Contents

0. Motivation: A glimpse of Algebraic Geometry

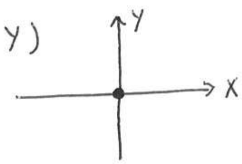
k algebraically closed field ($\mathbb{C}, \overline{\mathbb{Q}}, \overline{\mathbb{F}}_p, \dots$)

<u>Def</u> Consider the <u>affine n-space</u> $\mathbb{A}^n(k) := k^n$.

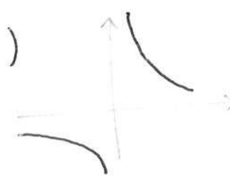
An <u>algebraic subset</u> of $\mathbb{A}^n(k)$ is a set of the form
$$V(f_1, \dots, f_m) := \{ \underline{a} = (a_1, \dots, a_n) \in k^n \mid f_i(\underline{a}) = 0 \ \forall i = 1, \dots, m \}$$
cut out by polynomials $f_1, \dots, f_m \in R := k[X_1, \dots, X_n]$.

<u>Ex</u> <u>$n=1$:</u> Proper alg. subsets of $\mathbb{A}^1(k)$ are precisely the finite sets.

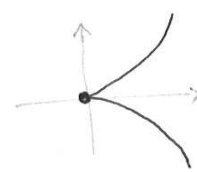
<u>$n=2$:</u> • $V(XY) = V(X) \cup V(Y)$



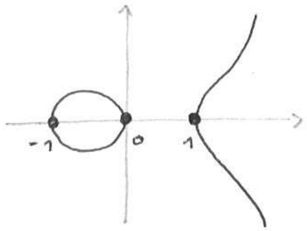
• $V(XY-1)$



• $V(Y^2 - X^3)$



• $V(Y^2 - X(X-1)(X+1))$



etc.

<u>Remark</u> • The choice of $f_1,\dots,f_m$ is ambiguous,

$V := V(f_1,\dots f_m)$ only depends on the ideal

$J := (f_1,\dots,f_m) \trianglelefteq R$.

• The latter is still ambiguous: $V(J)=V(J^N)\ \forall N\in\mathbb{N}$.

$\Longrightarrow$ no smallest possible choice,

but $\exists$ natural biggest choice:

take $J := \mathcal{J}(V) := \{ f\in R \mid f(\underline{a})=0\ \forall\, \underline{a}\in V\}$.

Let's call ideals of this form "<u>vanishing ideals</u>".

<u>Thm</u> The assignment

$$\left\{\begin{matrix}\text{algebraic}\\ \text{subsets of } \mathbb{A}^n(k)\end{matrix}\right\} \xrightarrow{\sim} \left\{\begin{matrix}\text{vanishing}\\ \text{ideals in } k[X_1,\dots,X_n]\end{matrix}\right\}$$

$$\begin{matrix} \text{\rotatebox{90}{$\in$}} & & \text{\rotatebox{90}{$\in$}} \\ W & \longmapsto & \mathcal{J}(W) \end{matrix}$$

is a bijection.

Pf. Surjective by def^n of "vanishing ideal".

Injective: Let $W \subseteq \mathbb{A}^n(k)$ be algebraic,

then we claim

$$\boxed{W = V(\mathcal{J}(W))}$$

Indeed

$$V(\mathcal{J}(W)) = \{\underline{a}\in k^n \mid f(\underline{a})=0\ \forall f\in \mathcal{J}(W)\}$$

$$= \{\underline{a}\in k^n \mid f|_W\equiv 0 \text{ implies } f(\underline{a})=0\}$$

$$= W$$

"$\supseteq$" trivial

"$\subseteq$": Let $\underline{a}\notin W$ and put $W = V(J)$ with $J \trianglelefteq k[X_1,\dots,X_n]$,

then $\exists f\in J$ with $f(\underline{a})\neq 0$ by def^n of $V(J)$,

but obviously $J\subseteq \mathcal{J}(V(J))$, hence $f|_W\equiv 0$. $\square$

<u>Ex</u> $\underline{a}\in k^n$, $W=\{\underline{a}\}$ $\Longrightarrow$ $\mathcal{J}(W) = (X_1-a_1,\dots,X_n-a_n) =: \mathfrak{m}_{\underline{a}}$.

<u>Note</u> $\mathfrak{m}_{\underline{a}} \trianglelefteq R = k[X_1,\dots,X_n]$ is a maximal ideal

since $R/\mathfrak{m}_{\underline{a}} \cong k$.

We'll see later that <u>all</u> max. ideals of R arise

like this ($\rightarrow$ "Hilbert's Nullstellensatz").

Also, vanishing ideals are precisely the so-called "<u>radical ideals</u>"...

Upshot: Geometry $\rightsquigarrow$ Algebra
(hard) (much easier)

$$\begin{array}{ccc} \mathbb{A}^n(k) & \xrightarrow{\ \sim\ } & \mathrm{Spm}(R) := \{\text{max. ideals of } R\} \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ \underline{a} & \longmapsto & \mathfrak{m}_{\underline{a}} \end{array}$$

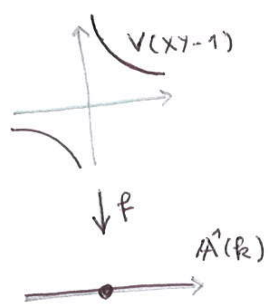
Note: Via this bijection,

$$V(J) \longmapsto \{\mathfrak{m} \in \mathrm{Spm}(R) \mid J \subseteq \mathfrak{m}\} \cong \mathrm{Spm}(R/J)$$

$\Longrightarrow$ Use algebra (theory of rings & their ideals) to do geometry!

Ex Intersections: $V(J) \cap V(\mathcal{J}) = V(J + \mathcal{J})$

Unions: $V(J) \cup V(\mathcal{J}) = V(J \cdot \mathcal{J}) = V(J \cap \mathcal{J})$



Ex Projection maps:

e.g. $f : V(XY-1) \longrightarrow \mathbb{A}^1(k)$
$\underline{a} = (a_1, a_2) \longmapsto a_1$

corresponds to the ring homomorphism

$$\tilde{R} := k[X,Y]/(XY-1) \xleftarrow{\ f^*\ } R := k[X]$$

(via $f = \mathrm{Spm}(f^*)$)

Note that f is not surjective, but induces a bijection $f : V(XY-1) \xrightarrow{\ \sim\ } \mathbb{A}^1(k) \setminus \{0\}$.

Algebraically, $f^* : R \longrightarrow \tilde{R}$ is not a ring isomorphism but becomes so after inverting the element $X \in R$:

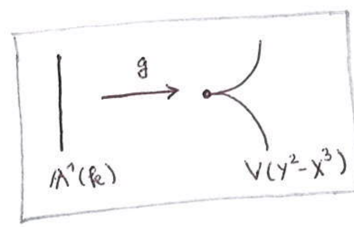
Since $f^*(X) \in \tilde{R}^*$ is a unit, we have a factorization

$$\begin{tikzcd} R \arrow[r, "f^*"] \arrow[d] & \tilde{R} = k[X,Y]/(XY-1) \\ R[\tfrac{1}{X}] = k[X, \tfrac{1}{X}] \arrow[ur, dashed, "\exists!\ \text{iso}"'] & \end{tikzcd}$$

"Localization of R at the multiplicative set $S := \{1, X, X^2, \ldots\}$"

Ex Resolution of singularities:

e.g. $g : \mathbb{A}^1(k) \longrightarrow V(Y^2 - X^3)$
$t \longmapsto (t^2, t^3)$



corresponds to

$$\begin{array}{ccc} k[T] & \xleftarrow{\ g^*\ } & k[X,Y]/(Y^2-X^3) \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ P(T^2, T^3) & \longleftarrow\!\shortmid & P(X,Y) \bmod (Y^2-X^3) \end{array}$$

(via $g = \mathrm{Spm}(g^*)$)

(etc.)

Grothendieck:

Why only consider $k[X_1, \dots, X_n]/J$ with $\begin{cases} k \text{ alg closed field} \\ J \text{ radical ideal} \end{cases}$?

Try the same for arbitrary commutative rings R !

Rem. a) In general a ring homom. $f: R \to S$ does NOT induce $f^*: \operatorname{Spm} S \not\to \operatorname{Spm} R$

usually $f^{-1}(m) \trianglelefteq R$ is not maximal for $m \in \operatorname{Spm} S$.

But we do get $f^*: \operatorname{Spec} S \to \operatorname{Spec} R := \{\text{prime ideals of } R\}$,

ie $f^{-1}(\mathfrak{p}) \trianglelefteq R$ is prime $\forall \mathfrak{p} \in \operatorname{Spec} S$.

$\Longrightarrow$ work with $\operatorname{Spec} R$ instead of $\operatorname{Spm} R$, get many "new" points ("generic points")...

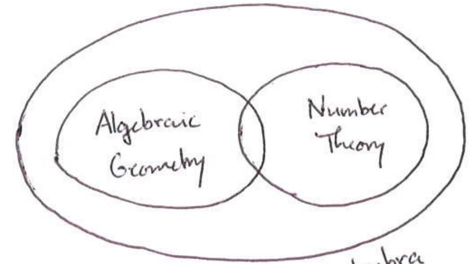
b) R may have nilpotents, eg $R = k[X]/(X^n)$

$\Longrightarrow$ get "functions" on $\operatorname{Spec} R$ that "vanish everywhere"

Taylor series up to n^{th} order

$\to$ view $\operatorname{Spec} R$ as n^{th} infinitesimal thickening of the point $\operatorname{Spec} k$...

$\Longrightarrow$ Very powerful & flexible language, eg. can study polynomial eq^{ns} over $\mathbb{Z}$ such as $x^n + y^n = z^n$ ...



commutative algebra

= study of rings, ideals & modules

Possible topics:

I. Rings and modules

II. Chain conditions

III. Integral extensions

IV. Primary decomposition

V. Dimension theory

VI. Homological algebra

⋮

(we won't be able to cover all of these in one semester)

I. Rings and Modules

1. Rings, ideals, homomorphisms

Def A monoid is a set R
w/ an operation $\cdot : R \times R \longrightarrow R$
which is

- associative: $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a,b,c \in R$,
- unital: $\exists\, 1 \in R$ with $1 \cdot a = a = a \cdot 1 \quad \forall a \in R$.

The monoid is commutative if $a \cdot b = b \cdot a \quad \forall a,b \in R$.

NB The element $1 \in R$ is determined uniquely and called the unit of the monoid $(R, \cdot)$.

Def A ring with unit is a set R endowed with two operations $+, \cdot : R \times R \to R$
sth

- $(R,+)$ is an abelian gp
  whose neutral element we denote by 0,

- $(R,\cdot)$ is a monoid
  whose unit we denote by 1,

- Distributivity holds:
  $$a\cdot(b+c) = a\cdot b + a\cdot c \quad \forall a,b,c \in R.$$

A ring $(R,+,\cdot)$ is called commutative
if the monoid $(R,\cdot)$ is so.

From now on, we use the convention

$$\boxed{\text{" ring := commutative ring with unit "}}$$

Def A zero divisor is an element $a \in R\setminus\{0\}$
w/ $a\cdot b = 0$ for some $b \in R\setminus\{0\}$.

We say R is an integral domain if it has no zero divisors
(and $1 \neq 0$).

The group of units is
$$R^* := \{a \in R \mid \exists b \in R \text{ with } a\cdot b = 1\}.$$

Ex.
- Any field K is an integral domain
  with $K^* = K\setminus\{0\}$.

- $R = \mathbb{Z}$ is an integral domain w/ $R^* = \{\pm 1\}$.

- $R = \mathbb{Z}[i] = \{a+bi \in \mathbb{C} \mid a,b \in \mathbb{Z}\}$
  is an integral domain w/ $R^* = \{\pm 1, \pm i\}$.

- If R is an integral domain, then so is the
  polynomial ring $S = R[X]$ w/ $S^* = R^*$.

- For $n \in \mathbb{N}$ we have:
  $$\mathbb{Z}/n\mathbb{Z} \text{ integral domain} \iff \mathbb{Z}/n\mathbb{Z} \text{ field} \iff n = p \text{ prime}$$

  and
  $$(\mathbb{Z}/n\mathbb{Z})^* = \{a \bmod n\mathbb{Z} \mid \gcd(a,n) = 1\}.$$

- With our convention, for $n > 1$ and $R \neq \{0\}$
  the matrix ring $\mathrm{Mat}_{n\times n}(R)$ is not a ring
  (not commutative!)

- We do allow the zero ring $R = \{0\}$ where $1 = 0$,
  but by def^n this is not an integral domain...

The class of rings is a category w/ the obvious notion of morphisms:

<u>Def</u> A <u>homomorphism</u> between rings R and S is a map of sets $f: R \to S$ which is both a group homomorphism for "+" and a monoid — " — "$\cdot$"

i.e. $\forall a, b \in R$,

- $f(a+b) = f(a) + f(b)$
- $f(a \cdot b) = f(a) \cdot f(b)$
- $f(1) = 1$ (don't forget this condition...)

Notation: $\mathrm{Hom}(R,S) := \{ f: R \to S \text{ ring hom.} \}$,

$\mathrm{End}(S) := \mathrm{Hom}(S,S)$ "<u>endomorphisms</u>"

We say f is a

- <u>monomorphism</u> if f is injective
- <u>epimorphism</u> — " — surjective
- <u>isomorphism</u> — " — bijective.

<u>Rem.</u> a) The category of rings has initial object $\mathbb{Z}$ and terminal object the zero ring $\{0\}$:

For any ring R, $\exists!$ homomorphisms

$$\mathbb{Z} \xrightarrow[\substack{\text{unique because} \\ \text{we imposed } 1 \mapsto 1.}]{} R \longrightarrow \{0\}.$$

b) Caution with the notion of epi:

If $f: R \to S$ is epi, then
$$\begin{aligned} \mathrm{Hom}(S,T) &\hookrightarrow \mathrm{Hom}(R,T) \\ g &\longmapsto g \circ f \end{aligned}$$
is injective for all rings T

but NOT conversely in general, consider for instance the inclusion $f: R = \mathbb{Z} \hookrightarrow S = \mathbb{Q}$.

However, for mono's we do have

$$f: R \to S \text{ mono} \iff \begin{aligned} \mathrm{Hom}(T,R) &\hookrightarrow \mathrm{Hom}(T,S) \\ g &\longmapsto f \circ g \end{aligned}$$
injective for all rings T

(exercise).

Most rings in Alg. Geometry + Number Theory arise from some base ring R by successively forming

- polynomial rings $R[X]$
- power series rings $R[\![X]\!]$
- quotient rings $R/\mathfrak{a}$ by ideals $\mathfrak{a} \trianglelefteq R$, etc.

Recall:

<u>Def</u> An <u>ideal</u> of a ring R is a subset $\mathfrak{a} \subseteq R$ which is

- an additive subgp: $a_1 + a_2 \in \mathfrak{a} \quad \forall a_1, a_2 \in \mathfrak{a}$
- stable under scalar multiplication:
$$ra \in \mathfrak{a} \quad \forall a \in \mathfrak{a},\ r \in R.$$

Notation: $\mathfrak{a} \trianglelefteq R$.

<u>Ex.</u> For $a_1, \dots, a_n \in R$ put $(a_1, \dots, a_n) := \{\sum_{i=1}^n a_i r_i \mid r_i \in R\} \trianglelefteq R$

Ideals of this form are called <u>finitely generated</u>.

For $n = 1$ we call $(a) = aR$ a <u>principal ideal</u>.

Trivial cases: $(0) = \{0\} \trianglelefteq R$ <u>zero ideal</u>
$(1) = R \trianglelefteq R$ <u>unit ideal</u>.

<u>Def</u> A <u>principal ideal domain</u> (PID) is an integral domain in which every ideal is principal.

<u>Ex.</u>
- $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $k[X]$ (k a field) are PID's (in fact Euclidean)
- $\mathbb{Z}[X]$ is NOT a PID (look at $\mathfrak{a} := (2, X)$)
- $\mathbb{Z}[\sqrt{-5}]$ is NOT a PID
(look at $\mathfrak{a} := (2, 1+\sqrt{-5})$ and use the norm map $N: \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$ ...)

<u>Rem.</u> Let $R := \mathbb{Z}[X_1, X_2, X_3, \dots]$ be the polynomial ring in ∞ many variables, then the ideal

$$\mathfrak{a} := (X_1, X_2, X_3, \dots)$$
$$:= \{\sum_{i=1}^N X_i \cdot f_i \mid f_i \in R,\ N \in \mathbb{N}\} \trianglelefteq R$$

is not finitely generated, because any finite number of generators would involve only finitely many of the variables.

We'll later focus on the class of <u>Noetherian rings</u> where such phenomena don't happen.

Back to quotients:

<u>Def</u> For ideals $\mathfrak{a} \trianglelefteq R$ consider the equivalence relation mod $\mathfrak{a}$ on R defined by

$$r \equiv s \bmod \mathfrak{a} \;:\Longleftrightarrow\; r - s \in \mathfrak{a}.$$

We endow

$$R/\mathfrak{a} := \{ r \bmod \mathfrak{a} \mid r \in R \}$$

with the ring structure

$$(r \bmod \mathfrak{a}) + (s \bmod \mathfrak{a}) := (r + s \bmod \mathfrak{a})$$
$$(\quad '' \quad) \cdot (\quad '' \quad) := (r \cdot s \bmod \mathfrak{a}),$$

ie the unique ring structure sth the quotient map $R \xrightarrow{\pi} R/\mathfrak{a}$ is a ring homomorphism.

