

Primary decomposition

$\mathbb{Z} \Rightarrow 18 = 2 \cdot 9 = 2 \cdot \underline{3^2}$
 $3, 2 = \text{prime numbers and prime ideals } P \subseteq R$
 3^2 ~~no~~ could generalize to $P^2 \dots$
 $3^2 \hat{=} \text{"primary ideal"}$

$R = \text{noetherian ring}$

Def: $Q \subseteq R$ ideal. Q is called "primary" \iff in R/Q every zero-divisor is nilpotent.

Corollary: prime \implies primary

Example: $Q = \text{primary} \iff \forall a, b \in R: \text{if } ab \in Q, \text{ and } a \notin Q, \text{ then } \exists k: b^k \in Q$
 $R = \mathbb{Z}[x, y], Q = (x^2, y) \rightsquigarrow \mathbb{Z}[x, y]/(x^2, y) \cong \mathbb{Z}[x]/(x^2)$
 $Q' = (x^2, y^2)$ is also primary!

Remark: $Q = \text{primary} \implies \sqrt{Q} = \text{prime ideal!}$

Proof: Let $a, b \in R, ab \in \sqrt{Q} \implies \exists k: a^k b^k \in Q$. Goal: $a \in \sqrt{Q}$ or $b \in \sqrt{Q}$.
 If $a^k \notin Q \implies \exists \ell: (b^k)^\ell \in Q \implies b \in \sqrt{Q}$. \square

\rightsquigarrow If $Q = \text{primary}, P = \sqrt{Q}$ then $Q = \text{"P-primary"}$
Lemma: $Q, Q' = \text{P-primary} \implies Q \cap Q' = \text{P-primary}$, ($Q, Q' = \text{primary} \not\Rightarrow Q \cap Q' = \text{primary}$)
Example: $R = \mathbb{Z}[x, y], Q = (x), Q' = (y) \rightsquigarrow Q \cap Q' = (x) \cap (y) = (xy) = xy \cdot \mathbb{Z}[x, y]$
 $xy \in Q \cap Q', x, y \notin Q \cap Q'$

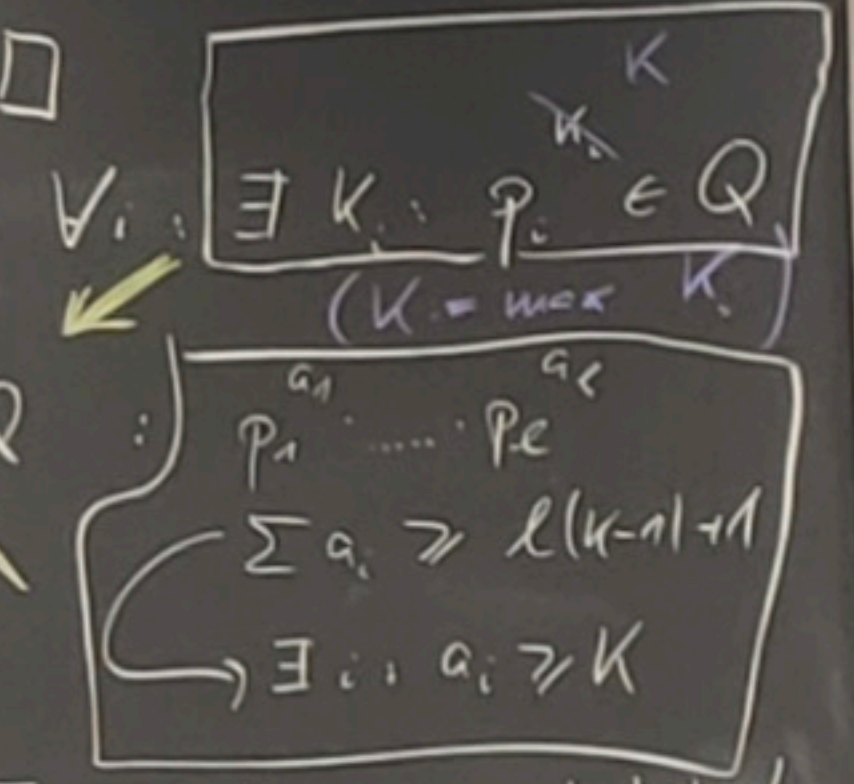
Proof (Lemma): $Q = \text{P-primary} \iff \forall a, b \in R: [ab \in Q, a \notin Q \implies b \in P]$, i.e. $[ab \in Q \implies a \in Q \text{ or } b \in P]$

