphi^{-1}(q') = p$.

Indeed, if $p^e \subseteq q'$, then

$p \subseteq \varphi^{-1}(p^e) \subseteq \varphi^{-1}(q') \subseteq \varphi^{-1}(q) = p$,

and conversely, if $\varphi^{-1}(q') = p$.

$q' \supseteq \varphi^{-1}(q')^e = p^e$

Thus the primes of B/p^e contained

in q/p^e are in 1-1 correspondence

with elements of $(\varphi^*)^{-1}(\mathfrak{p})$ contained in $\mathfrak{q}$.

Now we have an induced map $\tilde{\varphi} : A_{\mathfrak{p}} \to B_{\mathfrak{q}}$, and hence $\tilde{\varphi}^* : \operatorname{Spec} B_{\mathfrak{q}} \to \operatorname{Spec} A_{\mathfrak{p}}$.

The primes of $B_{\mathfrak{q}}$ are in 1-1 correspondence with the primes of B contained in $\mathfrak{q}$, and hence the primes of $B/\mathfrak{p}^e$ contained in $\mathfrak{q}/\mathfrak{p}^e$ are in 1-1 correspondence with primes of $(\tilde{\varphi}^*)^{-1}(\mathfrak{p}A_{\mathfrak{p}})$. However, this set can be identified, via Example Sheet I, with

$$\operatorname{Spec} B_{\mathfrak{q}} \otimes_{A_{\mathfrak{p}}} k(\mathfrak{p}),$$ hence the claim.

In particular, to show the inequality, we can replace A with $A_{\mathfrak{p}}$, B with $B_{\mathfrak{q}}$, and so assume $(A, \mathfrak{p})$, $(B, \mathfrak{q})$ are local with $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$. We need to show

$$\dim B \leq \dim A + \underset{\substack{\uparrow \\ \text{height of } \mathfrak{q}/\mathfrak{p}B}}{\dim(B/\mathfrak{p}B)}$$

Let $a_1, \dots, a_r$ be a system of parameters for A, $I = (a_1, \dots, a_r)$, an ideal of definition, $r = \dim A$. Then $\mathfrak{p}^{\nu} \subseteq I \subseteq \mathfrak{p}$ for some $\nu > 0$, so

$$(\mathfrak{p}^{\nu})^e \subseteq I^e \subseteq \mathfrak{p}^e$$

Then I^e and p^e have the same radical in B

[Certainly $\sqrt{I^e} \subseteq \sqrt{p^e}$.

If $f^n \in p^e$, then $f^{nv} \in (p^e)^v \subseteq I^e$

so $f \in \sqrt{I^e}$.

Thus $\sqrt{p^e} \subseteq \sqrt{I^e}$.]

So from the definition of dimension

$\dim(B/pB) = \dim(B/IB)$

If $\dim B/IB = s$, and

$\bar{b}_1, \ldots, \bar{b}_s$ is a system of parameters

of B/IB, then taking lifts

$b_1, \ldots, b_s \in B$ of $\bar{b}_1, \ldots, \bar{b}_s$, we

see that

$$b_1, \ldots, b_s, \varphi(a_1), \ldots, \varphi(a_r)$$

generate an ideal of definition for B. Thus $\dim B \leq r+s$

$$= \dim A + \dim B/pB.$$

(2)

$$\begin{array}{c} p^e \subseteq q \in \operatorname{Spec} B \\ \big\downarrow \varphi^* \\ p \in \operatorname{Spec} A \end{array}$$

We want to show that if going-down holds for $\varphi : A \to B$, then $ht(q) = ht(p) + ht(q/p^e)$

$\leq$ is (1).

If $ht(q/p^e) = s$, $\exists$ a chain of primes of B

$$q = q_0 \supsetneq q_1 \supsetneq \cdots \supsetneq q_s \supseteq p^e$$

Now $\quad p = q^c \supseteq q_i^c \supseteq p^{ec} \supseteq p$

so $\quad \varphi^*(q_i) = p \quad \forall i.$

If $\ ht(p) = r$, then $\exists$ a chain

$$p = p_0 \supsetneq p_1 \supsetneq \cdots \supsetneq p_r$$

of primes in A. Then by going-down, I can find a chain of primes of B

$$q_s = q_0' \supsetneq q_1' \supsetneq \cdots \supsetneq q_r'$$

with $\varphi^{-1}(q_i') = p_i$.

Thus we have a chain of primes

$$q = q_0 \supset \cdots \supset q_s \supset q_1' \supset \cdots \supset q_r'$$

a chain of length $r+s$.

Thus $ht(q) \geq r+s$.

Thus $ht(q) \geq ht(p) + ht(q/p^e)$.

(3) We now assume $\varphi^*: \operatorname{Spec} B \to \operatorname{Spec} A$ is surjective and going-down holds.