<u>NB</u> Can recover the ideal as $\mathfrak{a} = \ker(\pi)$, where for any ring homomorphism $f: R \to S$ we define the <u>kernel</u> by

$$\ker(f) := \{ r \in R \mid f(r) = 0 \} \trianglelefteq R.$$

$\Rightarrow$ Ideals = kernels of ring homomorphisms,

and we have:

<u>Lemma.</u> Let $\mathfrak{a} \trianglelefteq R$. Then for any $f: R \to S$ with $\mathfrak{a} \subseteq \ker(f)$, $\exists!$ factorization

$$\begin{tikzcd} R \arrow[rr, "f"] \arrow[dr, two heads, "\pi"'] & & S \\ & R/\mathfrak{a} \arrow[ur, dashed, "\exists! \bar{f}"'] & \end{tikzcd}$$

Moreover,

$$\bar{f} \text{ monomorphism} \Longleftrightarrow \mathfrak{a} = \ker(f).$$

Pf. Uniqueness of $\bar{f}$ clear since $\pi: R \twoheadrightarrow R/\mathfrak{a}$ epi.

Existence of $\bar{f}$ clear since $\mathfrak{a} \subseteq \ker(f)$ means that $f(a)$ only depends on $a \bmod \mathfrak{a}$.

Finally $\ker(\bar{f}) = \ker(f)/\mathfrak{a} \trianglelefteq R/\mathfrak{a}$,
so $\bar{f}$ is mono iff $\mathfrak{a} = \ker(f)$. $\square$

<u>NB</u> $\{\text{Ideals in } R/\mathfrak{a}\} \xleftrightarrow{1:1} \{\text{Ideals in } R \text{ containing } \mathfrak{a}\}$

$$\mathfrak{b}/\mathfrak{a} \longleftrightarrow \mathfrak{b} \text{ with } \mathfrak{b} \supseteq \mathfrak{a}$$

2. The spectrum of a ring (Can you "see" algebra?)

Def An ideal $\mathfrak{a} \trianglelefteq R$ is called

- prime if $R/\mathfrak{a}$ is an integral domain
- maximal if $R/\mathfrak{a}$ is a field.

NB By our convention then in particular $\mathfrak{a} \neq (1)$ is not the unit ideal.

Notation: $\mathfrak{a} \underset{\neq}{\trianglelefteq} R$.

Ex. The prime ideals in $\mathbb{Z}$ are precisely the ideals $(p) \trianglelefteq \mathbb{Z}$ with p prime or $p = 0$, and all nonzero ones are maximal.

($\rightarrow$ outlook: $\dim(\mathbb{Z}) = 1$)

Ex. In $k[X,Y]$ (k field) one has a chain of prime ideals

$$(0) \trianglelefteq (X) \trianglelefteq (X,Y) \trianglelefteq k[X,Y],$$

of which only the last one is maximal.

($\rightarrow$ outlook: $\dim k[X,Y] = 2$)

Lemma A proper ideal $\mathfrak{a} \underset{\neq}{\trianglelefteq} R$ is

(a) prime iff $a, b \notin \mathfrak{a}$ implies $a \cdot b \notin \mathfrak{a}$.

(b) maximal iff it is not contained in any bigger proper ideal of R.

Pf.

For (a) write $\bar{a} := a \bmod \mathfrak{a} \in R/\mathfrak{a}$ etc.

then
$$\begin{aligned} a \in \mathfrak{a} &\iff \bar{a} = 0 \\ b \in \mathfrak{a} &\iff \bar{b} = 0 \\ a \cdot b \in \mathfrak{a} &\iff \overline{a \cdot b} = 0 \end{aligned}$$

For (b) note

$$\begin{aligned} R/\mathfrak{a} \text{ field} &\iff R/\mathfrak{a} \text{ has no nontrivial ideals} \\ &\iff (0) \trianglelefteq R/\mathfrak{a} \text{ maximal wrt inclusion of proper ideals} \\ &\iff \mathfrak{a} \trianglelefteq R \end{aligned}$$

$\square$

Notation:
$$\begin{aligned} \operatorname{Spec} R &:= \{\text{prime ideals } \mathfrak{p} \trianglelefteq R\} \\ &\cup \\ \operatorname{Spm} R &:= \{\text{maximal ideals } \mathfrak{m} \trianglelefteq R\} \end{aligned}$$

Why do we care?

① Number Theory:

Rings of algebraic integers such as $\mathbb{Z}[\sqrt{-5}]$ are usually not UFD's, e.g.

$$(1+\sqrt{-5})\cdot(1-\sqrt{-5}) = 2\cdot 3 \qquad (*)$$

irreducible in $\mathbb{Z}[\sqrt{-5}]$ but no two differ by a unit!

But: Any ideal in such a ring factors uniquely as a product of powers of prime ideals, e.g.

$$(2) = \mathfrak{p}^2$$
$$(3) = \mathfrak{q}\cdot\bar{\mathfrak{q}} \qquad \text{refines } (*)$$
$$(1+\sqrt{-5}) = \mathfrak{p}\cdot\mathfrak{q}$$
$$(1-\sqrt{-5}) = \mathfrak{p}\cdot\bar{\mathfrak{q}}$$

with
$$\left.\begin{aligned} \mathfrak{p} &:= (2, 1+\sqrt{-5}) \\ \mathfrak{q} &:= (3, 1+\sqrt{-5}) \\ \bar{\mathfrak{q}} &:= (3, 1-\sqrt{-5}) \end{aligned}\right\} \in \mathrm{Spm}(\mathbb{Z}[\sqrt{-5}]).$$

② Algebraic Geometry:

Let k be a field,

$\mathbb{A}^n(k) := k^n$ affine n-space,

$R := k[X_1, \dots, X_n]$ the ring of polynomial fct's on it.

$\Longrightarrow$ get a map

$$\begin{array}{ccc} \mathbb{A}^n(k) & \xrightarrow{\varphi} & \mathrm{Spm}(R) \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ x = (x_1, \dots, x_n) & \longmapsto & \mathfrak{m}_x := (X_1 - x_1, \dots, X_n - x_n) \end{array}$$

"ideal of functions vanishing at x"

(to see that $\mathfrak{m}_x \trianglelefteq R$ is maximal, note that $R/\mathfrak{m}_x \simeq k$ is a field).

We'll see later:

If k is algebraically closed, then φ is bijective!

($\to$ Hilbert's Nullstellensatz, chapter III)

Want to study algebraic varieties,

ie zero loci

$$V(f_1, \dots, f_m) := \{ x \in \mathbb{A}^n(k) \mid f_1(x) = \dots = f_m(x) = 0 \}$$

cut out by finitely many polynomials $f_1, \dots, f_m \in R$.

Clearly $V(f_1, \dots, f_m) = V(\mathfrak{a})$

only depends on the ideal $\mathfrak{a} := (f_1, \dots, f_m) \trianglelefteq R$

(in fact only on its radical $\sqrt{\mathfrak{a}}$, see later ...)

For k alg. closed we get:

$$\begin{tikzcd}
\mathbb{A}^n(k) \arrow[r, "\sim"] & \mathrm{Spm}(R) & \ni \mathfrak{m} = \pi^{-1}(\mathfrak{m}/\mathfrak{a}) \\
\cup & \cup & \\
V(\mathfrak{a}) \arrow[r, "\sim"] & \mathrm{Spm}(R/\mathfrak{a}) & \ni \mathfrak{m}/\mathfrak{a} \arrow[u]
\end{tikzcd}$$

$(\pi : R \twoheadrightarrow R/\mathfrak{a})$

with $\mathfrak{m} \trianglelefteq R$, $\mathfrak{a} \subseteq \mathfrak{m}$

... generalize:

$\Longrightarrow$ For **any** ring R,

want to view $\mathrm{Spm}(R)$ as a top. space

w/ closed subsets given by $\mathrm{Spm}(R/\mathfrak{a}) \subset \mathrm{Spm}(R)$

for ideals $\mathfrak{a} \trianglelefteq R$.

Q:
- $\mathrm{Spm}(R) \neq \emptyset$?
- topology ?
- functorial properties ?

Lemma Any ring $R \neq 0$ has a maximal ideal,

ie. $\mathrm{Spm}(R) \neq \emptyset$.

Pf. Recall Zorn's lemma:

> $I \neq \emptyset$ partially ordered set
> s.th. every totally ordered subset $J \subseteq I$
> has an upper bound in I
>
> $\Longrightarrow$ I contains a maximal element

Apply this to

$I := \{ \text{proper ideals } \mathfrak{a} \subsetneq R \}$

partially ordered by inclusion.

Assumptions of Zorn's lemma hold:

- $I \neq \emptyset$ since $(0) \in I$ (this uses $R \neq 0$!)
- $\mathfrak{J} \subseteq I$ totally ordered, wlog $\neq \emptyset$

$\Rightarrow \forall \mathfrak{a}, \mathfrak{b} \in \mathfrak{J}, \quad \mathfrak{a} \subseteq \mathfrak{b}$ or $\mathfrak{b} \subseteq \mathfrak{a}$

$\Rightarrow \mathfrak{c} := \bigcup_{\mathfrak{a} \in \mathfrak{J}} \mathfrak{a} \;\trianglelefteq_{\neq}\; R$ is a proper ideal:

Ideal since $\begin{matrix} a, b \in \mathfrak{c} \\ r \in R \end{matrix} \Rightarrow \exists\, \mathfrak{a}, \mathfrak{b} \in \mathfrak{J}: \begin{matrix} a \in \mathfrak{a} \\ b \in \mathfrak{b} \end{matrix}$

wlog $\mathfrak{a} \subseteq \mathfrak{b}$,
then $a, b \in \mathfrak{b}$
hence $a + b \in \mathfrak{b}$, $ra \in \mathfrak{b}$

$\Rightarrow a + b \in \mathfrak{c}$, $ra \in \mathfrak{c}$

Proper since $1 \in \mathfrak{c}$ would imply $1 \in \mathfrak{a}$ for some $\mathfrak{a} \in \mathfrak{J}$ $\lightning$

By construction $\mathfrak{a} \subseteq \mathfrak{c} \;\; \forall \mathfrak{a} \in \mathfrak{J}$,
i.e. $\mathfrak{c} \in I$ is an upper bound for $\mathfrak{J}$. $\square$

Cor. Any proper ideal $\mathfrak{a} \subsetneq R$ is contained in a maximal one.

Pf. Consider $\pi: R \twoheadrightarrow R/\mathfrak{a}$.
Let $\tilde{\mathfrak{m}} := \pi^{-1}(\mathfrak{m})$ for any $\mathfrak{m} \in \operatorname{Spm}(R/\mathfrak{a})$. $\square$

$\Rightarrow \tilde{\mathfrak{m}} \in \operatorname{Spm}(R)$ & $\mathfrak{a} \subseteq \tilde{\mathfrak{m}}$.

Caution: For arbitrary ring homomorphisms $f: R \to S$ and $\mathfrak{m} \in \operatorname{Spm}(S)$ usually $f^{-1}(\mathfrak{m}) \notin \operatorname{Spm}(R)$,
think of $f: \mathbb{Z} \hookrightarrow \mathbb{Q}$ and $\mathfrak{m} = (0) \trianglelefteq \mathbb{Q}$ ...

But still get prime ideals:

Lemma. $\operatorname{Spec}(-)$ is a functor on rings:
Any ring homom. $f: R \to S$ induces a
map

$$\begin{matrix} \operatorname{Spec}(S) & \longrightarrow & \operatorname{Spec}(R) \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ \mathfrak{p} & \longmapsto & f^{-1}(\mathfrak{p}) \end{matrix}$$

and these are compatible with composition.

Pf. For $\mathfrak{p} \in \mathrm{Spec}(S)$,

have
$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, two heads] & S \arrow[d, two heads] \\ R/f^{-1}(\mathfrak{p}) \arrow[r, hook, "\exists!"] & S/\mathfrak{p} \end{tikzcd}$$

$\leftarrow$ integral domain because $\mathfrak{p}$ prime.

monomorphism because $f^{-1}(\mathfrak{p}) = \ker(R \to S/\mathfrak{p})$

Subrings of integral domains are integral domains

$\Rightarrow$ $R/f^{-1}(\mathfrak{p})$ integral domain $\Rightarrow$ $f^{-1}(\mathfrak{p})$ prime. $\square$

Thus: Rather than $\mathrm{Spm}(R)$, should use $\mathrm{Spec}(R)$ to do geometry!

Def (a) For ideals $\mathfrak{a}_i \trianglelefteq R$ ($i \in I$ $\leftarrow$ any index set, may be infinite) put

$$\sum_{i \in I} \mathfrak{a}_i := \Big\{ \sum_{i\in I} a_i \;\Big|\; a_i \in \mathfrak{a}_i, \text{ almost all zero} \Big\}$$

$:=$ smallest ideal containing each $\mathfrak{a}_i$.

(b) For $\mathfrak{a}_1, \dots, \mathfrak{a}_n \trianglelefteq R$ put

$\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n :=$ ideal generated by the products $a_1 \cdots a_n$ with $a_i \in \mathfrak{a}_i$.

Lemma. $\exists!$ topology on the set $\mathrm{Spec}(R)$ whose closed sets are the subsets $\mathrm{Spec}(R/\mathfrak{a}) \subseteq \mathrm{Spec}(R)$ for $\mathfrak{a} \trianglelefteq R$.

Pf.

⓪ For $\mathfrak{a} \trianglelefteq R$ the map $\pi : R \twoheadrightarrow R/\mathfrak{a}$ induces an injective map
$$\begin{array}{ccc} \mathrm{Spec}(R/\mathfrak{a}) & \hookrightarrow & \mathrm{Spec}(R) \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ \mathfrak{p} & \longmapsto & \pi^{-1}(\mathfrak{p}) \end{array}$$

because $\mathfrak{p} = \pi(\pi^{-1}(\mathfrak{p}))$.

Denote by
$$V(\mathfrak{a}) := \{ \mathfrak{q} \in \mathrm{Spec}(R) \mid \mathfrak{a} \subseteq \mathfrak{q} \}$$
its image, and declare these subsets to be closed.

① Clearly $\mathrm{Spec}(R) = V((0))$, $\emptyset = V((1))$ are closed.

② Arbitrary intersections of closed subsets are closed:

$\mathfrak{a}_i \trianglelefteq R$ ($i \in I$)
$$\Rightarrow \bigcap_{i \in I} V(\mathfrak{a}_i) = \{ \mathfrak{p} \in \mathrm{Spec} R \mid \mathfrak{a}_i \subseteq \mathfrak{p} \ \forall i \} = V(\mathfrak{a})$$
for $\mathfrak{a} := \sum_{i \in I} \mathfrak{a}_i$.

③ Finite unions of closed subsets are closed:

$\mathfrak{a}, \mathfrak{b} \trianglelefteq R$

$$\Rightarrow \quad V(\mathfrak{a}) \cup V(\mathfrak{b}) = \{ \mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{a} \subseteq \mathfrak{p} \text{ or } \mathfrak{b} \subseteq \mathfrak{p} \}$$

$$= \{ \mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{p} \} = V(\mathfrak{a} \cdot \mathfrak{b}).$$

"$\subseteq$" obvious

"$\supseteq$" uses that $\mathfrak{p}$ is prime:

$\left.\begin{array}{l} a \in \mathfrak{a} \setminus \mathfrak{p} \\ b \in \mathfrak{b} \setminus \mathfrak{p} \end{array}\right\} \Rightarrow ab \in \mathfrak{a} \cdot \mathfrak{b} \setminus \mathfrak{p}$

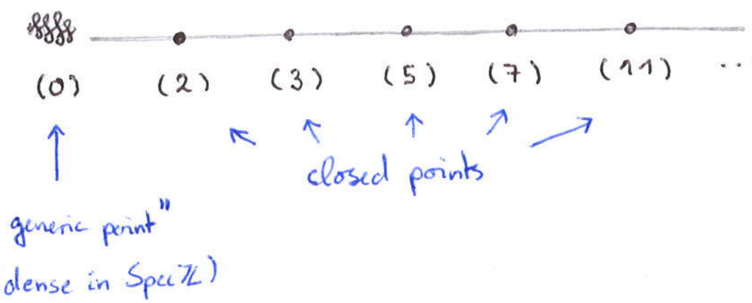
$\square$

The above topology is called the Zariski topology.

Rem. (a) We recover $\operatorname{Spm}(R) \subseteq \operatorname{Spec}(R)$ as the set of closed points in the Zariski topology (exercise). Thus using primes rather than maximal ideals leads to non-closed points (see pictures below)!

(b) The Zariski topology is not Hausdorff, e.g. any proper closed subset of $\operatorname{Spec}(\mathbb{Z})$ is finite!

Ex. (a) $\operatorname{Spec}(\mathbb{Z})$:



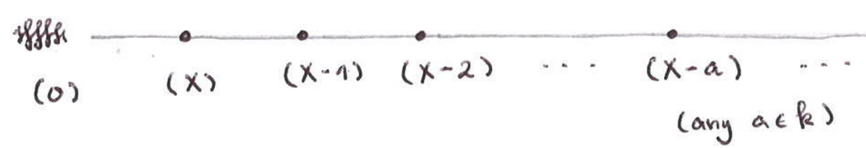
(b) $\operatorname{Spec} k[X]$, k a field:

Maximal ideals are all of the form $(f(X))$ w/ $f \in k[X]$ irreducible,

and the only non-maximal prime ideal is (0)

(use that $k[X]$ is a PID).