Let $ab \in Q \cap Q', b \in P$ then
 $\downarrow \in Q, \in Q' \implies a \in Q, a \in Q' \implies a \in Q \cap Q'$

Remark: $Q = \text{P-primary} \implies \exists k: P^k \subseteq Q \subseteq P$. $\sqrt{Q} = P$

Conj: $P = \text{prime ideal} \implies \forall k: Q := P^k$ is P-primary

WRONG: Example: $R = \mathbb{Z}[x, y, z]/(xy - z^2), P = (x, z)$ prime ideal
 $Q := P^2 = (x^2, xz, z^2) \rightsquigarrow R/Q = \mathbb{Z}[x, y, z]/(xy - z^2, x^2, xz, z^2) \cong \mathbb{Z}[x, y, z]/(xy, x^2, xz, z^2)$: $y = \text{zero divisor, } \neq \text{nilpotent!}$



but: Lemma: $m \in \text{Max Spec } R$, if $Q \subseteq R$ ideal with $\sqrt{Q} = m \implies Q$ is primary

Proof: $\sqrt{Q} \subseteq R/Q$ becomes $\overline{0} = \{ \text{nilpotent elements} \}$
 $m \subseteq R/Q$ is contained in every prime ideal of R/Q
 $\{ \text{zero divisors} \} \cup \{ 0 \} = \bigcup \text{Ass}(R/Q)$
 $= m = \overline{0}$ \rightsquigarrow all zero-divs are nilpotent! \square

(Indeed, $P = (x, z)$ from the example was not max!)

Goal: all ideals are intersections of primary ideals.

Def: I is \mathbb{N} -irreducible \iff If $I = I_1 \cap I_2 \implies I = I_1$ or $I = I_2$

Prop: Every ideal can be written as a finite intersection of \mathbb{N} -irred. ideals

Proof: If I is not \mathbb{N} -irred $\implies \exists I = I_1 \cap I_2, I_1, I_2 \not\supseteq I$
 If either I_1 or I_2 are not \mathbb{N} -irred $\implies I_1 = I_{n1} \cap I_{n2}, I_{n1}, I_{n2} \not\supseteq I_1 \dots$ terminates!

alternative / cleaner version of proof: $S = \{ I \subseteq R \mid I \text{ is not vpr. as a finite intersection of } \mathbb{N}\text{-irred. ideals} \}$

Claim: $S \neq \emptyset$, if not $\implies \exists$ maximal element $I \in S \implies I \neq (\mathbb{N}\text{-irred})$
 $\implies I_1, I_2 \notin S \implies I_1 = \text{finite int. of } \mathbb{N}\text{-irred. ideals} \implies I \text{ is } \mathbb{N}\text{-irred.} \implies I = I_1 \cap I_2 (I_1, I_2 \not\supseteq I)$ \square

Example: maximal ideal in $\mathbb{Z}[x, y]$: $(x^3, xy^2) = I \implies \sqrt{I} = (x) = \text{prime}$
 $I \neq \text{primary}$

$[I = I_1 \cap I_2, I_1, I_2 = \text{maximal}]$

$\text{st}(I) = \text{st}(I_1) \cup \text{st}(I_2)$

$\{ \text{max. in } \mathbb{Z}[x, y]/I \} \cong \{ \text{max. in } \mathbb{Z}[x] \} \cup \{ \text{max. in } I \}$

Goal: \mathbb{N} -irreducible? \implies primary?

$I_1 = (x^3, xy^2)$
 $I_2 = (x^3, xy^2, y^3) \neq \text{irreducible}$

$(x^3) \rightsquigarrow \sqrt{(x^3)} = (x)$
 (x^3) primary

Lemma Every \mathcal{N} -ideal is primary.