$\dim B \geq \dim A$ is immediate from the inequality

$$ht(q) = ht(p) + ht(q/p^e) \geq ht(p)$$

so if $p \subseteq A$ is a prime with $ht(p) = \dim A$, and $\exists\, q$ s.t. $\varphi^*(q) = p$, so

$$\dim B \geq ht(q) \geq ht(p) = \dim A.$$

Now let $I \subseteq A$, $I^e \subseteq B$.

We want to show $ht(I) = ht(I^e)$

Let $q \supseteq I^e$ be a minimal prime over I^e so that $ht(q) = ht(I^e)$

[Note $I^e \neq B$ if $I \neq A$ by surjectivity of φ^*: if $p \supseteq I$ a prime, then $\exists\, q \subseteq B$ with $q^c = p$ and $q \supseteq p^e \supseteq I^e$.]

Now let $p = q^c$. Then $ht(q/p^e) = 0$. Indeed, if $\exists$ a prime q' with

$$q \supsetneq q' \supset p^e, \quad \text{then}$$

$$p = q^c \supseteq (q')^c \supseteq p^{ec} \supseteq p$$

so $(q')^c = q^c = p$ and

$$(q')^c = q^c \supseteq I^{ec} \supseteq I$$

Thus $q \supseteq I^e$ and thus q is not minimal over I^e.

Thus by (2), $ht(q) = ht(p) + ht(q/p^e)$

$= ht(p)$.

But $ht(q) = ht(I^e)$, and $p \supseteq I$

so $ht(p) \geq ht(I)$.

$\therefore$ $ht(I^e) \geq ht(I)$.

Conversely, let $p \supseteq I$ with $ht(p) = ht(I)$. Let $q \subseteq B$ be a prime with $\varphi^*(q) = p$.

By replacing q with a smaller prime, I can assume that q is minimal over $p^e \supseteq I^e$.

Thus

$$ht(I) = ht(p) = ht(q) \geq ht(I^e). \;\blacksquare$$

by (2) again since $ht(q/p^e) = 0$

<u>Theorem</u>: Let A be a Noetherian ring, $B = A[x_1, \ldots, x_n]$. Then

$$\dim B = \dim A + n.$$

<u>Pf</u>: Can take $n=1$ and repeat, so suppose $B = A[x]$.

B is a flat A-algebra (1st example sheet) so going-down holds.

Let $p \subseteq A$ be prime, $q \subseteq B$ a prime ideal maximal amongst those lying over p

[Note: $p^e = p[x] \neq B$ is prime, so

$\exists$ primes lying over p. [Example Sheet II])

I claim $ht(q/pe) = 1$.

After localizing A and B at $S = A \setminus p$, I can assume p is maximal and $B/pB = (A/p)[X]$ is a polynomial ring in one variable over a field. Thus B/pB is a principal ideal domain and every maximal ideal has height 1.

So $ht(q/p^e) = 1$, so $ht(q) = ht(p) + 1$ by (2) of previous theorem.

Since $\operatorname{Spec} B \to \operatorname{Spec} A$ surjective, the result follows. $\square$

Cor: Let k be a field. Then $\dim k[X_1, \dots, X_n] = n$, and the ideal $I = (X_1, \dots, X_i)$ is a prime of $k[X_1, \dots, X_n]$ of height i.

Pf: Since

$$(0) \subsetneq (X_1) \subsetneq \cdots \subsetneq (X_1, \dots, X_n)$$

is a chain of primes of length n, and $\dim k[X_1, \dots, X_n] = n$ by Theorem, each $(X_1, \dots, X_i)$ must be height i. ☒

Integrality and integral closure

Def: Let $A \subseteq B$ rings. An element $x \in B$ is *integral* over A if x satisfies an equation

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

for $a_1, \ldots, a_n \in A$.

<u>Example</u>: $A = \mathbb{Z}$, $B = \mathbb{Q}$

$x \in \mathbb{Q}$ is integral over $\mathbb{Z}$ if and only if $x \in \mathbb{Z}$. (See Numbers + Sets.)

<u>Prop</u>: Fix $A \subseteq B$. The following conditions are equivalent:

1. $x \in B$ is integral over A.
2. $A[x] \subseteq B$ is a finitely generated A-module. Here $A[x]$ is the subring of B generated by A and x, i.e., all polynomials in x.
3. $A[x] \subseteq C \subseteq B$ for some subring C of B with C

a f.g. A-module.

(4) $\exists$ a faithful $A[x]$-module $\underset{B}{\overset{\cap}{}}$

M which is f.g. as an A-module.

[Faithful means $\mathrm{Ann}_{A[x]}(M) = 0$.]