If k is alg. closed, then any irreducible polynomial has the form $f(X) = c \cdot (X-a)$ w/ $a \in k$, $c \in k^*$ and we get the affine line:



These are "1-dimensional" examples, similar picture for Spec R when R is any Dedekind domain (in case you know this from number theory).

Let's go one dimension up:

Ex Spec $k[X,Y]$ and Spec $\mathbb{Z}[Y]$:

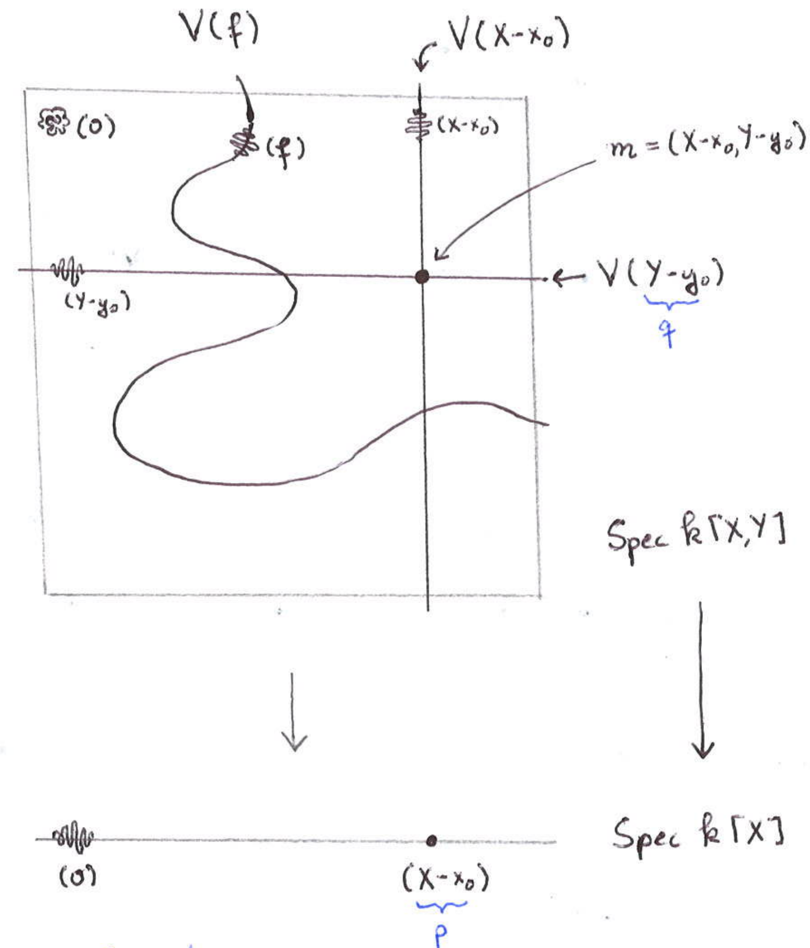
Let $A = k[X]$ or $A = \mathbb{Z}$ (or any other PID), then we have

Lemma. All prime ideals in $R = A[Y]$ are of the following form:

- (0)
- (f) for irreducible $f \in R$
- maximal ideals $m = (p, q)$
  where $p \in A$ is irreducible in A,
  $q \in R = A[Y]$ is a polynomial whose reduction $\bar{q} \in (A/(p))[Y]$ is irreducible.

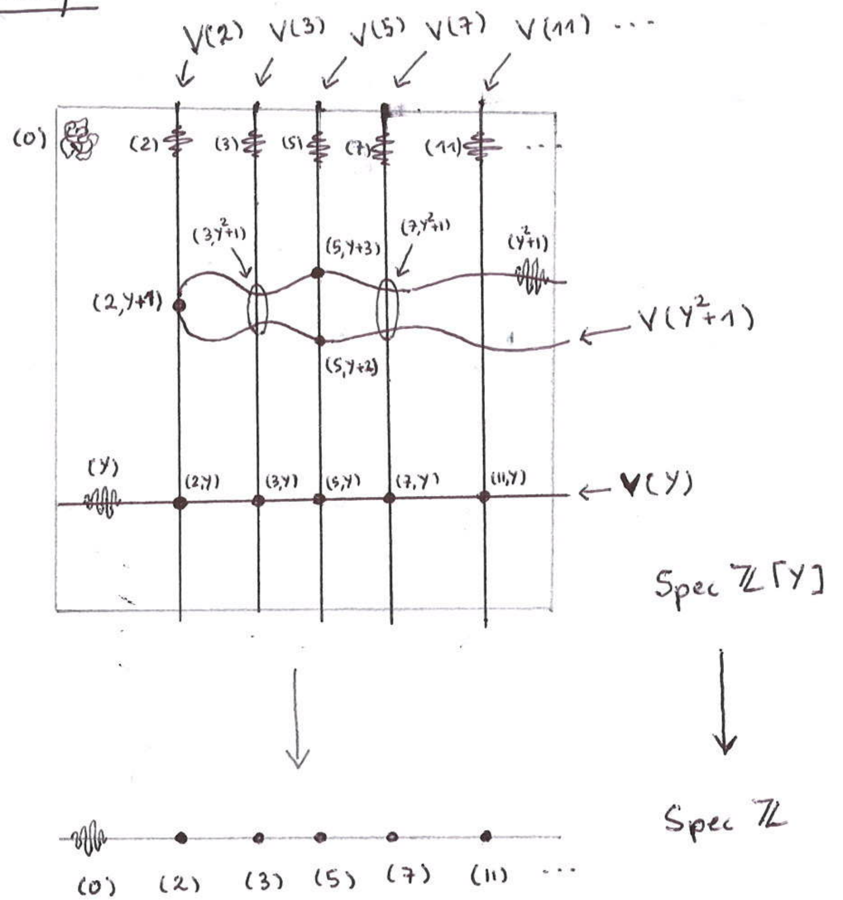
Note: For $R = k[X,Y]$ with k algebraically closed, these maximal ideals have the form $m = (X-x_0, Y-y_0)$ with $x_0, y_0 \in k$, so we get the affine plane.

Picture:



$\Rightarrow$ get 3 types of points:
* closed points $(X-x_0, Y-y_0)$
* a "big generic point" (0)
* for each curve $V(f)$ a generic pt (f) on that curve

Similarly:



Note the different types of fibers for $V(Y^2+1) \to \operatorname{Spec} \mathbb{Z}$:

$Y^2+1 = (Y+1)^2$ in $\mathbb{F}_2[Y]$,

Y^2+1 irreducible in $\mathbb{F}_3[Y]$,

$Y^2+1 = (Y+2)(Y+3)$ in $\mathbb{F}_5[Y]$, ...

Pf of the lemma.

A a PID

$R = A[Y] \hookrightarrow K[Y]$ where $K = \operatorname{Quot}(A)$ (quotient field)

$\mathfrak{p} \in \operatorname{Spec}(R)$

wlog not a principal ideal

$\Rightarrow \exists\, f_1, f_2 \in \mathfrak{p}$ which do not have any common divisor in R (except units)

Gauss' lemma Then f_1, f_2 don't have any common divisor in $K[Y]$ (except units)

$\Rightarrow$ Since $K[Y]$ is a PID, we get $(f_1, f_2) = (1) \trianglelefteq K[Y]$,

i.e. $a_1 f_1 + a_2 f_2 = 1$ for some $a_i \in K[Y]$

$\Rightarrow$ Since $K = \operatorname{Quot}(A)$, we can find $c \in A \setminus \{0\}$ with $c_i := c \cdot a_i \in A[Y] \subseteq K[Y]$ for $i = 1, 2$.

$\Rightarrow \quad c = c_1 f_1 + c_2 f_2 \in \mathfrak{P} \cap A$

hence $\mathfrak{P} \cap A \neq (0)$

$\Rightarrow$ Since A is a PID,
$\exists$ irreducible $p \in A$ with $\mathfrak{P} \cap A = (p)$
and $A/(p)$ is a field

Put $\bar{\mathfrak{P}} := \text{image}(\mathfrak{P}) \trianglelefteq \underbrace{(A/(p))[Y]}_{\text{this is a PID}}$

$\Rightarrow$ $\bar{\mathfrak{P}}$ principal ideal $\neq (0)$ and prime,
ie. $\bar{\mathfrak{P}} = (\bar{q})$ for some irreducible
$\bar{q} \in (A/(p))[Y]$

$\Rightarrow$ Can take $q :=$ (any lift of $\bar{q}$) $\in A[Y]$.

$\square$

3. More on PID and UFD

Let A be an integral domain.

For $a, b \in A$ we say <u>a divides b</u> (notation $a | b$)
if $b = ac$ for some $c \in A$.

What are the analogs of prime numbers in A?

<u>Def</u> We say $a \in A \setminus (A^* \cup \{0\})$ is

- <u>prime</u> if $a | bc$ implies $a | b$ or $a | c$,
- <u>irreducible</u> if it can't be written as $a = bc$ with $b, c \notin A^*$.

<u>Rem</u> • prime $\Rightarrow$ irreducible,
indeed: If $a = bc$ is prime
then wlog $a | b$, say $b = ad$,
ie $a = adc$ and so $a \cdot (1 - cd) = 0$,
whence $cd = 1$ (integral domain!), so $c \in A^*$.

• Converse fails in general,
eg. $(1+\sqrt{-5})(1-\sqrt{-5}) = 2 \cdot 3$ in $A = \mathbb{Z}[\sqrt{-5}]$

irreducible but not prime in A

Def A is a <u>unique factorization domain</u> (UFD) if every $a \in A \setminus \{0\}$ can be written as a finite product $a = u \cdot p_1 \cdots p_n$ $(*)$ with a unit $u \in A^*$ and prime elements $p_i \in A$.

Rem • The def^n of "prime" implies that the prime factorization $(*)$ is unique up to reordering the factors and multiplying them by units.

• In a UFD we have irreducible $\Leftrightarrow$ prime.

In particular, in the definition of UFD it's not enough to assume the p_i irreducible (see previous example).

Prop Euclidean $\Rightarrow$ PID $\Rightarrow$ UFD.

Pf. a) Assume A Euclidean,

ie. $\exists\, N: A \setminus \{0\} \longrightarrow \mathbb{N}$ sth $\forall a, b \in A \setminus \{0\}$,

- $N(a) \leq N(ab)$
- $\exists\, q, r \in A$: $a = qb + r$ where $r = 0$ or $N(r) < N(b)$.

Given $\mathfrak{a} \trianglelefteq A$, pick $b \in \mathfrak{a} \setminus \{0\}$ with $N(b)$ minimal, then $\mathfrak{a} = (b)$ (exercise).

(b) Assume A is a PID.

Claim 1: Then irreducibles are prime.

Indeed, let $a \in A$ irreducible and $a \mid bc$.

Being irreducible, a has no proper divisors, and since A is a PID, we get that $(a) \trianglelefteq A$ is maximal.

Then:

- either $(a, b) = (a)$ $\Rightarrow b \in (a)$ $\Rightarrow a \mid b$
- or $(a, b) = (1)$ $\Rightarrow \exists\, r, s \in A: ar + bs = 1$ $\Rightarrow c = a \cdot rc + bc \cdot s$ $\Rightarrow a \mid c$

Thus a is prime.

Claim 2: Any $a \in A \setminus (A^* \cup \{0\})$ is a finite product of irreducibles.

Indeed, in a PID we have: "a reducible $\Leftrightarrow (a) \trianglelefteq A$ not maximal", so if the claim fails we can find an infinite chain $(a_1) \overset{\neq}{\hookrightarrow} (a_2) \overset{\neq}{\hookrightarrow} \cdots \trianglelefteq A$ of ideals.

Put $\mathfrak{a} := \bigcup_{n \in \mathbb{N}} (a_n) \trianglelefteq A$, again an ideal!

$\underset{\text{PID}}{\Longrightarrow}$ $\mathfrak{a} = (a)$ for some $a \in \mathfrak{a}$

But then $a \in (a_n)$ for some $n \in \mathbb{N}$,

so $(a_n) = (a_{n+1}) = (a_{n+2}) = \cdots = (a)$ ↯ $\square$

Rem. • In general UFD $\not\Rightarrow$ PID $\not\Rightarrow$ Euclidean.

• The above has shown that in a PID, any ascending chain of ideals stabilizes. Such rings are called Noetherian and will be discussed in detail later.

Goal for the rest of this section:

$$A \text{ UFD} \Longrightarrow A[X] \text{ UFD}$$

(this is NOT true for PID, think of $A = \mathbb{Z}$ and $(2, X) \trianglelefteq \mathbb{Z}[X]$ ...)

Def We say $d \in A$ is a greatest common divisor (gcd) of $a_1, \dots, a_n \in A$ if

- $d \mid a_i \; \forall i$
- any e with $e \mid a_i \; \forall i$ satisfies $e \mid d$.

In a UFD any $a_1, \dots, a_n \in A$ have a gcd, which is unique up to multiplication by a unit and we denote by $\gcd(a_1, \dots, a_n) \trianglelefteq A$ the ideal it generates.

Def Let A be a UFD. The content of $f \in A[X]$ is the ideal
$c(f) := \gcd(\text{coefficients of } f) \trianglelefteq A$.

We say f is primitive if $c(f) = (1)$.

Gauss' lemma For any $f, g \in A[X]$,

$$c(fg) = c(f)c(g).$$

In particular:

fg primitive $\Longleftrightarrow$ f and g both primitive.

Pf. Put $c(f) =: (d)$
$c(g) =: (e)$ with $d, e \in A$

$\Rightarrow$ $f = d f_0$
$g = e g_0$ with $f_0, g_0 \in A[X]$ primitive

Replacing f by f_0
g by g_0 can assume wlog f, g primitive.

If fg were not primitive,

$\exists$ prime $p \in A$ with $p \mid fg$

$\Rightarrow$ the reductions $\bar{f}, \bar{g} \in A/(p)[X]$

satisfy $\bar{f}\bar{g} = \overline{fg} = 0$ in $\underbrace{A/(p)[X]}_{\substack{\text{integral} \\ \text{domain!} \\ \text{(because } p \\ \text{is prime in } A)}}$

$\Rightarrow$ $\bar{f} = 0$ or $\bar{g} = 0$

$\Rightarrow$ $p \mid f$ or $p \mid g$,
ie. f or g not primitive $\lightning$ $\square$

Cor Let A be a UFD and $K = \mathrm{Quot}(A)$.
If $f \in A[X]$ has degree > 0 and is reducible in $K[X]$, then also in $A[X]$.

Pf. Wlog f primitive (factor out $c(f)$).

Assume $f = f_1 f_2$ with $f_i \in K[X]$, $\deg f_i > 0$.

Write $f_i = c_i \cdot g_i$ with $c_i \in K^*$
$g_i \in A[X]$ primitive.

$\Rightarrow$ $f = c \cdot g_1 g_2$ with $c := c_1 c_2$.

A priori $c \in K^*$, we're done if we show $c \in A^*$.

Write $c = \frac{a}{b}$ with $a, b \in A \setminus \{0\}$, $\gcd(a, b) = 1$

$\Rightarrow$ $bf = a g_1 g_2$

$\Rightarrow$ $(b) \underset{\substack{\uparrow \\ f \text{ primitive}}}{=} c(bf) = c(a g_1 g_2) = (a) \cdot c(g_1 g_2) \underset{\substack{\uparrow \\ g_1 g_2 \text{ primitive} \\ \text{by Gauss' lemma}}}{=} (a)$

$\Rightarrow$ $(b) = (a)$, ie. $c = \frac{a}{b} \in A^*$
is a unit. $\square$

Rem In fact we have shown: For $f \in A[X]$,

if a primitive polynomial $g \in A[X]$ divides f in $K[X]$,

then it does so already in $A[X]$.

Thus: If $f_1, f_2 \in A[X]$ have no common divisor in $A[X]$

except units, then they also don't in $K[X]$,

as we used in the lemma of section 2.

Finally, let's summarize:

Thm Let A be a UFD and $K = \mathrm{Quot}(A)$.

Then

(a) $A[X]$ is a UFD

(b) its irreducible (= prime) elements are

- constant polynomials $f(X) \equiv c$ with $c \in A$ irreducible,

- primitive polynomials $f(X) \in A[X]$ that are irreducible of $\deg > 0$ in $K[X]$.

Pf. Given $f \in A[X] \setminus (A^* \cup \{0\})$,

factor it into irreducibles in $K[X]$.

Clearing denominators & using Gauss' lemma,

we get a factorization of f as a product of elements

described in (b), which are irreducible.

So it only remains to show that the elements in (b) are prime.

- $c \in A$ irreducible in A ($\Rightarrow$ prime in A since A is a UFD)

  and $c \mid fg$ in $A[X]$

  for $f, g \in A[X]$

  $\Rightarrow$ writing $c(f) = (d)$, $c(g) = (e)$ we have $c \mid de$ in A

  $\Rightarrow$ $c \mid d$ or $c \mid e$ because $c \in A$ is prime

  $\Rightarrow$ $c \mid f$ or $c \mid g$ in $A[X]$

- $f \in A[X]$ primitive of $\deg > 0$ & irred. in $K[X]$

  with $f \mid gh$ in $A[X]$ for some $f, g \in A[X]$

  $\Rightarrow$ $f \mid gh$ in the UFD $K[X]$

  but there f is prime

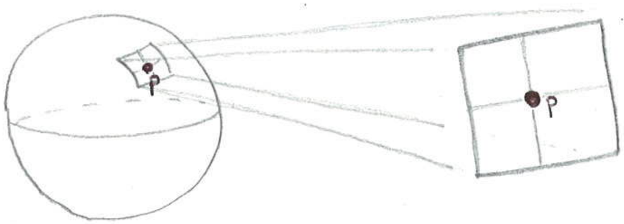
  $\Rightarrow$ $f \mid g$ or $f \mid h$ in $K[X]$

  $\Rightarrow$ idem in $A[X]$ by the previous remark, since f is primitive.