Proof Let $I = \mathcal{N}$ -ideal, goal: R/I : [zero div \Rightarrow nilpotent]

$R \cong R/I$, i.e. $I = (0)$ THAT is: $(0) = \mathcal{N}$ -ideal; show: [z.d. \Rightarrow n.p. in R]

Claim $y \in R \rightsquigarrow \text{Ann}(y^k) \subseteq R$ ideal $(\forall k \in \mathbb{N})$

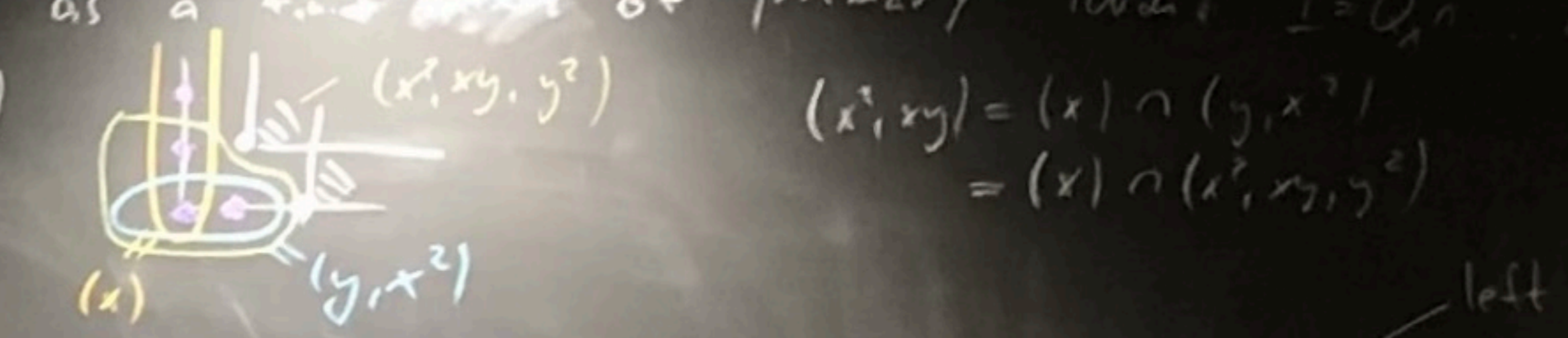
$\text{Ann}(y^k) \subseteq \text{Ann}(y^{k+1})$ ascending $\Rightarrow \exists K: \text{Ann}(y^k) = \text{Ann}(y^{k+1})$

this means: $\text{Ann}(y^k) \cap (y^k) = (0) \Rightarrow$ either $y^k = 0$ or $\text{Ann}(y^k) = 0$.

$y^k z = y \cdot y^{k-1} z = 0$
 $\hookrightarrow z \in \text{Ann}(y^{k-1}) = \text{Ann}(y^k) \Rightarrow y^k z = 0$

Let $y =$ zero divisor in R
 $\Rightarrow y^k \neq 0: y^k y = 0 \Rightarrow \text{Ann}(y^k) \neq 0$
 $\Rightarrow y^k = 0$ for $k \gg 0$
 i.e. nilpotent!! \square

Corollary Each $I \subseteq R =$ noeth.v. is repr. as a finite ~~and~~ of primary ideals $I = Q_1 \cap \dots \cap Q_m$.

Problem: not unique!! Ex $I = (x^2, xy)$ 

Recall $\sqrt{I} = \bigcap M_{\mathfrak{p}}(R/I)$
 $\sqrt{0} = \bigcap M_{\mathfrak{p}}(R) = \bigcap \text{Spec} R$

Def. $I = Q_1 \cap \dots \cap Q_m$ ($Q_i =$ primary ideals) is "reduced" / "unstable" \iff $\bullet \forall i, Q_i \cap \dots \cap Q_m \supseteq I$
 $\bullet i \neq j \Rightarrow \sqrt{Q_i} \neq \sqrt{Q_j}$

