Def R ring, R' R-algebra, $x \in R'$ integral$/R$ $\iff$ $x^n + a_1 x^{n-1} + \dots + a_n = 0$, $a_i \in R$

R' integral$/R$ $\iff$ $\forall x \in R'$, integral$/R$

Analogue: Algebraic extensions of fields

Proposition

R ring, $R' \ni x$ R-algebra. TFAE:

1) x integral$/R$ (deg n)

2) $R[x]$ is gen. as an R-module by $1, x, \dots, x^{n-1}$

3) x lies in a subalg. of R' gen. as R-module by n elements

4) $\exists$ faithfull $R[x]$-module M gen. over R by n elements

Pf. 1) $\Rightarrow$ 2) Suppose $p(x) = 0$ and $f(x) \in R[x]$. By division algorithm $f(x) = q(x)p(x) + r(x)$, where deg $r(x) <$ deg $p(x) = n$. $\Rightarrow f(x) \in \langle 1, \dots, x^{n-1} \rangle$.

2) $\Rightarrow$ 3) $R[x] \subset R'$.

3) $\Rightarrow$ 4) $M = R[x]$. Then $xM = 0 \Rightarrow x \cdot 1 = x = 0$

4) $\Rightarrow$ 1) Let $\varphi = \mu_x : M \xrightarrow{x} M$. Cayley-Hamilton $\Rightarrow$ $P_M(\varphi) = 0$

i.e. $P_M(x) = 0 \Rightarrow x$ integral$/R$.

Notice

R ring, R' R-alg fin. gen R-module, M fin. gen R'-module $\Rightarrow$ M fin. gen R-module

Tower Law of Integrality

R ring, R' R-algebra integral/R, $R'' \ni x$ R'-algebra, x integral/R' $\Rightarrow$ x integral/R

Pf. $p(x) = x^n + a_1 x^{n-1} + \dots + a_n = 0$, $a_i \in R'$ $\Rightarrow$ $R[a_0, \dots, a_n] \subset R'$

$\Rightarrow$ a_n integral/$R[a_0, \dots, a_{n-1}]$ $\Rightarrow$ $R[a_0, \dots, a_n]$ gen/$R[a_0, \dots, a_{n-1}]$

by $1, a_n, a_n^2, \dots, a_n^r$. By induction $R[a_0, \dots, a_n]$ is fin. gen/R

But x integral/$R[a_0, \dots, a_n]$ $\Rightarrow$ $R[a_0, a_n](x)$ fin. gen/$R[a_0, \dots, a_n]$

R — $R[a_0, \dots, a_n]$ fin. gen/R — $R[a_0, \dots, a_n][x]$ fin. gen/$R[a_0, \dots, a_n]$

$\Rightarrow$ $R[a_0, \dots, a_n](x)$ fin. gen/R

$\Rightarrow$ x integral/R

Definition

R ring, R' R-algebra

$$R \subset \overline{R} \subset R'$$

$\overline{R} = \{x \in R' \mid x \text{ integral}/R\}$

integral closure of R in R'

If $R = \overline{R}$, R is integrally closed in R'

R domain, $R' = \mathrm{Frac}(R)$, then $\overline{R}$ is the normalization of R

If $R = \overline{R}$: R normal.

Teorem (Gauss)

R UFD $\Rightarrow$ R normal

Pf. $x = \frac{r}{s} \in \mathrm{Frac}(R)$ $(\gcd(r,s)=1)$. Suppose $x^n + a_1 x^{n-1} + \dots + a_0 = \frac{r^n}{s^n} + a_1 \frac{r^{n-1}}{s^{n-1}} + \dots + a_0 = 0$

$\Rightarrow$ $r^n = -a_1 r^{n-1} s - a_2 r^{n-2} s^2 - \dots - a_n s^n$

$= s(-a_1 r^{n-1} - \dots - a_n s^{n-1})$ $\Rightarrow$ s unit in R

$\Rightarrow$ $\frac{1}{s} \in R \Rightarrow x \in R$.

<u>Ex.</u>

$$R = k[t^2, t^3] \subset k[t] \Rightarrow \mathrm{Frac}(R) \subset \mathrm{Frac}(k[t]) = k(t)$$

$$\Rightarrow \mathrm{Frac}(R) \ni \frac{t^3}{t^2} = t \Rightarrow k[t] \subset \mathrm{Frac}(R) \Rightarrow k(t) \subset \mathrm{Frac}(R)$$

$$\Longrightarrow \mathrm{Frac}(R) = k(t).$$

(*) t integral $/R$; $p(t) = 0$ where $p(x) = x^2 - t^2$.