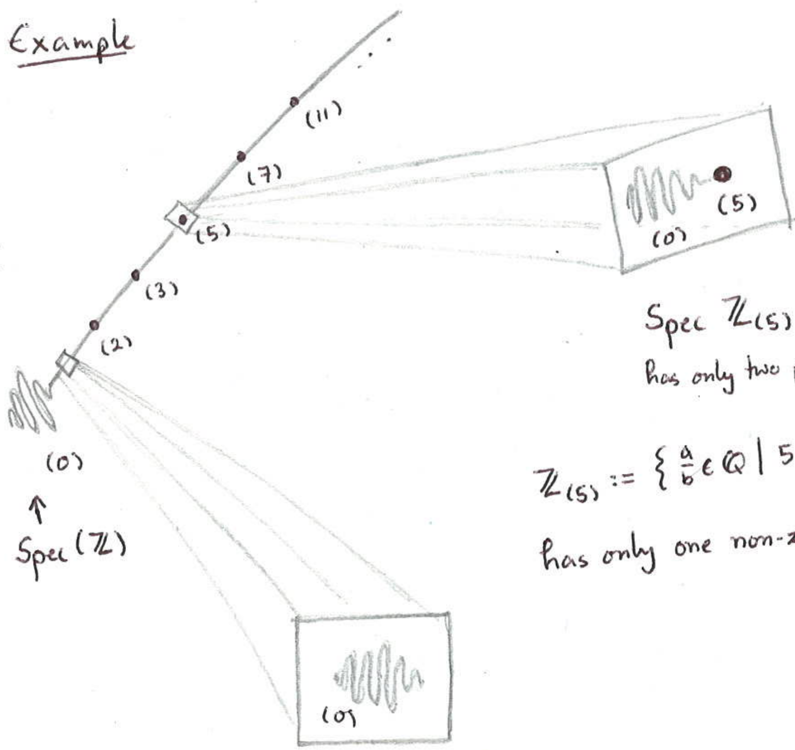
$\square$

4. Localization (making life easy)

Idea: Simplify things by working "locally"



Example



Spec $\mathbb{Z}_{(5)}$

has only two points:

$\mathbb{Z}_{(5)} := \{ \frac{a}{b} \in \mathbb{Q} \mid 5 \nmid b \}$

has only one non-zero prime ideal!

Spec $\mathbb{Q} = \{(0)\}$

only the generic point!

Def A local ring is a ring R with a unique maximal ideal $\mathfrak{m} \subsetneq R$. (ie Spec R contains a unique closed point)

Lemma Let R be a ring and $\mathfrak{m} \trianglelefteq R$, $\mathfrak{m} \neq R$ a proper ideal. Then TFAE:

a) R is local w/ maximal ideal $\mathfrak{m}$.

b) $R \setminus \mathfrak{m} \subseteq R^*$.

c) $\mathfrak{m} \in \mathrm{Spm}(R)$ and $\underbrace{1+\mathfrak{m}}_{\{1+x \mid x \in \mathfrak{m}\}} \subseteq R^*$.

Pf. $a \Leftrightarrow b$:

$r \in R \setminus \mathfrak{m} \Rightarrow (r) \not\subseteq \mathfrak{m}$
but then $(r) = R$ by a)
since $\mathfrak{m}$ is the only max. ideal in R
$\Rightarrow r \in R^*$ & converse is trivial

$b \Rightarrow c$:

$R \setminus \mathfrak{m} \subseteq R^* \Rightarrow \mathfrak{m}$ maximal.
and $\forall x \in \mathfrak{m}$, $1 + x \notin \mathfrak{m}$ (since $1 \notin \mathfrak{m}$),
so $1 + x \in R \setminus \mathfrak{m} \underset{(b)}{\subseteq} R^*$

(c) $\Rightarrow$ (b):

$r \in R \setminus m \Rightarrow m + (r) = (1)$ by maximality of m

ie. $x + rs = 1$ for some $x \in m$, $s \in R$

$\Rightarrow rs = 1 - x \in 1 + m \underset{\substack{\uparrow \\ (c)}}{\subseteq} R^*$ $\square$

$\Rightarrow r \in R^*$

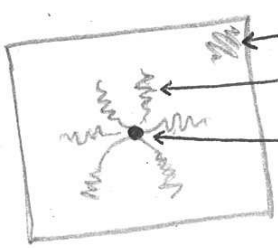
Ex
- Any field k is a local ring with $m = (0)$.
- Any discrete valuation ring (DVR), ie. PID with a unique prime element (up to units), such as

$$\mathbb{Z}_{(p)} := \{ \tfrac{a}{b} \in \mathbb{Q} \mid p \nmid b \} \text{ for } p \text{ prime},$$

$$k[X]_{(X)} := \{ \tfrac{a}{b} \in k(X) \mid b(0) \neq 0 \}$$

for k a field,

- $k[X,Y]_{(X,Y)} := \{ \frac{a}{b} \in k(X,Y) \mid b(0,0) \neq (0,0) \}$



All these examples arise from a given ring A by inverting all elements of a subset $S \subset A$, namely

- $S = k \setminus \{0\} \subset k$
- $S = \mathbb{Z} \setminus (p) \subset \mathbb{Z}$
- $S = k[X] \setminus (X) \subset k[X]$
- $S = k[X,Y] \setminus (X,Y) \subset k[X,Y]$

More systematically:

Def By a multiplicative subset of a ring A we mean a submonoid $S \subset (A, \cdot)$, ie. a subset $S \subset A$ with $\begin{cases} 1 \in S \\ st \in S \ \forall s,t \in S \end{cases}$

Want to invert those "as economically as possible":

Thm Let A be a ring and $S \subset A$ multiplicative. Then $\exists$ a ring A_S with a natural homom. $A \xrightarrow{\varphi} A_S$ sth

a) $\varphi(S) \subset A_S^*$

b) any other ring homom. $\psi: A \to B$ with $\psi(S) \subset B^*$ factors uniquely over φ:

i.e.

$$\begin{tikzcd} A \arrow[rr, "\psi"] \arrow[dr, "\varphi"'] & & B \\ & A_S \arrow[ur, dashed, "\exists!\,\overline{\psi}"'] & \end{tikzcd}$$

Pf.

Intuitive idea: $A_S = $ " $\{ \frac{a}{s} \mid a \in A, s \in S \}$ "

Step 1: Define a relation "$\sim$" on the set $A \times S$ by

$$(a,s) \sim (a',s') :\Longleftrightarrow t \cdot (as' - a's) = 0$$

for some $t \in S$

Claim: This is an equivalence relation!

(⚠ The extra factor t is needed for this if A has zero divisors ...)

- reflexive + symmetric: obvious (can take $t = 1$)
- transitive:

$$\begin{matrix} (a,s) \sim (a',s') \\ (a',s') \sim (a'',s'') \end{matrix} \Longrightarrow \begin{matrix} t \cdot (as' - a's) = 0 & (*) \\ t' \cdot (a's'' - a''s') = 0 & (**) \end{matrix}$$

$$\Longrightarrow \underbrace{s's''tt'}_{\in S} \cdot (as'' - a''s) = (s'')^2 t' \cdot (*) + ss''t \cdot (**) = 0.$$

OK!

Step 2: Put $A_S := (A \times S)/_\sim$ as a set.

For $(a,s) \in A \times S$ put $\frac{a}{s} :=$ "equivalence class of (a,s) mod $\sim$"

Claim: A_S is a ring with

$$\frac{a}{s} + \frac{b}{t} := \frac{at + bs}{st}$$

$$\frac{a}{s} \cdot \frac{b}{t} := \frac{ab}{st}.$$

Main point is to see these operations are well-defined:

Let $\frac{a}{s} = \frac{a'}{s'}$ and $\frac{b}{t} = \frac{b'}{t'}$

$\Longrightarrow u(as' - a's) = v(bt' - b't) = 0$ with $u, v \in S$ (*)

$$\Longrightarrow \left[(at+bs) \cdot s't' - (a't' + b's') \cdot st \right] \cdot uv$$

$$= \underbrace{uas'}_{\substack{= ua's \\ \text{by} (*)}} \cdot tt'v + \underbrace{vbt'}_{\substack{= vb't \\ \text{by} (*)}} \cdot ss'u - ua's \cdot tt'v - vb't \cdot ss'u$$

$$= 0 \qquad \Longrightarrow \frac{a}{s} + \frac{b}{t} = \frac{a'}{s'} + \frac{b'}{t'}$$

and

$$\left[abs't' - a'b'st \right] \cdot uv = \underbrace{uas'} \cdot vbt' - ua's \cdot vb't \underset{(*)}{=} 0 \Longrightarrow \frac{a}{s} \cdot \frac{b}{t} = \frac{a'}{s'} \cdot \frac{b'}{t'}$$

OK!

Step 3: Define $\varphi : A \to A_S$

by $\varphi(a) := \frac{a}{1}$.

$\Longrightarrow$ this is a ring homomorphism: $\left|\ \begin{array}{l} \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} \\ \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1} \end{array}\right.$

Claim: Properties a) and b) hold.

a) For $a = s \in S$,

$\varphi(s) = \frac{s}{1} \in A_S^*$ w/ inverse $s^{-1} = \frac{1}{s}$ (obvious),

hence $\varphi(S) \subset A_S^*$.

b) Let $\psi : A \to B$ be given with $\psi(S) \subset B^*$.

If $\exists$ factorization $\psi = \bar{\psi} \circ \varphi$,

necessarily

$$
\begin{aligned}
\bar{\psi}\left(\tfrac{a}{s}\right) &= \bar{\psi}\left(\tfrac{a}{1} \cdot \tfrac{1}{s}\right) \\
&= \bar{\psi}\left(\tfrac{a}{1}\right) \cdot \bar{\psi}\left(\tfrac{1}{s}\right) \qquad (\bar{\psi} \text{ homomorphism}) \\
&= \bar{\psi}(\varphi(a)) \cdot \bar{\psi}(\varphi(s)^{-1}) \qquad (\text{def}^n \text{ of } \varphi) \\
&= \bar{\psi}(\varphi(a)) \cdot \bar{\psi}(\varphi(s))^{-1} \qquad (\bar{\psi} \text{ homomorphism}) \\
&= \psi(a) \cdot \psi(s)^{-1} \qquad (\psi = \bar{\psi} \circ \varphi)
\end{aligned}
$$

$\Longrightarrow$ $\bar{\psi}$ is unique (if it exists at all)

Existence:

Define $\bar{\psi}\left(\frac{a}{s}\right) := \psi(a) \cdot \psi(s)^{-1}$

$\uparrow$ using $\psi(S) \subseteq B^*$

Welldefined:

Let $\frac{a}{s} = \frac{a'}{s'}$, then $t(as' - a's) = 0$ for some $t \in S$

$\Longrightarrow \underbrace{\psi(t)}_{\in B^*} \cdot \big(\psi(a) \cdot \underbrace{\psi(s')}_{\in B^*} - \psi(a') \underbrace{\psi(s)}_{\in B^*}\big) = 0$

$\Longrightarrow \psi(a) \cdot \psi(s)^{-1} = \psi(a') \cdot \psi(s')^{-1}$ ok!

$\square$

This $\bar{\psi}$ is a ring homomorphism (obvious).

Def / Rem. We call A_S the localization of A at S and also denote it by $S^{-1}A := A_S$.

It is determined uniquely by the UMP a), b) up to iso: If $\tilde{\varphi} : A \to \tilde{A}_S$ also satisfies a), b),

look at

$$
\begin{tikzcd}
A \arrow[r, "\varphi"] \arrow[d, "\varphi"'] \arrow[dr, "\tilde{\varphi}"] & A_S \\
A_S \arrow[r, dashed, "\exists!"] \arrow[ur, bend right, "= id"'] & \tilde{A}_S \arrow[u, dashed, "\exists!"']
\end{tikzcd}
$$

by uniqueness $\left(\begin{array}{l} \text{\& idem with} \\ A_S, \tilde{A}_S \\ \text{interchanged} \end{array}\right)$.

Ex

1a) For any $\wp \in \operatorname{Spec}(A)$, the subset $S := A \setminus \wp$ is multiplicative.

By abuse of notation we put $A_\wp := A_S$

e.g. $A_{(0)} = \operatorname{Quot}(A)$ for A integral domain,

$\mathbb{Z}_{(p)} = \{ \frac{a}{b} \in \mathbb{Q} \mid p \nmid b \}$,

$k[X]_{(X)} = \{ \frac{f}{g} \in k(X) \mid g(0) \neq 0 \}$, ...

1b) Similarly for families $(\wp_i \in \operatorname{Spec}(A))_{i \in I}$, can consider $S := A \setminus \bigcup_{i \in I} \wp_i = \bigcap_{i \in I} A \setminus \wp_i$

e.g. $\mathbb{Z}_S = \{ \frac{a}{b} \in \mathbb{Q} \mid p_i \nmid b \ \forall i \in I \}$.

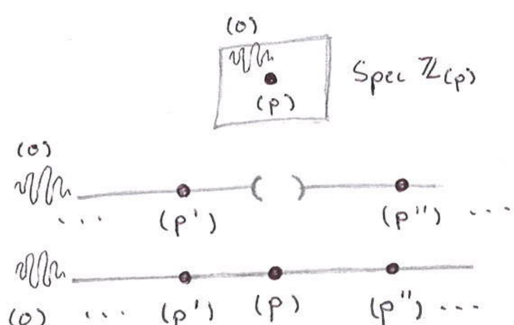
2a) For $f \in A$ take $S = \{ f^n \mid n \in \mathbb{N}_0 \}$.

By abuse of notation we put $A_f := A[f^{-1}] := A_S$.

⚠ NEVER use this notation for $A = \mathbb{Z}$ & $f = p$.

For historic reasons $\mathbb{Z}_p := (\text{completion of } \mathbb{Z}_{(p)}) \neq \mathbb{Z}[\frac{1}{p}]$

these two are really opposite to each other ...



Spec $\mathbb{Z}_{(p)}$

Spec $\mathbb{Z}[\frac{1}{p}] = (\operatorname{Spec} \mathbb{Z}) \setminus \{(p)\}$

Spec $\mathbb{Z}$

2b) For families $(f_i \in A)_{i \in I}$ put $S :=$ monoid generated by the f_i

$= \{$ finite products of elements $f_i, i \in I \}$

__Lemma__ In this case

$$A_S \simeq A[T_i \mid i \in I] / (1 - f_i T_i \mid i \in I)$$

where the T_i are formal variables.

Pf. Check universal property for the natural homom.

$$\varphi : A \longrightarrow B := A[T_i \mid i \in I] / (1 - f_i T_i \mid i \in I).$$

a) $\varphi(f_i) \in B^*$ since $\varphi(f_i) \cdot T_i \equiv 1$ in B

$\Rightarrow \varphi(S) \subset B^*$

b) Let $\psi : A \to C$ with $\psi(S) \subset C^*$.

The universal property of polynomial rings says:

$\forall c_i \in C \ (i \in I) \quad \exists! \ \tilde{\psi} : A[T_i \mid i \in I] \longrightarrow C$ with $T_i \longmapsto c_i$.

Apply this to $c_i := \psi(f_i)^{-1} \in C^*$

$$\Rightarrow \begin{tikzcd} \tilde{\psi} : A[T_i \mid i \in I] \arrow[r] \arrow[dr] & C \\ & B \arrow[u, dashed, "\exists! \bar{\psi}"'] \end{tikzcd}$$

since $\ker(\tilde{\psi}) \ni 1 - f_i T_i \ \forall i \in I$.

$\square$

⚠ Caution about zero divisors:

Lemma. Let A be a ring and $S \subset A$ multiplicative.

(a) $\ker(A \xrightarrow[\varphi]{} A_S) = \{ a \in A \mid \exists s \in S : as = 0 \}$

(b) $A_S = \{0\} \iff 0 \in S$

(c) $\varphi : A \xrightarrow{\sim} A_S$ iso $\iff S \subset A^*$

Pf.

a) $\varphi(a) = 0 \iff \frac{a}{1} = \frac{0}{1} \iff s \cdot \underbrace{(a \cdot 1 - 0 \cdot 1)}_{=a} = 0$ for some $s \in S$

b) $A_S = \{0\} \iff \frac{1}{1} = \frac{0}{1} \iff s \cdot 1 = 0$ for some $s \in S$

ie $0 \in S$

c) "$\Rightarrow$" trivial since $\varphi(S) \subset A_S^*$

"$\Leftarrow$" If $S \subset A^*$ then $\tilde{\varphi} := \mathrm{id} : A \to B := A$ has the universal property of localization. $\square$

Back to our geometric motivation for localization:

What about (prime) ideals?