P_1, \dots, P_m should be mutually different

Remark $\sqrt{I} = \sqrt{Q_1 \cap \dots \cap Q_m} = P_1 \cap \dots \cap P_m \Rightarrow$ any $\mathcal{K} \{P_i\} \supseteq M_{\mathfrak{p}}(R/I) = M_{\mathfrak{p}}(R/\sqrt{I})$

$(\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J})$?
 "S" \checkmark YES
 $\Rightarrow a \in \sqrt{I \cap J} \Rightarrow \exists k: a^k \in I \cap J \Rightarrow a^k \in I \Rightarrow a \in \sqrt{I}$

Theorem (1st uniqueness) $I = Q_1 \cap \dots \cap Q_m$ reduced primary decomposition
 $\Rightarrow \{P_1, \dots, P_m\} = \text{Ass}(R/I)$ with $\bigcup M_{\mathfrak{p}}(R/I) = \text{Ass}(R/I) = M_{\mathfrak{p}}(R/I)$

Proof Proposition $Q = P$ -primary ideal $\iff \sqrt{Q} = P$
 $x \in R \rightsquigarrow (Q : x) = \{a \in R \mid ax \in Q\} \supseteq Q$

$(Q : x) =$ primary:
 $a \in (Q : x), a \notin P$
 $a(x) \in Q \Rightarrow \exists r \in Q \Rightarrow r \in (Q : x)$

$x \in Q \Rightarrow (Q : x) = (R)$
 $x \notin Q \Rightarrow Q \subseteq (Q : x) \subseteq P$ P -primary
 and $(Q : x)$ is P -primary, $\{a \mid ax \in Q, x \notin Q\} \Rightarrow a \in P$


1. step $\text{Ass}(R/I) \subseteq \{P_1, \dots, P_m\}$ First: Assume that $I = 0$.
 Let $x \in R$ not a unit of $\text{Ann}(x)$ ($\in \text{Ass}(R)$) if $\text{Ann}(x) =$ prime \checkmark
 $(Q : (I \cap J) : x) \stackrel{?}{=} (I : x) \cap (J : x) \checkmark \Rightarrow (0 : x) = (Q_1 : x) \cap \dots \cap (Q_m : x)$

$\Rightarrow \text{Ann} x = \bigcap_{Q_i \not\ni x} (Q_i : x) \Rightarrow \sqrt{\text{Ann} x} = \bigcap_{Q_i \not\ni x} \sqrt{(Q_i : x)} = \bigcap_{Q_i \not\ni x} P_i$

If $\text{Ann} x \in \text{Ass}(R) \Rightarrow P_{\text{Ann} x} =$ prime $= \bigcap_{Q_i \not\ni x} P_i \Rightarrow \exists i: \text{Ann} x = P_i$ (otherwise: $\exists y \in P_i \setminus \text{Ann} x \Rightarrow \exists y \in \bigcap P_i \setminus \text{Ann} x$)

2nd step: take P_i mins $\in \text{Ass}(R)$
 take $x \in I_i = \bigcap_{j \neq i} Q_j = Q_1 \cap \dots \cap Q_{i-1} \cap Q_{i+1} \cap \dots \cap Q_m \supseteq (0) \Rightarrow x \notin Q_i \Rightarrow \sqrt{\text{Ann} x} = P_i$

3rd step: suppose $x \in P_i \setminus I_i$, st $P_i \cdot I_i = 0$ (it exists: $Q_i \cdot I_i = 0, \exists m: P_i^m \subseteq Q_i$)
 $\Rightarrow \text{Ann} x = P_i \setminus \{P_i \cdot x = 0\}$
 $y \in \text{Ann} x \Rightarrow yx = 0 \Rightarrow y \in Q_i \Rightarrow y \in P_i$

$I = Q_1 \cap \dots \cap Q_n$ reduced primary representation $\Rightarrow \{P_i = \sqrt{Q_i}\} = \text{Ass}(R/I)$
 Theorem: If $P_i \in \text{Min}(R/I) \Rightarrow Q_i$ is uniquely determined.
 Example: $(xy, x^2) = I$  $\text{Ass}(R/I) = \{(x), (x, y)\}$

Primary decomposition can be done by computer algebra: - Macaulay 2
 - Singular

Proof: $P_i \in \text{Min}(R/I)$; $I = Q_1 \cap \dots \cap Q_n \mid \mathcal{O}_R/P_i$ minimally primary below P_i source!