Pf: (1) $\Rightarrow$ (2) We have

$$x^{n+r} = -(a_1 x^{n+r-1} + \dots + a_n x^r)$$

$\forall r > 0$, so by induction,

all positive powers of x lie in

the A-submodule of B generated by

$1, x, \dots, x^{n-1}$. So $A[x]$ is

a f.g. A-module.

(2) $\Rightarrow$ (3) $C = A[x]$.

(3) $\Rightarrow$ (4) Take $M = C$, acting

$yC = 0 \Rightarrow y \cdot 1 = 0 \Rightarrow y = 0$, so

$\mathrm{Ann}_{A[x]}(C) = 0$

(4) $\Rightarrow$ (1) Let $\phi : M \to M$ be given by multiplication by x, noting $xM \subseteq M$ since M is an $A[x]$-module. Thus $\exists\, a_1, \dots, a_n \in A$ such that

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

This tells us that $x^n + a_1 x^{n-1} + \cdots + a_n$ annihilates M, thus

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

Cor: Let $x_1, \dots, x_n \in B$ be elements integral over A. Then

$A[x_1, \dots, x_n]$ is a finitely generated A-module.

Pf: Induction on n. $n=1$ is the previous proposition. If $A[x_1, \dots, x_{n-1}]$ is a f.g. A-module, and $A[x_1, \dots, x_n]$ is a f.g. $A[x_1, \dots, x_{n-1}]$-module, hence $A[x_1, \dots, x_n]$ is a f.g. A-module. ☒

Cor: The set $C \subseteq B$ of elements of B integral over A is a subring of B containing A.

Pf: Given $x, y \in C$, $A[x, y]$ is f.g. over A, so $x+y$, xy are integral over A. ☒

Def: We call C the integral closure of A in B. If $C = A$, we say A is *integrally closed* in B

If $C = B$, we say B is *integral* over A.

Example: $\mathbb{Q} \subseteq K$ a finite field extension: $A = \mathbb{Z} \subseteq B = K$

The integral closure of A in B is written as $\mathcal{O}_K$, the number ring of K.

Cor: If $A \subseteq B \subseteq C$ are rings, and B integral over A, C integral over B, then C is integral over A.

Pf: If $x \in C$, have

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

Let $B' = A[b_1, \ldots, b_n] \subseteq B$.

Then B' is a f.g. A-module, and x is integral over B', so $B'[x]$ is a finitely generated B'-module, so $B'[x] \subseteq C$ is a f.g. A-module, so x is integral over A ☒

Cor: Let $A \subseteq B$ rings, C the integral closure of A in B. Then C is integrally closed in B.

Pf: Let $x \in B$ be integral over C. Then the same argument as in the previous corollary shows that

x is also integral over A. Thus $x \in C$. ☒

<u>Prop</u> $A \subseteq B$, B integral over A.

Then

① If $I \subseteq B$ is an ideal and

$J = I^c = I \cap A$, then B/I

is integral over A/J.

② If $S \subseteq A$ is mult. closed, then

$S^{-1}B$ is integral over $S^{-1}A$.

<u>Pf</u>: ① If $x \in B$, then

(*) $\quad x^n + a_1 x^{n-1} + \cdots + a_n = 0$ for

some $a_i \in A$. Reduce this equation

mod J to get an equation

satisfied by $x + I \in B/I$.

② Let $x/s \in S^{-1}B$, $x \in B$, $s \in S$

Have equation (*) for x.

Divide (*) by s^n to get

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

so x/s is integral over $S^{-1}A$. ☒

<u>Prop</u>: $A \subseteq B$, C integral closure of A in B. Let $S \subseteq A$ be mult. closed subset. Then $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.

<u>Pf</u>: Previous proposition implies $S^{-1}C$ integral over $S^{-1}A$, and hence $S^{-1}C$ is contained in the integral closure of $S^{-1}A$ in $S^{-1}B$.

Now suppose $\frac{b}{s} \in S^{-1}B$ is integral over $S^{-1}A$. Then have

$$\left(\frac{b}{s}\right)^n + \left(\frac{a_1}{s_1}\right)\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_n}{s_n} = 0.$$

$(a_i \in A,\ s_i \in S)$.

Clear denominators by multiplying by $(st)^n$ where $t = \prod_{i=1}^{n} s_i$

Get $(bt)^n + \cdots = 0$

an equation of integrality for bt but in $S^{-1}B$. So $\exists\ t' \in S$.

s.t. $t'((bt)^n + \cdots) = 0$ in B.

Thus $(btt')^n + \cdots = 0$ in B,

so btt' is integral over A,
so $btt' \in C$,
and hence $\dfrac{b}{s} = \dfrac{btt'}{stt'} \in S^{-1}C$ $\square$

Def: An integral domain is said to be integrally closed (or normal) if it is integrally closed in its field of fractions.