Prop a) We have a natural map

$$\left\{ \begin{matrix} \text{proper ideals} \\ \mathfrak{b} \trianglelefteq_{\neq} A_S \end{matrix} \right\} \hookrightarrow \left\{ \begin{matrix} \text{ideals } \mathfrak{a} \trianglelefteq A \\ \text{with } S \cap \mathfrak{a} = \emptyset \end{matrix} \right\}$$

$$\mathfrak{b} \longmapsto \varphi^{-1}(\mathfrak{b}) =: \mathfrak{a},$$

which is injective with left inverse given by the map $\mathfrak{b} := \mathfrak{a} \cdot A_S \longleftarrow\!\shortmid\ \mathfrak{a}$

i.e. we have $\varphi^{-1}(\mathfrak{b}) \cdot A_S = \mathfrak{b} \quad \forall\, \mathfrak{b} \trianglelefteq_{\neq} A_S$.

b) On prime ideals this induces a bijection

$$\mathrm{Spec}(A_S) \xrightarrow{\sim} \{ \mathfrak{p} \in \mathrm{Spec}(A) \mid S \cap \mathfrak{p} = \emptyset \}$$

$$\mathfrak{q} \longmapsto \varphi^{-1}(\mathfrak{q}) =: \mathfrak{p}$$

with inverse $\mathfrak{q} := \mathfrak{p} \cdot A_S \longleftarrow\!\shortmid\ \mathfrak{p}$,

i.e. we also have $\varphi^{-1}(\mathfrak{p} \cdot A_S) = \mathfrak{p}$

$\forall\, \mathfrak{p} \in \mathrm{Spec}(A)$ with $\mathfrak{p} \cap S = \emptyset$.

Pf.

a) Clearly $\varphi^{-1}(\mathfrak{b}) \trianglelefteq A$ is an ideal for any $\mathfrak{b} \trianglelefteq A_S$,

and

- $\mathfrak{b} = A_S \Rightarrow 1 = \frac{1}{1} \in \mathfrak{b} \Rightarrow 1 \in \varphi^{-1}(\mathfrak{b}) = \mathfrak{a} \Rightarrow S \cap \mathfrak{a} \neq \emptyset$
- $S \cap \mathfrak{a} \neq \emptyset \Rightarrow \exists s \in S \cap \mathfrak{a} \Rightarrow \frac{s}{1} \in \mathfrak{b} \Rightarrow \mathfrak{b} = A_S$ because $\frac{s}{1} \in A_S^*$.

Thus

$$\varphi^{-1} : \{ \mathfrak{b} \underset{\neq}{\trianglelefteq} A_S \} \longrightarrow \{ \mathfrak{a} \trianglelefteq A \mid S \cap \mathfrak{a} = \emptyset \}.$$

Claim:

$$\varphi^{-1}(\mathfrak{b}) \cdot A_S := \begin{pmatrix} \text{ideal of } A_S \text{ generated} \\ \text{by } \frac{a}{1} \text{ for } a \in \varphi^{-1}(\mathfrak{b}) \end{pmatrix} \overset{!}{=} \mathfrak{b}$$

Indeed "$\subseteq$" obvious,

for "$\supseteq$" let $\frac{b}{s} \in \mathfrak{b}$,

then $\frac{b}{1} = \frac{s}{1} \cdot \frac{b}{s} \in \mathfrak{b} \Rightarrow b \in \varphi^{-1}(\mathfrak{b})$

$\Rightarrow \frac{b}{s} = \frac{b}{1} \cdot \frac{1}{s} \in \varphi^{-1}(\mathfrak{b}) \cdot A_S$ ok!

b) Clearly $\varphi^{-1}(\mathfrak{q}) \in \operatorname{Spec} A$ for $\mathfrak{q} \in \operatorname{Spec} A_S$.

Conversely:

$\left.\begin{matrix} \mathfrak{p} \in \operatorname{Spec} A \\ \mathfrak{p} \cap S = \emptyset \end{matrix}\right| \Rightarrow \mathfrak{p} \cdot A_S \in \operatorname{Spec} A_S$:

Suppose $\frac{a}{s}, \frac{b}{t} \in A_S$ and $\frac{a}{s} \cdot \frac{b}{t} \in \mathfrak{p} \cdot A_S$

$\Rightarrow \frac{a}{s} \cdot \frac{b}{t} = \frac{c}{u} \in A_S$ with $c \in \mathfrak{p}$, $u \in S$

$\Rightarrow (abu - \underset{\substack{\uparrow \\ c \in \mathfrak{p}}}{c}st) \cdot \underset{\substack{\uparrow \\ v \notin \mathfrak{p} \\ \text{since } \mathfrak{p} \cap S = \emptyset}}{v} = 0$ in A for some $v \in S$

$\Rightarrow abu \in \mathfrak{p}$

$\Rightarrow a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ (since $u \notin \mathfrak{p}$)

$\Rightarrow \frac{a}{s} \in \mathfrak{p}A_S$ or $\frac{b}{t} \in \mathfrak{p}A_S$,

ie

$\mathfrak{p}A_S \in \operatorname{Spec} A_S$.

Final claim: $\varphi^{-1}(\mathfrak{p}A_S) = \mathfrak{p}$.

Indeed "$\supseteq$" obvious (without using that $\mathfrak{p}$ is prime).

For "$\subseteq$" let $a \in \varphi^{-1}(\mathfrak{p}A_S)$,

then $\frac{a}{1} \in \mathfrak{p}A_S$, say $\frac{a}{1} = \frac{b}{s}$ with $b \in \mathfrak{p}$, $s \in S$

$\Rightarrow t \cdot (sa - 1 \cdot b) = 0$ for some $t \in S$

$\underset{t \notin \mathfrak{p}}{\Rightarrow} sa - b \in \mathfrak{p} \underset{b \in \mathfrak{p}}{\Rightarrow} sa \in \mathfrak{p} \underset{s \notin \mathfrak{p}}{\Rightarrow} a \in \mathfrak{p}$.

$\square$

<u>Rem.</u> The last step used that $\mathfrak{p}$ was prime.

In general

$$\mathfrak{a} \subseteq \varphi^{-1}(\mathfrak{a} A_S)$$

can be a strict inclusion if $\mathfrak{a}$ is not prime!

(unlike $\mathfrak{b} = \varphi^{-1}(\mathfrak{b}) \cdot A_S$ which always holds).

e.g. this happens for $A = k[X, Y]$

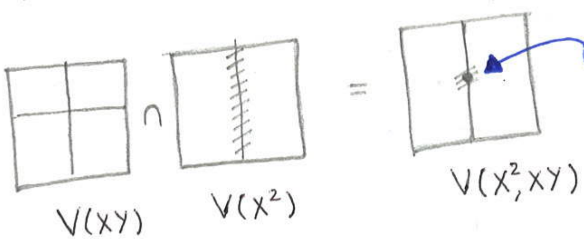
$S = A \setminus (X)$

$\mathfrak{a} = (X^2, XY)$:

Here $Y \in S \Rightarrow \frac{X}{1} = \frac{XY}{Y} \in \mathfrak{a} A_S$

$\Rightarrow \varphi^{-1}(\mathfrak{a} A_S) = (X) \overset{\neq}{\hookleftarrow} \mathfrak{a} = (X^2, XY)$

Picture:



Problem comes from this so-called "embedded point".

$\to$ We'll study such things later in the section on <u>primary decomposition</u>.

Back to prime spectra:

<u>Cor.</u> a) For $\mathfrak{p} \in \operatorname{Spec} A$, the localization $A_\mathfrak{p}$ is a local ring w/ maximal ideal $\mathfrak{p} \cdot A_\mathfrak{p}$.

b) For $f \in A$, one has

$$\operatorname{Spec}(A_f) = D(f) := \{\mathfrak{p} \in \operatorname{Spec} A \mid f \notin \mathfrak{p}\} \underset{\uparrow}{\subset} \operatorname{Spec} A$$

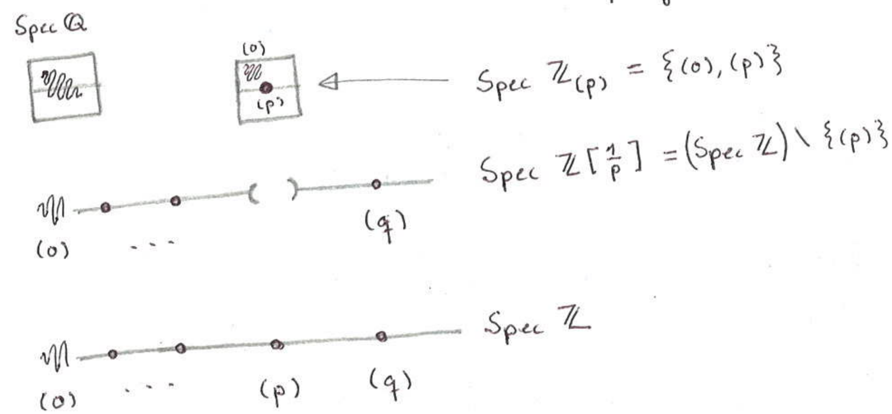
Zariski-open (exercise)

Pf. a) Proposition says

$$\operatorname{Spec} A_\mathfrak{p} = \{\mathfrak{q} \in \operatorname{Spec} A \mid \underbrace{\mathfrak{q} \cap (A \setminus \mathfrak{p}) = \emptyset}_{\text{i.e. } \mathfrak{q} \subseteq \mathfrak{p}}\}$$

thus $\mathfrak{p} \cdot A_\mathfrak{p}$ is the unique maximal ideal of $A_\mathfrak{p}$.

b) Similarly $\operatorname{Spec} A_f = \{\mathfrak{p} \in \operatorname{Spec} A \mid \underbrace{\mathfrak{p} \cap \{f^n \mid n \in \mathbb{N}_0\} = \emptyset}_{\text{ie. } f \notin \mathfrak{p}}\}$ $\square$



5. Radicals (Fun with zero functions)

Recall: Want to view R as a ring of "functions" on the "space" $\mathrm{Spm}\, R$, or better $\mathrm{Spec}\, R$, viewing $\wp \in \mathrm{Spec}\, R$ as the ideal of functions vanishing at the corresponding point.

Q: What about functions vanishing everywhere ???

Def For a ring R we put

- $\mathrm{Jac}(R) := \bigcap_{m \in \mathrm{Spm}\, R} m$ "Jacobson radical" (= functions vanishing at all closed points ...)
- $\mathrm{Rad}(R) := \bigcap_{\wp \in \mathrm{Spec}\, R} \wp$ "Nilradical / Radical" (= functions vanishing at all points ...)

Ex 1) $R = \mathrm{DVR}$ w/ max. ideal $(\pi) \trianglelefteq R$ $\Rightarrow$ $\mathrm{Jac}(R) = (\pi)$, $\mathrm{Rad}(R) = (0)$

2) $R = k[t]/(t^2)$ (k a field) $\Rightarrow$ $\mathrm{Spec}\, R = \{(\varepsilon)\}$, $\varepsilon := t \bmod (t^2)$
$\Rightarrow$ $\mathrm{Rad}\, R = \mathrm{Jac}\, R = (\varepsilon)$

3) $\mathrm{Jac}(R)$ is a max. ideal iff R is local.

Prop Let R be a ring.

a) $\mathrm{Jac}(R) = \{ a \in R \mid 1 - ab \in R^* \ \forall b \in R \}$

b) $\mathrm{Rad}(R) = \{ a \in R \mid a^n = 0 \text{ for some } n \in \mathbb{N} \}$ "nilpotent elements"

Pf.

a) "$\subseteq$" $a \in \mathrm{Jac}(R) \Rightarrow a \in m \ \forall m \in \mathrm{Spm}(R)$
$\Rightarrow 1 - ab \notin m \ \forall m \in \mathrm{Spm}(R) \ \forall b \in R$
$\Rightarrow 1 - ab \in R^* \ \forall b \in R$
(any non-unit lies in some max ideal by Zorn's lemma)

"$\supseteq$" $a \in R \setminus \mathrm{Jac}(R)$
$\Rightarrow \exists m \in \mathrm{Spm}(R) : \ a \notin m$
$\Rightarrow (m, a) = (1)$, ie. $1 = x + ab$ with $x \in m$, $b \in R$
$\Rightarrow 1 - ab = x \in m$, hence not a unit in R.

b) "$\supseteq$" $a^n = 0 \Rightarrow a^n \in \wp \ \forall \wp \in \mathrm{Spec}\, R$
$\Rightarrow a \in \wp$ by def^n of prime ideal, $\forall \wp \in \mathrm{Spec}\, R$
$\Rightarrow a \in \mathrm{Rad}(R)$

"$\subseteq$" $a^n \neq 0 \quad \forall n \in \mathbb{N}$

$\Rightarrow S := \{a^n \mid n \in \mathbb{N}_0\} \not\ni 0$

hence $R_S \neq \{0\}$ by §4

Pick any $\mathfrak{q} \in \mathrm{Spm}(R_S)$,

and put $\mathfrak{p} := \varphi^{-1}(\mathfrak{q}) \in \mathrm{Spec}(R)$ for $\varphi : R \to R_S$

(the localization map).

$\Rightarrow a \notin \mathfrak{p}$ because $\mathfrak{p} \cap S = \emptyset$ by §4 $\square$

$\Rightarrow a \notin \mathrm{Rad}(R)$

Why care about nilpotents?

Ex Inside $\mathrm{Spec}\, k[X]$ (k a field)

have the vanishing loci

$$V(X) = V(X^2) = V(X^3) = \cdots = \{(X)\} \subset \mathrm{Spec}\, k[X].$$

As sets they are all equal, because if $\mathfrak{p} \trianglelefteq k[X]$ is prime, then $X^n \in \mathfrak{p} \iff X \in \mathfrak{p}$

for any $n \in \mathbb{N}$.

Aside: The quotient map $k[X] \twoheadrightarrow k[X]/(X^n)$ sends a polynomial f to the first n terms of its Taylor expansion – so for $n > 1$ it keeps more info than just the value $f(0)$. Intuitively we think of $\mathrm{Spec}(k[X]/(X^n))$ as an "infinitesimal thickening" of the origin in the affine plane, though as a topological space it is just a single point – need algebraic geometry (scheme theory) to make sense of this...

Q: How to get rid of this ambiguity?

Def A ring R is reduced if it has no nilpotents $\neq 0$, i.e. if $\mathrm{Rad}(R) = \{0\}$.

Ex $k[X]/(X^n)$ is reduced iff $n = 1$.

Def Let R be a ring. The radical of $\mathfrak{a} \trianglelefteq R$ is defined as $\sqrt{\mathfrak{a}} := \{f \in R \mid f^n \in \mathfrak{a} \text{ for some } n \in \mathbb{N}\}$

Ex. $\sqrt{(0)} = \mathrm{Rad}(R)$. For $R = k[X]$, $\sqrt{(X^n)} = (X)$.

Lemma Let R be a ring and $\mathfrak{a} \trianglelefteq R$. Then

$$\sqrt{\mathfrak{a}} = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec} R \\ \mathfrak{a} \subseteq \mathfrak{p}}} \mathfrak{p} = q^{-1}(\operatorname{Rad}(R/\mathfrak{a}))$$

where $q : R \twoheadrightarrow R/\mathfrak{a}$ denotes the quotient map.

Cor. In particular, $\sqrt{\mathfrak{a}} \trianglelefteq R$ is an ideal.

Pf of the lemma.

By def^n $\operatorname{Rad}(R/\mathfrak{a}) = \bigcap_{\bar{\mathfrak{p}} \in \operatorname{Spec} R/\mathfrak{a}} \bar{\mathfrak{p}}$

Now recall that $q^{-1} : \{\text{ideals of } R/\mathfrak{a}\} \xrightarrow{\sim} \left\{\begin{matrix}\text{ideals of } R \\ \text{containing } \mathfrak{a}\end{matrix}\right\}$ is an inclusion-preserving bijection, and idem for "ideals" replaced by "prime ideals".

$$\Longrightarrow \quad q^{-1}(\operatorname{Rad}(R/\mathfrak{a})) = q^{-1}\Big(\bigcap_{\bar{\mathfrak{p}} \in \operatorname{Spec} R/\mathfrak{a}} \bar{\mathfrak{p}}\Big)$$

$$= \bigcap_{\bar{\mathfrak{p}} \in \operatorname{Spec} R/\mathfrak{a}} q^{-1}(\bar{\mathfrak{p}}) = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec} R \\ \mathfrak{a} \subseteq \mathfrak{p}}} \mathfrak{p}.$$

On the other hand,

$$\begin{aligned} f \in \sqrt{\mathfrak{a}} &\iff \exists n : f^n \in \mathfrak{a} \\ &\iff \exists n : (q(f))^n = 0 \text{ in } R/\mathfrak{a} \\ &\iff q(f) \in \operatorname{Rad}(R/\mathfrak{a}) \\ &\iff f \in q^{-1}(\operatorname{Rad}(R/\mathfrak{a})). \end{aligned}$$

$\square$

Geometric interpretation:

For any subset $V \subset \operatorname{Spec} R$ consider the ideal

$$\mathcal{I}(V) := \bigcap_{\mathfrak{p} \in V} \mathfrak{p} = \text{"functions vanishing at all points of } V\text{"}$$

Similarly, for $\mathfrak{a} \trianglelefteq R$ we've put

$$V(\mathfrak{a}) := \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{a} \subseteq \mathfrak{p}\} = \text{"vanishing locus of the ideal } \mathfrak{a}\text{"}$$

The lemma says:

$$\mathcal{I}(V(\mathfrak{a})) = \sqrt{\mathfrak{a}},$$

ie: "The radical $\sqrt{\mathfrak{a}}$ is the ideal of all functions that vanish on all points of the Zariski closed subset $V(\mathfrak{a}) \subset \operatorname{Spec} R$."

Upshot: The information about $\mathfrak{a} \trianglelefteq R$ captured by the subset $V(\mathfrak{a}) \subset \operatorname{Spec} R$ is precisely the radical $\sqrt{\mathfrak{a}}$.