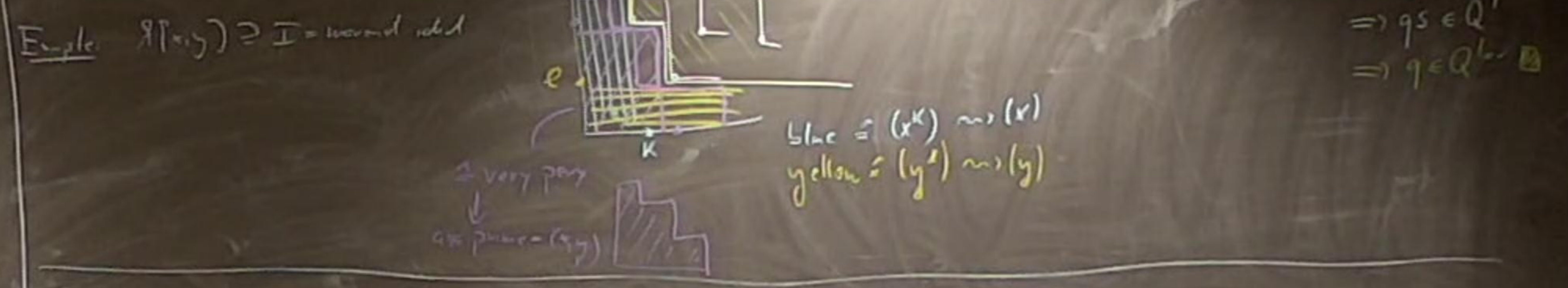
• (1) Q_i is s.t. $\{P_i \not\subseteq P_j\} \Rightarrow P_i \neq P_j$ $I \subseteq P_i$ sits minimally above P_i

$\Rightarrow Q_i \circ_R R_{P_i} = (R_{P_i})^{-1} Q_i = (1)$

because $Q_i \not\subseteq P_i \Rightarrow Q_i \not\subseteq P_i \Rightarrow \exists q \in Q_i, q \notin P_i \Rightarrow q \in \mathcal{O}_{R, P_i} \setminus P_i$
 becomes a unit after localization

$\Rightarrow I \circ R_{P_i} = Q_i \circ R_{P_i} = (Q_i)_{P_i} = (R_{P_i})^{-1} Q_i \Rightarrow \text{not (yet) the } Q_i, \text{ but } Q_i \circ R_{P_i} \text{ is uniquely det.}$

Remark to show: $Q, Q' = P$ -primary, $[Q_P - Q'_P \xrightarrow{?} Q - Q']$
 Proof: Let $q \in Q \setminus Q'$ $\Rightarrow q \in Q_P = Q'_P \Rightarrow \exists q' \in Q' : q = \frac{q'}{s}$ $\Rightarrow qs - q' \in Q'$
 $\Rightarrow qs - q' = 0 \Rightarrow qs = q' \Rightarrow qs \in Q' \Rightarrow q \in Q'$



⑥ Integral ring extensions

R w/out zero-div. = integral domain
 $R \subseteq B$ ring, $b \in B$. b is called integral over A if

\exists equation $1 \cdot b^n + a_1 b^{n-1} + \dots + a_{n-1} b + a_n = 0$ $| a_i \in A$
 $(a_n = 1)$

Example: $\mathbb{Z} \subseteq \mathbb{R}$: $\sqrt{2}$ is integral over \mathbb{Z} : $\sqrt{2}^2 - 2 = 0$
 $a_1 = -2$ ($\in \mathbb{Z}$)

$\sqrt{2}$ is not integral because it is transcendental over \mathbb{Q} , i.e. $\exists a_0 \neq 0, \dots, a_n = 0$ will $a_i \in \mathbb{Z}$