(**) $k[t]$ normal since it is a UFD.

$$\begin{tikzcd} & k[t] \arrow[r, hook, "*"] \arrow[dr, Rightarrow] & \bar{R} \\ R \arrow[ur, hook] \arrow[dr, hook] & & k[t] \\ & \bar{R} \arrow[ur, hook] & \end{tikzcd} \Longrightarrow \underline{\bar{R} = k[t]}$$

Notation

$$\begin{array}{lll} R' & R\text{-algebra} \supseteq \mathfrak{q} & \text{prime} \\ \varphi \uparrow & & \\ R & \supset \mathfrak{p} & \text{prime} \end{array}$$

$\mathfrak{q}$ lies over $\mathfrak{p}$ if $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$.

Remark: 1) $\forall \mathfrak{q}$, $\exists \mathfrak{p}$ s.t. $\mathfrak{q}$ lies over $\mathfrak{p}$

2) Many primes can lie over the same ideal

Special for integral extensions!

$\mathfrak{p} \subseteq R \hookrightarrow R' \supset \mathfrak{q}', \mathfrak{p}'$
prime, integral extension, primes

$\mathfrak{a}' \subset R'$ arbitrary ideal

1) Let $\mathfrak{p}'$ lie over $\mathfrak{p}$. Then $\mathfrak{p}'$ max iff $\mathfrak{p}$ max

2) If $\mathfrak{p}', \mathfrak{q}'$ lie over $\mathfrak{p}$, then $\mathfrak{p}' = \mathfrak{q}'$

3) $\exists\, \mathfrak{r}' \subset R'$ prime lying over $\mathfrak{p}$

Going up: 4) Suppose $\mathfrak{a}' \cap R \subset \mathfrak{p}$. Then in 3) we can take $\mathfrak{r}'$ to contain $\mathfrak{a}'$.

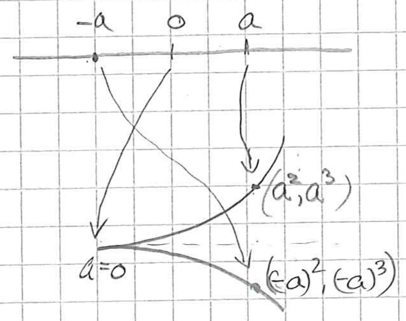
Illustration:

$$\begin{array}{ccccccc}
R' & \mathrm{Spec}(R') & \mathfrak{p}' & \max & \mathfrak{p}' \nearrow \mathfrak{q}' & \exists\, \mathfrak{r}' & \mathfrak{a}' \subset \mathfrak{r}' \\
\uparrow & \downarrow & \downarrow & \Updownarrow & \searrow \ \swarrow \ \Rightarrow \mathfrak{p}' = \mathfrak{q}' & \downarrow & \downarrow \\
R & \mathrm{Spec}(R) & \mathfrak{p} & \max, & \mathfrak{p} & \mathfrak{p}, & \mathfrak{a}' \cap R \subset \mathfrak{p}
\end{array}$$

$\underbrace{\max, \ \mathfrak{p}}_{\text{preserves dimension}}$, surjective

Ex.

$$\begin{array}{c}
k[t] \\
\uparrow \varphi \\
k[x,y]/(y^2 - x^3) \simeq k[t^2, t^3]
\end{array}$$



$$\varphi^{-1}(t-a) = (x - a^2, y - a^3) = (t^2 - a^2, t^3 - a^3)$$

$$\varphi(t^2 - a^2, t^3 - a^3) \subset k[t]$$

$$t^3 - a^3 = (t-a)(t^2 + at + a^2), \quad t^2 - a^2 = (t+a)(t-a)$$

$$\Rightarrow \varphi(t^2 - a^2, t^3 - a^3) = (t-a)$$

Pf. **Lemma:** $R \hookrightarrow R'$ integral extension : R field $\iff$ R' field (alg ext)

Pf. If R' field, $0 \neq x \in R \Rightarrow \frac{1}{x} \in R'$. By integrality

$$\left(\tfrac{1}{x}\right)^n + a_1 \left(\tfrac{1}{x}\right)^{n-1} + \dots + a_n = 0$$
$$\Downarrow$$
$$\frac{1}{x} = -a_1 - a_2 x - \dots - a_n x^{n-1} \in R$$

If R field, $y \in R'$. By integr.

$$y^m + b_1 y^{m-1} + \dots + b_m = 0 \quad , b_m \neq 0$$
$$\Downarrow$$
$$y(y^{m-1} + b_1 y^{m-2} + \dots + b_{m-1}) = -b_m$$
$$\Rightarrow \quad y^{-1} \in R'.$$