Def We say that $\mathfrak{a} \trianglelefteq R$ is a radical ideal if $\mathfrak{a} = \sqrt{\mathfrak{a}}$ (i.e. if the ring $R/\mathfrak{a}$ is reduced).

Ex For any $\mathfrak{a} \trianglelefteq R$ the ideal $\sqrt{\mathfrak{a}}$ is a radical ideal.

Conclusion We have a bijective, inclusion-reversing correspondence

$$\left\{ \begin{array}{l} \text{Zariski closed} \\ \text{subsets } V \subset \operatorname{Spec} R \end{array} \right\} \overset{1:1}{\longleftrightarrow} \left\{ \begin{array}{c} \text{radical ideals} \\ \mathfrak{a} \trianglelefteq R \end{array} \right\}$$

$$V \longmapsto \mathcal{J}(V)$$

$$V(\mathfrak{a}) \longleftarrow\!\shortmid\ \mathfrak{a}.$$

Ex For $V_1, V_2 \subset \operatorname{Spec} R$ Zariski-closed,

$$\mathcal{J}(V_1 \cap V_2) = \sqrt{\mathcal{J}(V_1) + \mathcal{J}(V_2)}.$$

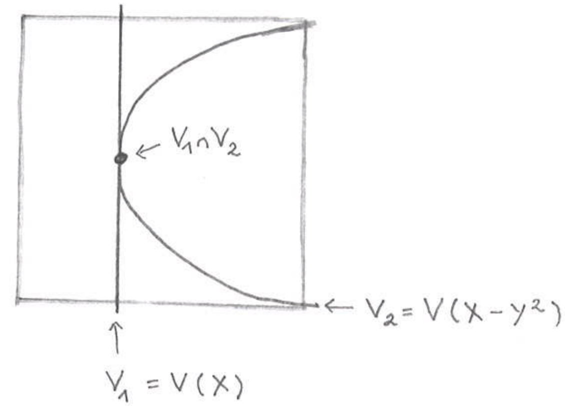
Indeed: $\mathfrak{p} \in V_1 \cap V_2 \iff \mathcal{J}(V_1) \subseteq \mathfrak{p}$ and $\mathcal{J}(V_2) \subseteq \mathfrak{p}$

$\iff \mathcal{J}(V_1) + \mathcal{J}(V_2) \subseteq \mathfrak{p}$

$\iff \mathfrak{p} \in V(\mathcal{J}(V_1) + \mathcal{J}(V_2))$

and hence $V_1 \cap V_2 = V(\mathcal{J}(V_1) + \mathcal{J}(V_2))$,

so $\mathcal{J}(V_1 \cap V_2) = \sqrt{\mathcal{J}(V_1) + \mathcal{J}(V_2)}$ by the lemma.



e.g. $R = k[X, Y]$

$\mathcal{J}(V_1) = (X)$

$\mathcal{J}(V_2) = (X - Y^2)$

$\mathcal{J}(V_1) + \mathcal{J}(V_2) = (X, Y^2)$

$\mathcal{J}(V_1 \cap V_2) = (X, Y)$

Rem. In general it's NOT enough to look at $\operatorname{Spm} R$:

e.g. let R be a local integral domain but not a field, and let $\mathfrak{m} \neq (0)$ be its max. ideal, then

$$V_1 := V(\mathfrak{m}) = \{\mathfrak{m}\} \overset{\neq}{\hookrightarrow} V_2 := V((0)) \ni (0)$$

but $V_1 \cap \operatorname{Spm} R = \{\mathfrak{m}\} = V_2 \cap \operatorname{Spm} R$.

Working with maximal ideals only recovers the Jacobson radical

$$\operatorname{Jac}(\mathfrak{a}) := \bigcap_{\substack{\mathfrak{m} \in \operatorname{Spm} R \\ \mathfrak{a} \subseteq \mathfrak{m}}} \mathfrak{m} \hookleftarrow \sqrt{\mathfrak{a}} = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec} R \\ \mathfrak{a} \subseteq \mathfrak{p}}} \mathfrak{p}$$

inclusion can be strict!

As before we have

$$\mathrm{Jac}(\mathfrak{a}) = q^{-1}(\mathrm{Jac}(R/\mathfrak{a}))$$

for the quotient map $q: R \to R/\mathfrak{a}$ (exercise)

A ring R is called <u>Jacobson ring</u> if $\sqrt{\mathfrak{a}} = \mathrm{Jac}(\mathfrak{a})$ for all $\mathfrak{a} \trianglelefteq R$.

We'll see later: $k[X_1, \ldots, X_n]$ is Jacobson for any field k ($\to$ <u>Hilbert's Nullstellensatz</u>).

<u>Rem</u>

- The nilradical is important because of its universal property: For any <u>reduced</u> ring S we have

$$\mathrm{Hom}(R, S) = \mathrm{Hom}(R^{red}, S)$$

where $R^{red} := R/\mathrm{Rad}(R)$ is the "biggest reduced quotient of R".

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[dr, two heads] & S \\ & R^{red} \arrow[u, dashed, "\exists! \bar{\varphi}"'] \end{tikzcd}$$
if S is reduced

- The Jacobson radical will return later in "Nakayama's lemma" (§7).

6. Modules

(Linear algebra over a ring)

Let R be a ring.

<u>Def</u> A <u>module over R</u> (or an <u>R-module</u>) is an abelian gp $(M, +)$ with a map $R \times M \to M$, $(r, m) \mapsto r \cdot m$ ("scalar multiplicat^n") which is

- unital: $1 \cdot m = m$
- associative: $a \cdot (b \cdot m) = (ab) \cdot m$
- distributive: $(a+b) \cdot m = a \cdot m + b \cdot m$

  $a \cdot (m+n) = a \cdot m + a \cdot n$

$\forall a, b \in R,\ m, n \in M.$

<u>Ex</u>

- $\mathbb{Z}$-modules = abelian groups
- if k is a field,

  k-modules = vector spaces over k.
- any ring R is a module over itself via multiplicat^n.
- for any $n \in \mathbb{N}$ we have the <u>free R-module of rk n</u>

  $M = R^n$ with $a \cdot (r_i)_{1 \le i \le n} := (a r_i)_{1 \le i \le n}$

  for $a \in R$, $(r_i)_{1 \le i \le n} \in R^n$.

Def We denote by $\mathrm{Mod}(R)$ the category of R-modules, with
- objects: the R-modules M
- morphisms: the homomorphisms of R-modules, i.e. maps $f: M \to N$ that are R-linear:

$$f(a \cdot m) = a \cdot f(m)$$
$$f(m_1 + m_2) = f(m_1) + f(m_2)$$
$$\forall a \in R$$
$$\forall m, m_1, m_2 \in M.$$

Notation: $\mathrm{Hom}_R(M,N) := \{ f: M \to N \text{ homom. of } R\text{-modules} \}$.

As usual, by a mono- / epi- / isomorphism of R-modules we mean a homomorphism that is injective / surjective / bijective.

By a submodule of $M \in \mathrm{Mod}(R)$ we mean a subgroup $N \hookrightarrow M$ s.th. $a \cdot n \in N$ $\forall a \in R, n \in N$.

($\Rightarrow$ $N \in \mathrm{Mod}(R)$ and the inclusion $N \hookrightarrow M$ is a monomorphism of R-modules).

Ex The submodules of R are precisely its ideals.

Note: If R is not a PID, then these usually cannot be generated (as an R-module) by a single element (unlike $R = R \cdot 1$).

Ex For any $M \in \mathrm{Mod}(R)$ we have the torsion submodule

$$M_{tors} := \{ m \in M \mid am = 0 \text{ for some } a \in R \setminus \{0\} \} \hookrightarrow M.$$

Any isomorphism of R-modules $f: M \xrightarrow{\sim} N$ restricts to $f: M_{tors} \xrightarrow{\sim} N_{tors}$. In particular:

$$M_{tors} \neq \{0\} \implies M \text{ is not isomorphic to a free } R\text{-module}$$

(e.g. $\mathbb{Z}/n\mathbb{Z}$ not free as a $\mathbb{Z}$-module.)

⚠ Converse "$\Leftarrow$" fails in general:

Lemma. Let R be an integral domain. Then an ideal $\mathfrak{a} \trianglelefteq R$, viewed as an R-submodule, is a free R-module iff it is a principal ideal.

Pf. "$\Longrightarrow$" Suppose $\exists$ index set I with iso $\varphi: R^I \xrightarrow{\sim} \mathfrak{a}$ as R-modules.

If $|I| \geq 2$, pick $i \neq j \in I$. Put

$$a_i := \varphi(e_i) \in \mathfrak{a}$$
$$a_j := \varphi(e_j) \in \mathfrak{a}$$

(e_i, e_j: standard basis vectors in R^I)

Then $\quad a_i a_j - a_j a_i = 0 \qquad$ (R is commutative)

but $\quad \varphi^{-1}(a_i a_j - a_j a_i) = a_i \cdot e_j - a_j \cdot e_i \qquad$ (φ^{-1} is R-linear)

$\neq 0 \qquad$ (R^I is free as an R-module and $i \neq j$)

$\lightning$

So we must have $|I| = 1$,

ie. $\quad \varphi : R \xrightarrow{\sim} \mathfrak{a}$ as an R-module.

$\Longrightarrow \quad \mathfrak{a} = R \cdot a \quad$ for $a := \varphi(1)$,

ie. $\mathfrak{a} = (a)$ is a principal ideal.

" $\Longleftarrow$ " Assume $\mathfrak{a} = (a) \trianglelefteq R$ principal.

Consider $\quad \varphi : R \longrightarrow \mathfrak{a}$

$\qquad\qquad b \longmapsto b \cdot a .$

This is an epimorphism but also mono since R is an integral domain!

$\square$

Slogan: The more complicated a ring is, the richer is its theory of modules!

Like for ideals we can take quotients:

<u>Def</u> For $M \in \mathrm{Mod}(R)$ and a submodule $N \subseteq M$, put

$$m_1 \equiv m_2 \mod N \quad :\Longleftrightarrow \quad m_1 - m_2 \in N .$$

We endow

$$M/N := \{ m \bmod N \mid m \in M \}$$

with the R-module structure

$$(m_1 \bmod N) + (m_2 \bmod N) := (m_1 + m_2 \bmod N)$$

$$a \cdot (m \bmod N) := (am \bmod N)$$

$$\forall\, a \in R,\ m_1, m_2, m \in M,$$

ie the unique R-module structure sth. the quotient map $M \xrightarrow{\pi} M/N$ is a homomorphism of R-modules.

<u>NB</u> Can recover the submodule as $N = \ker(\pi)$, where for any $f \in \mathrm{Hom}_R(M, M')$ we define the <u>kernel</u> by

$$\ker(f) := \{ m \in M \mid f(m) = 0 \} \hookrightarrow M .$$

$\Longrightarrow$ submodules = kernels of module homomorphisms,

and we have:

Lemma. Let $N \hookrightarrow M$ be an R-submodule.
Then $\forall f \in \mathrm{Hom}_R(M, M')$ with $N \subseteq \ker(f)$,
$\exists!$ factorization

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[dr, "\pi"', two heads] & M' \\ & M/N \arrow[u, dashed, "\exists!\, \bar{f}"'] \end{tikzcd}$$

Moreover, $\bar{f}$ monomorphism $\iff N = \ker(f)$. $\square$

Pf. Same as for ideals.

NB $\{\text{Submodules of } M/N\} \xleftrightarrow{1:1} \{\text{Submodules of } M \text{ containing } N\}$

$$\begin{array}{ccc} \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ M'/N & \longleftrightarrow & M' \text{ with } M' \supseteq N \end{array}$$

Def For $f \in \mathrm{Hom}_R(M, M')$ put $\mathrm{im}(f) := \{f(m) \mid m \in M\} \hookrightarrow M'$
(the *image* of f)

$\Longrightarrow$ $\exists$ natural factorization

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\pi"', two heads] & M' \\ M/\ker(f) \arrow[r, dashed, "\sim", "\exists!"'] & \mathrm{im}(f) \arrow[u, hook] \end{tikzcd}$$

Rem. This can be formalized in the abstract notion of an "abelian category", of which $\mathrm{Mod}(R)$ is the prototypical example.

How to get new modules from a given one?

Ex Let $M \in \mathrm{Mod}(R)$.

- For any $m \in M$ we have a submodule $Rm := \{a \cdot m \mid a \in R\} \hookrightarrow M$.
- More generally, for $m_1, \dots, m_n \in M$ put $Rm_1 + \dots + Rm_n := \{\sum_i a_i m_i \mid a_i \in R\} \hookrightarrow M$.
  Such submodules are called *finitely generated*.
  We say M is *finitely generated* if $M = Rm_1 + \dots + Rm_n$ for suitable $m_1, \dots, m_n \in M$.
- For any family of submodules $M_i \hookrightarrow M$ $(i \in I)$ their sum / intersection

$$\sum_{i \in I} M_i := \Big\{ \sum_{i \in I} m_i \;\Big|\; \begin{array}{l} m_i \in M_i \\ \text{almost all zero} \end{array} \Big\} \hookrightarrow M$$

$$\bigcap_{i \in I} M_i = \{ m \in M \mid m \in M_i \ \forall i \} \hookrightarrow M$$

are submodules.

Rem. In the sum $\sum_{i \in I} M_i \hookrightarrow M$ the submodules $M_i \hookrightarrow M$ needn't be "linearly independent over R", as in linear algebra ("sum" vs "direct sum").

Thm Let $M_i \in \mathrm{Mod}(R)$ for $i \in I$.

a) $\exists!!$ R-module $\bigoplus_{i\in I} M_i$ (called the "direct sum" of the M_i)

(unique up to unique isomorphism)

with monomorphisms $M_i \overset{\iota_i}{\hookrightarrow} \bigoplus_{i\in I} M_i$

sth for any $M \in \mathrm{Mod}(R)$,

$$\begin{array}{ccc} \mathrm{Hom}_R(\bigoplus_{i\in I} M_i, M) & \xrightarrow{\sim} & \prod_{i\in I} \mathrm{Hom}_R(M_i, M) \\ \text{\rotatebox{90}{$\in$}} & & \text{\rotatebox{90}{$\in$}} \\ f & \longmapsto & (f\circ \iota_i)_{i\in I}, \end{array}$$

ie. any collection of $f_i \in \mathrm{Hom}_R(M_i, M)$ arises from a unique $f \in \mathrm{Hom}(\bigoplus_{i\in I} M_i, M)$ as shown below:

$$\begin{tikzcd} M_i \arrow[r, hook, "\iota_i"] \arrow[dr, "f_i"'] & \bigoplus_{i\in I} M_i \arrow[d, dashed, "\exists! f"] \\ & M \end{tikzcd}$$

b) $\exists!!$ R-module $\prod_{i\in I} M_i$ (the "direct product" of the M_i) with epimorphisms $p_i : \prod_{i\in I} M_i \twoheadrightarrow M_i$ sth $\forall M \in \mathrm{Mod}(R)$,

$$\begin{array}{ccc} \mathrm{Hom}_R(M, \prod_{i\in I} M_i) & \xrightarrow{\sim} & \prod_{i\in I} \mathrm{Hom}_R(M, M_i) \\ \text{\rotatebox{90}{$\in$}} & & \text{\rotatebox{90}{$\in$}} \\ g & \longmapsto & (p_i\circ g)_{i\in I} \end{array}$$

ie.
$$\begin{tikzcd} M \arrow[d, dashed, "\exists! g"'] \arrow[dr, "g_i"] & \\ \prod_{i\in I} M_i \arrow[r, two heads, "p_i"'] & M_i \end{tikzcd}$$
for any $g_i \in \mathrm{Hom}_R(M, M_i)$ $(i \in I)$.

Pf. Uniqueness follows from universal property, so only need to check existence.

Put
$$\begin{tikzcd} M_i & \prod_{i\in I} M_i := \{(m_i)_{i\in I} \mid m_i \in M_i\} \arrow[l, two heads, "pr"'] \\ M_i \arrow[r, hook, "incl."'] & \bigoplus_{i\in I} M_i := \{(m_i)_{i\in I} \mid m_i \in M_i \text{ almost all zero}\} \arrow[u, hook] \end{tikzcd}$$

(set-theoretic product of the M_i)

Given $g_i \in \mathrm{Hom}_R(M, M_i)$ $\forall i \in I$, define $g \in \mathrm{Hom}_R(M, \prod_{i\in I} M_i)$ by $g(m) := (g_i(m))_{i\in I}$.

infinitely many of these may be $\neq 0$ so we need $\prod$ (not $\bigoplus$)

Given $f_i \in \mathrm{Hom}_R(M_i, M)$ $\forall i \in I$, define $f \in \mathrm{Hom}_R(\bigoplus_{i\in I} M_i, M)$ by $f((m_i)_{i\in I}) := \sum_{i\in I} f_i(m_i)$ (sum inside M)

only finitely many summands $\neq 0$ since we used $\bigoplus$ (not $\prod$)

$\square$

Ex Let $M \in \mathrm{Mod}(R)$. For any $m_i \in M$ $(i \in I)$ have an epimorphism

$$\bigoplus_{i\in I} R \xrightarrow{\ \varphi\ } \sum_{i \in I} R \cdot m_i \subseteq M$$
$$(a_i)_{i\in I} \longmapsto \sum_{i\in I} a_i m_i .$$

We call M a <u>free R-module</u> (generalizing our previous definition for the case of finite rank)

if the m_i can be chosen sth

- they generate M (ie $\sum_{i\in I} R m_i = M$), and
- they satisfy no R-linear relation (ie $\ker \varphi = 0$),

i.e. sth

$$\varphi : \bigoplus_{i \in I} R \xrightarrow{\ \sim\ } M .$$

We then say the m_i $(i \in I)$ form a <u>basis</u> of the free R-module M.