$\frac{1}{2} \in \mathbb{R}$ is not integral: $(\frac{1}{2})^n + a_1 (\frac{1}{2})^{n-1} + \dots + a_n = 0$ ($a_i \in \mathbb{Z}$)

$(\cdot 2^n) \Rightarrow 1 + 2a_1 + 4a_2 + \dots + 2^n a_n = 0$

(≤ 1 , $2 \cdot (\frac{1}{2})^n - 1 = 0$) even

Def: $R = \text{domain}$. $R =$ integrally closed in $\text{Quot } R =$ "normal" \Leftrightarrow If $r \in \text{Quot } R$ is integral over R then $r \in R$.

Proposition: $R =$ factorial domain (e.g. $R =$ principal ideal domain)

Proof: Let $r = \frac{a}{b} \in \text{Quot } R$ with $\text{gcd}(a, b) = 1$.
 $a^n + c_1 a^{n-1} b + \dots + c_n b^n = 0$ ($c_i \in R$) $/ \cdot b^n$
 $a^n + c_1 a^{n-1} b + \dots + c_n b^n = 0 \Rightarrow b \mid a^n$
 divide by b

Example: $\mathbb{Z}[\sqrt{5}] \supseteq \mathbb{Z}$ $d = \frac{\sqrt{5}+1}{2} \Rightarrow 2d = \sqrt{5} + 1$
 $\Rightarrow (2d-1)^2 = 5 \Rightarrow 4d^2 - 4d + 1 = 5 \Rightarrow 4d^2 - 4d - 4 = 0 \Rightarrow d^2 - d - 1 = 0$ d is integral over \mathbb{Z} !

$A \subseteq B$ no $\overline{A}^{(B)} := \{b \in B \mid b \text{ integral over } A\} \Rightarrow A \subseteq \overline{A}^{(B)} \subseteq B$

how to show: $\exists b^n + a_1 b^{n-1} + \dots + a_n = 0$ $\left\{ \begin{array}{l} a_i, a'_i \in A, b, c \in B \\ c^n + a'_1 c^{n-1} + \dots + a'_n = 0 \end{array} \right. \xrightarrow{?} (bc)^n + \dots = 0$
 \mathbb{Q} . Is this a solution? (YES)

Proposition Let $A \subseteq B$, $b \in B$. Then d.f.c.e:

- b is integral over A
- $A \subseteq A[b] \subseteq B$
- \exists finite A -algebra C : $A \subseteq A[b] \subseteq C \subseteq B$.
- \exists (f.g.) $A[b]$ -module M such that:
 - M is f.g. as an A -module
 - $\text{Ann}_{A[b]} M = 0$

$A[b]$ is finite A -algebra (i.e. is an A -algebra which is f.g. as an A -module)

Proof (1) \rightarrow (2) $b^n + a_{n-1}b^{n-1} + \dots + a_1b + a_0 = 0$
 Claim: $A[b]$ is gen. by $1, b, b^2, \dots$ as an A -module
 (Know: $A[b]$ is gen. by b as A -algebra)
 \rightarrow is gen. as an A -module by $\{1, b, b^2, \dots\}$

(eg: $\mathbb{Z}[x] =$ f.s. \mathbb{Z} -algebra / \neq finite \mathbb{Z} -algebra
 gen. set as a module $\{x^i \mid i \in \mathbb{N}\}$
 $\mathbb{Z}[b]$ is a f.s. \mathbb{Z} -algebra // generators: $\{1, \sqrt{5}\}$
 $\{a+b\sqrt{5}\}$)

(4) \Rightarrow (1) Cayley-Hamilton: $M = \text{f.s. } R\text{-module}$, $\varphi: M \rightarrow M \Rightarrow \exists f(x) \in R[x]$, highest coeff = 1, $f(\varphi) = 0$
 $M = M$, $R = A$, $\varphi = (\cdot b) \Rightarrow M \xrightarrow{b} M \Rightarrow f(x) \in A[x]$, highest coeff = 1, $f(b) = 0$ as a hom. $M \rightarrow M$
 $f(b) = 0 \in A[b] \leftarrow \text{e.g. } \forall m \in M, f(b) \cdot m = 0 \in M$ i.e. $f(b) \in \text{Ann}_{A[b]} M$