Being integrally closed is a local property:

Prop: Let A be an integral domain. The following conditions are equivalent:

1. A is normal
2. $A_{\mathfrak{p}}$ is normal $\forall$ primes $\mathfrak{p}$
3. $A_{\mathfrak{m}}$ is normal $\forall$ maximal ideals $\mathfrak{m}$.

Pf: $K = A_{(0)}$ the field of fractions, let C be the integral closure of A in K, so by previous

prop., $C_\mathfrak{p}$ is the integral closure

of $A_\mathfrak{p}$ in K. Let $f: A \to C$ be the inclusion.

Then A is integrally closed

$\iff$ f is surjective

$\iff$ $f_\mathfrak{p}: A_\mathfrak{p} \to C_\mathfrak{p}$ is surjective $\forall \mathfrak{p}$

$\iff$ $f_\mathfrak{m}: A_\mathfrak{m} \to C_\mathfrak{m}$ is surjective $\forall \mathfrak{m}$.

$\iff$ $A_\mathfrak{m}$ being integrally closed in K $\forall \mathfrak{m}$

$\iff$ $A_\mathfrak{p}$ being integrally closed in K $\forall \mathfrak{p}$. ▨

<u>Def</u>: If B is an integral domain with $K = B_{(0)}$ its field of fractions,

We say B is a <u>valuation ring</u> of K if for each non-zero $x \in K$, either $x \in B$ or $x^{-1} \in B$.

<u>Prop:</u> Let B be a valuation ring. Then

① B is a local ring.

② If $B \subseteq B' \subseteq K$, then B' is a valuation ring.

③ B is integrally closed in K (i.e., B is normal.)

<u>pf:</u> ② is obvious from the def'n.

① Let $m \subseteq B$ be the set of non-invertible elements of B. Enough to show m is an ideal.

If $a \in B$, $x \in m$, $ax \notin m$, then $0 \neq x$

$(ax)^{-1} \in B$, so $a \cdot (ax)^{-1} = x^{-1} \in B$;

a contradiction, so $ax \in m$.

$\therefore$ m is closed under multiplication

by elements of B.

If $x, y \in m$ both non-zero,

then either $xy^{-1} \in B$ or $x^{-1}y \in B$.

If $xy^{-1} \in B$, then

$$x + y = (1 + xy^{-1})\, y \in B \cdot m \subseteq m$$

so $x + y \in m$.

Similarly, if $x^{-1}y \in B$, then

$$x + y = (1 + x^{-1}y)\, x \in m.$$

(3) Let $x \in K$ be integral over B,

say $x^n + b_1 x^{n-1} + \cdots + b_n = 0$ with $b_i \in B$

If $x \notin B$, then $x^{-1} \in B$, and

$$x = -(b_1 + b_2 x^{-1} + \cdots + b_n x^{-n+1})$$

So $x \in B$. $\blacksquare$

<u>Example</u>: $\mathbb{Z}_{(p)}$, the localization at a prime (p).

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \cdot p^n \;\middle|\; \begin{array}{l} a, b \in \mathbb{Z} \text{ are coprime} \\ \text{to } p, \quad n \geq 0, \; b \neq 0 \end{array} \right\}$$

$$\mathbb{Q} = \left\{ \frac{a}{b} \cdot p^n \;\middle|\; \begin{array}{l} a, b \in \mathbb{Z} \text{ coprime to } p \\ n \in \mathbb{Z}, \quad b \neq 0 \end{array} \right\}$$

So if $n \geq 0$, $\frac{a}{b} p^n \in \mathbb{Z}_{(p)}$

if $n < 0$, $\left(\frac{a}{b} p^n\right)^{-1} \in \mathbb{Z}_{(p)}$.

<u>Situation</u>: Fix a field K, Ω an algebraically closed field.

Let Σ be the set of pairs

(A, f)

where

- $A \subseteq K$ is a subring of K
- $f : A \longrightarrow \Omega$ is a ring hom,

Σ comes with a partial ordering:

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

The hypotheses of Zorn's lemma hold, so Σ has maximal elements, assuming Σ is non-empty.

Let (B, g) be such a maximal element.

<u>Goal</u>: (B, g) is a valuation ring.

<u>Lemma</u>: B is a local ring with maximal ideal $\mathfrak{m} = \ker g$.

Pf: As $g(B) \subseteq \Omega$ is a subring, hence an integral domain, so $\mathfrak{m} = \ker g$ is a prime ideal. Can extend $g : B \longrightarrow \Omega$ to $g' : B_{\mathfrak{m}} \longrightarrow \Omega$, since every element of $B \setminus \mathfrak{m}$ has non-zero, hence invertible, image in Ω.

Since (B, g) is maximal, we thus see that $B = B_{\mathfrak{m}}$, which is only possible if $(B, \mathfrak{m})$ is a local ring. $\blacksquare$