<u>Caution:</u> Most modules are not free (unless R is a field) & most submodules are not direct summands ($\not\oplus$), eg think of the $\mathbb{Z}$-submodule $n\mathbb{Z} \hookrightarrow \mathbb{Z}$ $(n > 1)$. Such defects are studied in "homological algebra".

7. Tensor products (Multilinear algebra)

Let R be a ring.

Def For $M, N, T \in \mathrm{Mod}(R)$ a map $M \times N \xrightarrow[f]{} T$ is <u>R-bilinear</u>

if $\forall m \in M: \quad f(m, \cdot) \in \mathrm{Hom}_R(N, T)$

$\forall n \in N: \quad f(\cdot, n) \in \mathrm{Hom}_R(M, T)$.

Thm Let $M, N \in \mathrm{Mod}(R)$.

$\Rightarrow \exists!!$ R-module $M \otimes_R N$ (called the "tensor product" of M and N)

w/ a bilinear map

$$\otimes : M \times N \longrightarrow M \otimes_R N$$
$$(m, n) \longmapsto m \otimes n$$

over which any other bilinear map $f : M \times N \to T$ factors uniquely:

$$\begin{tikzcd} M \times N \arrow[r, "f"] \arrow[dr, "\otimes"'] & T \\ & M \otimes_R N \arrow[u, dashed, "\exists! \bar{f}"'] \end{tikzcd}$$

Pf. Uniqueness clear by universal property.

Existence:

Put $F := \bigoplus_{(m,n)\in M\times N} R$ the free R-module on the set $M\times N$,

w/ basis vectors $e_{m,n}$ indexed by $(m,n)\in M\times N$.

Its elements are finite sums $\sum_{\substack{m\in M\\ n\in N}} a_{m,n}\, e_{m,n}$ w/ $a_{m,n}\in R$ (almost all zero).

Let $F_0 \hookrightarrow F$ be the R-submodule generated by all elements

- $e_{m+m',n} - e_{m,n} - e_{m',n}$
- $e_{m,n+n'} - e_{m,n} - e_{m,n'}$
- $e_{am,n} - a\cdot e_{m,n}$
- $e_{m,an} - a\cdot e_{m,n}$

w/ $m,m'\in M$, $n,n'\in N$, $a\in R$.

Put $$M\otimes_R N := F/F_0,$$

and for $(m,n)\in M\times N$ write $m\otimes n := (e_{m,n} \bmod F_0)\in M\otimes N$

$\Rightarrow$ The map $M\times N \longrightarrow M\otimes N$, $(m,n)\mapsto m\otimes n$

is R-bilinear by def^n of F_0.

Furthermore, any map $f: M\times N \to T$ extends uniquely to an R-linear map $\tilde{f}: R^{M\times N} = F \longrightarrow T$ via $\tilde{f}(e_{m,n}) := f(m,n)$, and we have:

$$f \text{ is } R\text{-bilinear iff } \tilde{f}|_{F_0} = 0,$$

in which case $\tilde{f}$ factors uniquely over $M\otimes_R N = F/F_0$. $\square$

Rem 1) We simply write $M\otimes N := M\otimes_R N$ when R is clear from the context.

3) The notation $m\otimes n$ makes sense only if we specify the tensor product $M\otimes_R N$ in which it should live:

e.g. take $R = \mathbb{Z}$

$M = \mathbb{Z} \supset M' = 2\mathbb{Z} \ni 2$

$N = \mathbb{Z}/2\mathbb{Z} \ni \bar{1}$

then $2\otimes\bar{1} = 1\otimes 2\cdot\bar{1} = 0$ in $M\otimes_R N$

but $2\otimes\bar{1} \neq 0$ in $M'\otimes_R N$.

use part a) of the next lemma

$\Rightarrow$ here the map $M'\otimes N \xrightarrow{\text{incl}\otimes\text{id}} M\otimes N$ is NOT injective!

4) $\mathbb{Z}/2\otimes\mathbb{Z}/3 \simeq \{0\}$.

(hint: $\gcd = mx+ny$ with $x,y\in\mathbb{Z}$...)

In general, $\mathbb{Z}/m \otimes_{\mathbb{Z}} \mathbb{Z}/n \xrightarrow[\exists]{\sim} \mathbb{Z}/\gcd(m,n) \ni ab$

(exercise)

$\mathbb{Z}/m\times\mathbb{Z}/n \ni (a,b)$

2) Concretely, any element of $M \otimes N$ can be written as $\sum_{i=1}^{n} m_i \otimes n_i$ with $m_i \in M$, $n_i \in N$.

Usually we cannot achieve $n = 1$ though.

Elements of the form $m \otimes n$ are called "elementary tensors" and satisfy

$$a \cdot (m \otimes n) = am \otimes n = m \otimes an$$
$$(m + m') \otimes n = m \otimes n + m' \otimes n$$
$$m \otimes (n + n') = m \otimes n + m \otimes n' \quad \text{(by def}^{n}\text{)}.$$

<u>Lemma</u> Let $M, N, T \in \mathrm{Mod}(R)$, then $\exists$ natural iso's

a) Unity: $R \otimes_R M \xrightarrow{\sim} M$, $a \otimes m \longmapsto am$

b) Commutativity: $M \otimes_R N \xrightarrow{\sim} N \otimes_R M$, $m \otimes n \longmapsto n \otimes m$

c) Associativity:

$$(M \otimes_R N) \otimes_R T \xrightarrow{\sim} M \otimes_R (N \otimes_R T),$$
$$(m \otimes n) \otimes t \longmapsto m \otimes (n \otimes t).$$

Pf. a) Take $R \times M \longrightarrow M$, $(a, m) \longmapsto am$ which is R-bilinear

$\Rightarrow$ factors over $R \otimes_R M \xrightarrow{u} M$ with $a \otimes m \longmapsto am$.

The map $M \xrightarrow{v} R \otimes_R M$, $m \longmapsto 1 \otimes m$ is R-linear with $uv = \mathrm{id}_M$ and $vu = \mathrm{id}_{R \otimes M}$.

b) Consider

$$\begin{tikzcd}
M \times N \arrow[r, "\text{flip}"] \arrow[d, "\otimes"'] \arrow[dr, "R\text{-bilinear}"] & N \times M \arrow[r, "\text{flip}"] \arrow[d, "\otimes"] \arrow[dr, "R\text{-bilinear}"] & M \times N \arrow[d, "\otimes"] \\
M \otimes_R N \arrow[r, dashed, "\exists!\,\alpha"'] & N \otimes_R M \arrow[r, dashed, "\exists!\,\beta"'] & M \otimes_R N
\end{tikzcd}$$

By uniqueness $\beta\alpha = \mathrm{id}$, similarly $\alpha\beta = \mathrm{id}$. $\square$

c) Similar (exercise).

<u>Rem.</u> The properties a, b, c in the lemma (+ various compatibilities) can be formalized in the abstract notion of a <u>tensor category</u>, including the following

<u>Lemma.</u> For $M, M_i \in \mathrm{Mod}(R)$ ($i \in I$ any index family), $\exists$ natural iso

$$\Big(\bigoplus_{i \in I} M_i\Big) \otimes_R M \simeq \bigoplus_{i \in I} (M_i \otimes_R M)$$

("Distributivity").

Pf. Let $\iota_i : M_i \hookrightarrow \bigoplus_{j \in I} M_j$ be the inclusion

$\Rightarrow$ $\iota_i \otimes \mathrm{id} : M_i \otimes_R M \longrightarrow \big(\bigoplus_j M_j\big) \otimes_R M$

Sum over all i, using universal property of $\bigoplus_i (\cdots)$:

Get natural map

$$\bigoplus_{i\in I} M_i \otimes_R M \xrightarrow{\varphi} \Big(\bigoplus_{i\in I} M_i\Big) \otimes_R M$$

$$(m_i \otimes m)_{i\in I} \xleftarrow{\psi} (m_i)_{i\in I} \otimes m$$

by universal property of $\otimes$

Check $\psi\varphi = id$ and $\varphi\psi = id$ ... (exercise). $\square$

<u>Rem.</u> The analog for infinite products fails in general:

We have a canonical map

$$\psi : \Big(\prod_{i\in I} M_i\Big) \otimes_R M \longrightarrow \prod_{i\in I} M_i \otimes_R M$$

but it needn't be injective, eg. for $M_i := \mathbb{Z}/p^i\mathbb{Z}$

nor surjective, eg. for $M_i := \mathbb{Z}$

where in both cases $R := \mathbb{Z}$, $I := \mathbb{N}$, $M := \mathbb{Q}$

(exercise)

8. Change of rings (more fun with tensors)

For a ring homomorphism $f : A \to B$ we have the "<u>restriction of scalars</u>" functor

$$f_* : \mathrm{Mod}(B) \longrightarrow \mathrm{Mod}(A)$$

where $f_* N := N$ as an abelian gp

w/ scalar multiplication $a \cdot n := f(a)\cdot n$ $\forall a \in A,\ n \in N$

<u>Ex</u> If $f : A \hookrightarrow B$ is an embedding, then sometimes f_* is called "forgetful functor" since it forgets some of the structure,

e.g. $\mathrm{Vect}(\mathbb{Q}) = \mathrm{Mod}(\mathbb{Q}) \to \mathrm{Mod}(\mathbb{Z}) = \mathrm{AbGps}$.

Can we go back?

Given $M \in \mathrm{Mod}(A)$, put $f^* M := M \otimes_A B$ as abelian gp.

(B viewed as an A-module via $f : A \to B$)

For $b \in B$ have

$$\begin{tikzcd} M \times B \arrow[r, "A\text{-bilinear}"', "(m,c)\mapsto m\otimes bc"] \arrow[d] & M \otimes_A B \\ M \otimes_A B \arrow[ur, dashed, "\exists!\ id\otimes b\cdot id"'] & \end{tikzcd}$$

$\rightsquigarrow$ defines a "scalar mult^n by b" on f^*M!

$\Rightarrow$ get an "extension of scalars" functor

$$f^* : \mathrm{Mod}(A) \longrightarrow \mathrm{Mod}(B).$$

Universal property:

Prop The functor f^* is left adjoint to f_*,

i.e. $\exists$ natural iso

$$\mathrm{Hom}_A(M, f_* N) \cong \mathrm{Hom}_B(f^* M, N)$$

for all $M \in \mathrm{Mod}(A)$, $N \in \mathrm{Mod}(B)$.

Pf. Given $\varphi \in \mathrm{Hom}_A(M, f_* N)$ (i.e. an A-linear map $\varphi: M \to N$),

consider

$$\begin{tikzcd} M \times B \arrow[rr, "A\text{-bilinear!}", "(m,b) \mapsto b\cdot\varphi(m)"'] \arrow[dr] & & N \\ & M \otimes_A B \arrow[ur, dashed, "\exists!\,\tilde\varphi"'] & \end{tikzcd}$$

$\rightsquigarrow$ $\tilde\varphi \in \mathrm{Hom}_B(f^* M, N)$.

Conversely, given $\tilde\varphi$ put $\underbrace{\varphi := \tilde\varphi \circ \iota}_{\in\, \mathrm{Hom}_A(M, f_* N)}$ where $\iota: M \longrightarrow M \otimes_A B$, $m \longmapsto m \otimes 1$

These two assignments are mutually inverse. $\square$

Ex For $M \in \mathrm{AbGps} = \mathrm{Mod}(\mathbb{Z})$ & $N \in \mathrm{Vect}(\mathbb{Q}) = \mathrm{Mod}(\mathbb{Q})$, have

$$\mathrm{Hom}_{\mathrm{AbGps}}(M, N) \cong \mathrm{Hom}_{\mathrm{Vect}(\mathbb{Q})}(M \otimes_{\mathbb{Z}} \mathbb{Q}, N).$$

Ex For $\mathfrak{m} \in \mathrm{Spm}(A)$ w/ residue field $k := A/\mathfrak{m}$, the quotient map $f: A \twoheadrightarrow k$ induces

$$f_* : \mathrm{Mod}(A) \longrightarrow \mathrm{Vect}(k)$$

(much easier to study!)

Ex For $S \subset A$ a multiplicative subset & $M \in \mathrm{Mod}(A)$ define the localization

$$M_S := (M \times S)/\sim \quad \in \mathrm{Mod}(A_S)$$

where

$(m,s) \sim (m',s') :\Leftrightarrow \exists\, t \in S : t \cdot (s'm - sm') = 0$ in M,

with scalar multiplicat^n

$\frac{a}{s} \cdot \frac{m}{t} := \frac{am}{st}$ for $\frac{a}{s} \in A_S$, $\frac{m}{t} := ((m,t) \bmod \sim) \in M_S$,

then we have:

Lemma $\exists$ natural iso $M \otimes_A A_S \xrightarrow{\sim} M_S$.

Pf.

$$\begin{tikzcd} M \times A_S \arrow[rr, "A\text{-bilinear}", "(m,\frac{a}{s}) \mapsto \frac{am}{s}"'] \arrow[dr, "\otimes"'] & & M_S \\ & M \otimes_A A_S \arrow[ur, dashed, "\exists ! \varphi"'] & \end{tikzcd}$$

Inverse: $\psi : M_S \longrightarrow M \otimes_A A_S$, $\frac{m}{s} \mapsto m \otimes \frac{1}{s}$

is well-defined:

$\frac{m}{s} = \frac{m'}{s'}$ in M_S $\Rightarrow \exists t \in S : ts'm - tsm' = 0$ in M

$\Rightarrow (m \otimes \frac{1}{s} - m' \otimes \frac{1}{s'}) \cdot \underbrace{ss't}_{\in A_S^*} = 0$ in $M \otimes_A A_S$

$\Rightarrow m \otimes \frac{1}{s} - m' \otimes \frac{1}{s'} = 0$ in $M \otimes_A A_S$. $\square$

Rem. a) $\ker(M \to M_S) = \{ m \in M \mid \exists s \in S : sm = 0 \}$.
$\quad m \mapsto \frac{m}{1}$

b) If $f \in \mathrm{Hom}_A(M,N)$ is $\begin{cases} \text{mono} \\ \text{epi} \\ \text{iso} \end{cases}$ then $f_S \in \mathrm{Hom}_{A_S}(M_S, N_S)$ is so.

Pf. a) obvious.
b) for "epi" this holds for any extension of coeff^s functor.
For "mono" assume $f : M \hookrightarrow N$. Let $\frac{m}{s} \in M_S$ with $f_S(\frac{m}{s}) = 0$,
then $\exists t \in S : t \cdot f(m) = 0$ in N, so $tm \in \ker(f) = \{0\}$
$\Rightarrow \frac{m}{s} = 0$ in M_S. $\square$

Upshot: For any $\wp \in \mathrm{Spec}\, A$ w/ localization $A_\wp$
& residue field $k(\wp) := A_\wp / \wp A_\wp$,

coefficient extension gives functors

$$\begin{array}{ccccc} \mathrm{Mod}(A) & \xrightarrow{\otimes A_\wp} & \mathrm{Mod}(A_\wp) & \xrightarrow{\otimes k(\wp)} & \mathrm{Vect}(k(\wp)) \\ \wr & & \wr & & \wr \\ \text{maybe hard} & \rightsquigarrow & \text{easier} & \rightsquigarrow & \text{very simple} \end{array}$$

The localization functor keeps all information:

Lemma. The natural map $M \hookrightarrow \prod_{m \in \mathrm{Spm}\, A} M_m$ is injective.

In particular, $M = 0$ iff $M_m = 0$ $\forall m \in \mathrm{Spm}\, A$.

Pf. Assume $x \in M$ maps to $\frac{x}{1} = 0 \in M_m$ $\forall m \in \mathrm{Spm}\, A$, i.e.
$\exists a_m \in A \setminus m$ sth $a_m \cdot x = 0$ in M.

Note: $\mathfrak{a} := (a_m \mid m \in \mathrm{Spm}\, A) \trianglelefteq A$ is not contained in any
maximal ideal $m_0 \in \mathrm{Spm}\, A$, since $a_{m_0} \in \mathfrak{a}$.

$\Rightarrow \mathfrak{a} = (1)$ and hence $x = 1 \cdot x = 0$ in M. $\square$

Q: What about the "quotient functor"
$\mathrm{Mod}(A_m) \longrightarrow \mathrm{Vect}(k(m))$?

e.g. does $M \otimes k(m) \simeq \{0\}$
imply that $M \simeq \{0\}$?

($\rightarrow$ Nakayama's lemma)

9. Nakayama's lemma (the inverse function theorem in algebraic geometry)

Motivation: Suppose $M, N \in \mathrm{Mod}(R)$

$f \in \mathrm{Hom}_R(M,N)$ is $\begin{cases} \text{mono} \\ \text{epi} \end{cases}$

iff $\begin{cases} \ker(f) \cong 0 \\ \mathrm{cok}(f) := N/\mathrm{im}(f) \cong 0. \end{cases}$

$\Rightarrow$ Want a criterion for an R-module to be isomorphic to zero.

Def An R-module M is called *cyclic* if $\exists\, m \in M$ with $M = R \cdot m$. Then $f : R \twoheadrightarrow M,\ a \mapsto am$ is epi with $\ker(f) = \mathrm{Ann}(m) := \{a \in R \mid am = 0\} \trianglelefteq R$

(the "annihilator of m in R")

$\Rightarrow$ $M \in \mathrm{Mod}(R)$ is cyclic iff $M \simeq R/\mathfrak{a}$ for some $\mathfrak{a} \trianglelefteq R$.