Corollary $b, b' \in B \supseteq A$
 If b, b' integral over $A \Rightarrow A[b] = \text{f.s. } A\text{-module}$, $A[b'] = \text{f.s. } A\text{-module} \Rightarrow A[b, b'] = \text{f.s. } A[b]\text{-module}$
 $A[b, b'] = \text{f.s. } A\text{-module}$

Proof $A[b] = A x_1 + \dots + A x_k$, $A[b, b'] = A[b] y_1 + \dots + A[b'] y_l$
 $A[b, b'] = \sum_{i=1, k}^{j=1, l} (x_i y_j) \cdot A$
Corollary $A \subseteq B$, b is integral over A , C is integral over $A[b]$ $\Rightarrow C$ is integral over A .
Def. $A \subseteq B$ is called integral \iff all elements of B are integral over A .
Remark: $A \rightarrow B$ integral \rightarrow [f.g. as algebra \iff finite algebra]

Theorem Let $A \subseteq B$ be integral

- $A \subseteq B$ be domains. Then $A = \text{field}$ iff $B = \text{field}$.
- $Q \subseteq B$ is maximal $\iff Q \cap A$ is maximal.

Proof (1) \Rightarrow Let $b \in B$, good: $\frac{1}{b} \in B$
 $b^n + a_{n-1}b^{n-1} + \dots + a_0 = 0 \mid \cdot \frac{1}{b}$ inside Q of B
 $b^{n-1} + \dots + a_1 + a_0/b = 0 \Rightarrow \frac{a_0}{b} \in B$ and $a_0 \neq 0$
 $\frac{1}{a} \in Q \cap A \subseteq Q \cap B = B \Rightarrow \frac{1}{a} = \text{integral over } A \Rightarrow \left(\frac{1}{a}\right)^n + a_1 \left(\frac{1}{a}\right)^{n-1} + \dots + a_0 \left(\frac{1}{a}\right) = 0$
 $\Rightarrow \frac{1}{a} \in A$ and $A = \text{field}$!

(2) $A \rightarrow B \rightsquigarrow A \rightarrow B \rightarrow B/Q$
 $\rightsquigarrow A/A \cap Q \rightarrow B/Q$
 $(\cdot a^{-1}) = \frac{1}{a} + a_1 + a_2 a + \dots + a_0 a^{n-1} = 0$
 $\in A$

Theorem (3) Φ is injective in chains, i.e. if $Q_1 \subseteq Q_2$ (in $\text{Spec } B$), $Q_1 \cap A = Q_2 \cap A \Rightarrow Q_1 = Q_2$.

Proof $P = Q_1 \cap A = Q_2 \cap A$ localize everything by $S = (A \setminus P)$
 $A \rightsquigarrow A_P$, $B \rightsquigarrow S^{-1}B$
 $A_P \rightarrow S^{-1}B$ still integral, i.e. $\otimes_{A_P} A_P$
 $[P = \text{max}] \quad (Q_1 \subseteq Q_2) \xrightarrow{(2)} Q_1, Q_2 = \text{both maximal}$
 $\Rightarrow Q_1 = Q_2$

Theorem (4) ("going up theorem") Φ is surjective: $\text{Spec } B \rightarrow \text{Spec } A$
 $Q_2 \supseteq Q_1 \Rightarrow \exists Q_2 \supseteq Q_1: Q_2 \cap A = P_2$

(5) "going down + 1" $A, B = \text{domains}$, $A = \text{local}$
 \Rightarrow similarly for $Q_2 \supseteq Q_1$
Proof (4) 1st case: $(A, m) = \text{local max}$; $P_2 = m$, choose some max. ideal $Q_2 \supseteq Q_1 \rightsquigarrow Q_2 \cap A = \text{max. id. in } A \Rightarrow m$
 gen. case: $S = (A \setminus P_2) \rightsquigarrow$ localize.