1)
$$\begin{array}{ccccc} R' & & R'/\mathfrak{p}' & & \text{field} \\ \uparrow & \Rightarrow & \uparrow & & \Updownarrow \\ R & & R/\mathfrak{p} & & \text{field} \\ \text{integral} & & \text{integral} & & \end{array}$$

2) $S = R - \mathfrak{p}$.
$$\begin{array}{ccc} R' & \to & S^{-1}R' \\ \uparrow & & \uparrow \\ R & \to & S^{-1}R \end{array}$$
injective integral (loc. preserves inject. and integr.)

$$\mathfrak{p}' S^{-1}R' \quad \mathfrak{q}' S^{-1}R'$$

$\Rightarrow$

$$\mathfrak{p} S^{-1}R \ \text{max}$$

$\Rightarrow \mathfrak{p}' S^{-1}R' = \mathfrak{q}' S^{-1}R'$ max

$\Rightarrow \mathfrak{p}' = \mathfrak{q}'$

3) $S^{-1}R' \supset \underline{m}$ max ideal

$\uparrow$

local $S^{-1}R \supseteq \mathfrak{p} S^{-1}R$ max

But $\underline{m} \cap S^{-1}R = \mathfrak{p} S^{-1}R$ (by 1) and loc.)

4)
$$\begin{array}{c} R'/\mathfrak{q}' \\ \uparrow \\ R/\mathfrak{q}' \cap R \end{array}$$
Apply 3).

Ex. $R = \mathbb{Z}[\sqrt{d}] = \mathbb{Z}[x]/(x^2-d) = \mathbb{Z}\cdot 1 + \mathbb{Z}\, x$, $x^2 = d \in \mathbb{Z}$, d square-free

Assume $d \equiv 1 \pmod 4$, $x = \frac{1}{2}(1+\sqrt{d})$ $\left(\frac{d-1}{4} = q\right)$

1) x integral $/R$

$$\begin{array}{rrcl} 1 & x^2 & = & \frac{1}{4}(1+\sqrt{d})^2 = \frac{1}{4}(1+2\sqrt{d}+d) = \frac{1+d}{4} + \frac{1}{2}\sqrt{d} \\ -1 & x & = & \frac{1}{2} + \frac{1}{2}\sqrt{d} \\ -\frac{d-1}{4} \in \mathbb{Z} & 1 & = & 1 \\ \hline & & & 0 \end{array}$$

i.e. $p(x) = x^2 - x - \frac{d-1}{4} = 0$

2) $\frac{1}{2}(1+\sqrt{d}) \notin R$

3) $\frac{1}{2}(1+\sqrt{d}) = \dfrac{a+b\sqrt{d}}{c+e\sqrt{d}}$

means $c + e\sqrt{d} + c\sqrt{d} + ed = 2a + 2b\sqrt{d}$

or $c + ed = 2a$, $e + c = 2b$

$d = 4q+1 \Rightarrow \frac{d+1}{2} = \frac{4q+2}{2} = 2q+1$

Put $c = e = 1$, then $a = \frac{d+1}{2} \in \mathbb{Z}$ $b = \frac{1}{2}(e+c) = \frac{1}{2}2 = 1$

$\Rightarrow \frac{1}{2}(1+\sqrt{d}) = \dfrac{2q+1+\sqrt{d}}{1+\sqrt{d}} \in \mathrm{Frac}(R)$.

$\Rightarrow$ R is not normal.

Ex. $x \in R$ nilpotent $\Rightarrow$ $1+x$ unit $\qquad 1 = 1 + x^n = (1+x)(1 - x + x^2 - \cdots + x^{n-1})$

$\Downarrow$

$x^n = 0$ for some odd n.

x nilpotent, u unit $\Rightarrow$ $u^{-1}x$ nilpotent $\qquad (u^{-1}x)^n = u^{-n}\cdot x^n = 0$

$\Rightarrow$ $\underset{\text{unit}}{1 + u^{-1}x} = u^{-1}\underset{\text{unit}}{(u+x)}$.

Dimension of a ring:

Ex $R = k[x,y]$: $\quad (x-a,\ y-b)$ max ideal

$k = \bar{k}$ field

$$\begin{array}{ll} (x-a,\ y-b) & \text{max ideal} \\ \cup & \\ (f(x,y)) & \text{irr. polynomial (prime ideal)} \\ \cup & \\ (0) & \end{array}$$

$\operatorname{Dim} R = 2$.

In general $\quad \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \dots \subsetneq \mathfrak{p}_n \subseteq R$

max chain of nested primes.

$\Rightarrow \dim R = n$.

$\Rightarrow$ Integral extensions preserve dimension