Note If M is cyclic and $I \subseteq \mathrm{Ann}(M) := \{a \in R \mid am = 0\ \forall m \in M\}$ is an ideal with

$$I \cdot M = M,$$

then $M \simeq \{0\}$ (obviously).

Lemma. Any finitely generated module $M \in \mathrm{Mod}(R)$, $M \not\simeq \{0\}$, has a non-zero cyclic quotient $M \twoheadrightarrow Q \simeq R/\mathfrak{a}$, for some $\mathfrak{a} \underset{\neq}{\trianglelefteq} R$.

Pf. Pick a set of generators $m_1, \dots, m_n \in M$ with $n \in \mathbb{N}$ minimal ($n > 0$ since $M \not\simeq \{0\}$).

$\Rightarrow$ $N := Rm_1 + \dots + Rm_{n-1} \xhookrightarrow{\neq} M = Rm_1 + \dots + Rm_n$

$\Rightarrow$ $Q := M/N \not\simeq \{0\}$

but by construction $Q = R \cdot \overline{m}_n$ for the image $\overline{m}_n := m_n \bmod N$. $\square$

Rem Can assume $\mathfrak{a} = \mathfrak{m} \in \mathrm{Spm}\, R$ is a maximal ideal after replacing Q by an even smaller quotient.

Ex For $R = \mathbb{Z}$ the lemma says:

Any fin. gen. abelian gp $M \not\simeq \{0\}$ admits a quotient $M \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}$ for some prime p.

⚠ Finite generation is essential here, eg. the group $M = \mathbb{Q}$ has no quotient $\mathbb{Z}/p\mathbb{Z}$ ($\mathbb{Q}$ is a divisible gp while $\mathbb{Z}/p\mathbb{Z}$ is not: the only element of the form $x = p \cdot y$ w/ $y \in \mathbb{Z}/p\mathbb{Z}$ is the zero element)

Nakayama's lemma (version I) $M \in \mathrm{Mod}(R)$ fin. gen.
& $I \cdot M = M$
for some ideal $I \subseteq \mathrm{Jac}(R)$
$\Rightarrow M \simeq \{0\}$.

Pf. M fin. gen. $\Rightarrow \exists\, m_0 \in \mathrm{Spm}\, R$ and $\exists f: M \twoheadrightarrow Q := R/m_0$

But $I \subseteq \mathrm{Jac}\, R = \bigcap_{m \in \mathrm{Spm} R} m \subseteq m_0 \Rightarrow I \cdot Q = \{0\}$

$\Rightarrow I \cdot M \subseteq \ker(f)$

contradicting $IM = M$ $\lightning$ $\square$

NB This is useful if $\mathrm{Jac}(R)$ is big.
If $\mathrm{Jac}(R) = \{0\}$ it says nothing,
so we should first localize!

Nakayama's lemma (version II) R local ring
w/ max. ideal m,
residue field $k(m) = R/m$
$M \in \mathrm{Mod}(R)$ fin. gen.

then a) $M \otimes_R k(m) \cong \{0\} \Rightarrow M \cong \{0\}$

b) $N \subseteq M$ submodule w/ $M = N + m \cdot M \Rightarrow N = M$.

c) If $m_1, \dots, m_n \in M$ lift a basis $\bar{m}_1, \dots, \bar{m}_n$ of $M \otimes_R k(m)$
then $M = Rm_1 + \dots + Rm_n$.

Pf.

b) $\Rightarrow$ a): $M \otimes_R k(m) = M \otimes_R R/m = M/m \cdot M \cong \{0\}$

implies
$M = m M$
so we can
take $N = \{0\}$ in b)
to get $M = N = \{0\}$.

Exercise:
$M \otimes_R R/m \xrightarrow{\sim} M/mM$
via $x \otimes (a \bmod m) \mapsto ax \bmod mM$
$y \otimes (1 \bmod m) \leftarrow y \bmod mM$

b) $\Rightarrow$ c): Take $N := Rm_1 + \dots + Rm_n \subseteq M$
then $M = N + mM$
because $\bar{m}_1, \dots, \bar{m}_n$ generate M/mM,
hence $N = M$ by b).

b): $M = N + mM$ means $m \cdot Q = Q$
where $Q := M/N \in \mathrm{Mod}(R)$
(fin. gen.)

Nakayama I applied to Q & to $m = \mathrm{Jac}(R)$ (R local!) $\square$
implies $Q \simeq \{0\}$, so $N = M$.

Rem. ① Part c) is a kind of "inverse function thm":

e.g. take k a field,

$R := (k[X_1, \dots, X_n])_{\mathfrak{m}}$ for the max. ideal $\mathfrak{m} := (X_1, \dots, X_n)$

$M := \mathfrak{m}$ as an R-module
= "functions on $\mathbb{A}^n(k)$ vanishing at the origin"

then

$$M \otimes_R k(\mathfrak{m}) = M/\mathfrak{m}M = \mathfrak{m}/\mathfrak{m}^2$$

= "linear terms of Tayor series"

= cotangent space to $\mathbb{A}^n(k)$ at the origin,

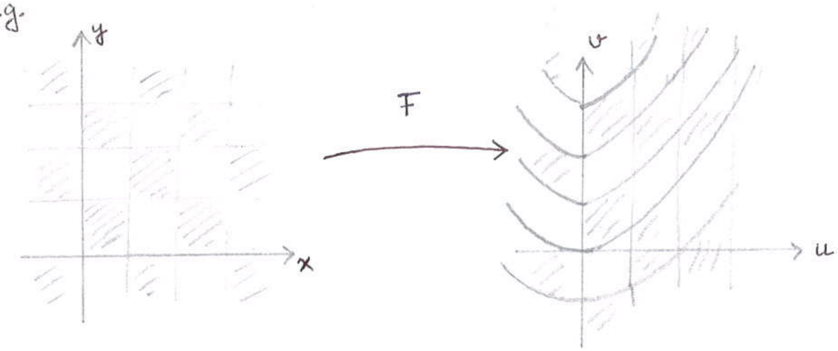
and Nakayama says:

If $f_1, \dots, f_n \in \mathfrak{m}$ are functions whose "differentials" $f_i'(0) := [f_i] \in \mathfrak{m}/\mathfrak{m}^2$ are linearly independent over $k = k(\mathfrak{m})$,

then $\mathfrak{m} = Rf_1 + \dots + Rf_n$.

("ie. $(f_1, \dots, f_n)$ behave a bit like a system of local coordinates near the origin")

e.g.

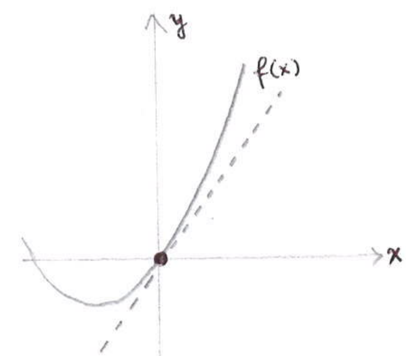


$$F(x,y) := (f_1(x,y), f_2(x,y)) := (x, y + x^2)$$

Here $(f_1'(0), f_2'(0)) = \begin{pmatrix} 1 & 2x \\ 0 & 1 \end{pmatrix}\Big|_{(x,y)=(0,0)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$\Longrightarrow$ $f_1'(0)$ & $f_2'(0)$ are linearly independent in $\mathfrak{m}/\mathfrak{m}^2 \cong k^2$

Warning: In general $\mathfrak{m} = Rf_1 + \dots + Rf_n$ does NOT imply that $(f_1, \dots, f_n) : \mathbb{A}^n(k) \to \mathbb{A}^n(k)$ has an inverse given by polynomials (even locally), think of $n = 1$ and $f(x) = (x+1)^2 - 1$



$f'(0) = 2(x+1)|_{x=0} = 2 \neq 0$

but

$y \mapsto$ "$\sqrt{y+1} - 1$"

is NOT a rational fct^n ...

Rem ② Part c) of Nakayama II does NOT imply that a module $M \in \mathrm{Mod}(R)$ is fin. gen. if $M \otimes_R k(m)$ is so. On the contrary:

Cor. If R is an integral domain which is not a field, then $k := \mathrm{Quot}(R)$ is not fin. gen. as an R-module.

Pf. Assume k fin.gen as R-module

$\Longrightarrow$ k fin.gen as R_m-module, for any $m \in \mathrm{Spm}(R)$

But if R is not a field, then $m \neq 0$,

so $I := m R_m \trianglelefteq R_m$ satisfies $I \cdot k = k$

Since $I \subseteq \mathrm{Jac}(R_m)$, Nakayama I implies $k = 0$ ↯ $\square$

Ex. $M := \mathbb{Q}$ is NOT fin. gen. as a module over $R := \mathbb{Z}_{(p)}$ for p prime, though

$$M \otimes_R R/m = \mathbb{Q} \otimes_{\mathbb{Z}_{(p)}} \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \simeq \mathbb{Q}/p \cdot \mathbb{Q} = \{0\}$$

($\Rightarrow$ Nakayama badly fails for modules that are not finitely generated).

Nakayama's lemma (version III) Let R be a ring (not necessarily local) $M \in \mathrm{Mod}(R)$ fin. gen. s.th. $I \cdot M = M$ for some ideal $I \trianglelefteq R$ (not necessarily $\subseteq \mathrm{Jac}(R)$).

$\Longrightarrow \exists\, i \in I$: For all $m \in M$, $im = m$.

(Mnemonic: $IM = M \Rightarrow im = m$)

Pf. Must see: $\exists\, s \in R$ with $s \equiv 1 \bmod I$ and $s \cdot M = \{0\}$

(then put $i := 1 - s \in I$).

Consider the set

$$S := 1 + I := \{1 + a \mid a \in I\} \subseteq R.$$

$\Longrightarrow$ S is multiplicative because I is an ideal

For any $\frac{a}{s} \in I R_S$ and all $\frac{b}{t} \in R_S$ $\quad (a \in I, b \in R, s, t \in S)$ we have

$$1 + \frac{a}{s} \cdot \frac{b}{t} = \frac{1}{st} \cdot \underbrace{(\underset{\substack{\cap \\ 1+I}}{st} + \underset{\substack{\cap \\ I}}{ab})}_{\in 1 + I = S} \in R_S^*$$

$\Longrightarrow\ I\cdot R_S \subseteq \{ x \in R_S \mid 1 + xy \in R_S^* \ \forall y \in R_S \} = \mathrm{Jac}(R_S)$

But by assumption $IM = M$

so $IR_S \cdot M_S = M_S$ and $M_S \in \mathrm{Mod}(R_S)$ is still fin.gen.

$\Longrightarrow\ M_S = \{0\}$ by Nakayama I $(*)$

Pick generators $m_1, \dots, m_n$ with $M = Rm_1 + \dots + Rm_n$

then by $(*)$ there exist $s_i \in S$ with $s_i \cdot m_i = 0$ in M

$\Longrightarrow\ s := s_1 \cdots s_n \in S$ satisfies $s \cdot m_i = 0 \ \forall i,$

hence $s \cdot M = \{0\}$. $\square$

Here's a fun application:

<u>Cor.</u> Let $M \in \mathrm{Mod}(R)$ be fin. gen.

$\Longrightarrow$ any epimorphism $f: M \twoheadrightarrow M$ is an iso.

Pf. Given $f \in \underset{\mathrm{End}_R(M)}{\mathrm{Hom}_R(M,M)}$, regard M as an $R[X]$-module

via $P(X)\cdot m := P(f)(m)$

for $P(X) \in R[X]$, $m \in M$.

f epi $\Longrightarrow\ X\cdot M = M$

$\Longrightarrow$ by Nakayama III for $I := (X) \trianglelefteq R[X]$,

$\exists P(X) \in R(X)$ sth $\underbrace{X \cdot P(X)}_{=: i \in I} \cdot m = m \ \forall m \in M$

$\Longrightarrow\ g := P(f) \in \mathrm{End}_R(M)$

satisfies $g \circ f = f \circ g = \mathrm{id}_M$ $\square$

<u>Rem.</u> The analogous statement for monomorphisms is obviously false, think of $f: \mathbb{Z} \hookrightarrow \mathbb{Z},\ n \mapsto 2n$.

<u>Cor</u> If $M \simeq R^n$ is a free R-module of rk n, then any set of n generators is a basis.

Pf. Consider the epi $R^n \twoheadrightarrow M \simeq R^n$

$(a_i)_{i=1,\dots,n} \longmapsto \sum_{i=1}^n a_i m_i$ for $M = Rm_1 + \dots + Rm_n$. $\square$

II. Finiteness Conditions

1. Some homological algebra (the snake lemma)

R ring

<u>Def</u> A sequence $M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} \cdots \xrightarrow{f_n} M_{n+1}$ in $\mathrm{Mod}(R)$ is called <u>exact</u> if

$$\mathrm{im}(f_{i-1}) = \ker(f_i) \quad \forall i \in \{1, \dots, n\}.$$

<u>Ex</u>
- $0 \to M' \xrightarrow{f} M$ is exact iff f is mono
- $M \xrightarrow{g} M'' \to 0$ is exact iff g is epi
- $0 \to M \xrightarrow{h} N \to 0$ is exact iff h is iso

<u>Def</u> By a <u>short exact sequence</u> we mean an exact sequence $0 \to M' \xrightarrow[f]{} M \xrightarrow[g]{} M'' \to 0$

ie one where
- f mono
- g epi
- $\mathrm{im}(f) = \ker(g)$

Rem Any mono $f : M' \hookrightarrow M$ fits into $0 \to M' \xrightarrow{f} M \to \mathrm{cok}(f) \to 0$ for the cokernel $\mathrm{cok}(f) := M/_{\mathrm{im}(f)}$.

Any epi $g : M \twoheadrightarrow M''$ fits into $0 \to \ker(g) \to M \to M'' \to 0$.

Any short exact sequence arises like this up to iso:

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r] \arrow[d, equal] & M \arrow[r] \arrow[d, equal] & \mathrm{cok}(f) \arrow[r] \arrow[d, "\exists! \wr"] & 0 \\
0 \arrow[r] & M' \arrow[r, "f"] & M \arrow[r, "g"] & M'' \arrow[r] & 0 \\
0 \arrow[r] & \ker(g) \arrow[r] \arrow[u, "\wr \exists!"] & M \arrow[r] \arrow[u, equal] & M'' \arrow[r] \arrow[u, equal] & 0
\end{tikzcd}$$

Def A <u>morphism</u> between s.e. sequences $0 \to M_i' \xrightarrow{f_i} M_i \xrightarrow{g_i} M_i'' \to 0$ is a commutative diagram in $\mathrm{Mod}(R)$,

$$\begin{tikzcd}
0 \arrow[r] & M_1' \arrow[r, "f_1"] \arrow[d, "\varphi'"] & M_1 \arrow[r, "g_1"] \arrow[d, "\varphi"] & M_1'' \arrow[r] \arrow[d, "\varphi''"] & 0 \\
0 \arrow[r] & M_2' \arrow[r, "f_2"'] & M_2 \arrow[r, "g_2"'] & M_2'' \arrow[r] & 0
\end{tikzcd}$$

We call it an <u>isomorphism</u> if $\varphi, \varphi', \varphi''$ are iso's.

Def A short exact sequence is called <u>split</u> if it is isomorphic to a sequence

$$0 \to M' \underset{\substack{\text{inclusion} \\ m' \mapsto (m',0)}}{\longrightarrow} M' \oplus M'' \underset{\substack{\text{projection} \\ (m',m'') \mapsto m''}}{\longrightarrow} M'' \to 0$$

Lemma For a short exact sequence $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$, the following are equivalent:

a) It splits.

b) $\exists$ "<u>section</u>" $s \in \mathrm{Hom}_R(M'', M)$ w/ $g \circ s = \mathrm{id}_{M''}$.

c) $\exists$ "<u>retraction</u>" $p \in \mathrm{Hom}_R(M, M')$ w/ $p \circ f = \mathrm{id}_{M'}$.

Pf. a) $\Rightarrow$ b) & c) via $s(m'') := (0, m'')$,
$p(m', m'') := m'$.

b) $\Rightarrow$ a):

Given a section $s : M'' \to M$,

consider

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "\mathrm{incl}"] \arrow[d, equal] & M' \oplus M'' \arrow[r, "\mathrm{pr}"] \arrow[d, "f \oplus s"] & M'' \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & M' \arrow[r, "f"'] & M \arrow[r, "g"'] & M'' \arrow[r] & 0
\end{tikzcd}$$

Claim 1: $f \oplus s$ mono, indeed $f(M') \cap s(M'') = 0$ $\quad m'' := g(m)$

Claim 2: $f \oplus s$ epi, indeed $\forall m \in M$, $m - s(m'') \in \ker(g) = \mathrm{im}(f)$

$\Rightarrow \exists\, m' \in M' : \ m - s(m'') = f(m')$

$\Rightarrow (f \oplus s)(m', m'') = f(m') + s(m'') = m.$

$\square$

c) $\Rightarrow$ a): Similar (exercise).

Rem The main purpose of homological algebra is to deal with non-split sequences.

The above proof is a special case of the

"Snake lemma" Consider a comm. diagram

$$\begin{tikzcd} & M_1' \arrow[r, "f_1"] \arrow[d, "\varphi'"] & M_1 \arrow[r, "g_1"] \arrow[d, "\varphi"] & M_1'' \arrow[r] \arrow[d, "\varphi''"] & 0 \\ 0 \arrow[r] & M_2' \arrow[r, "f_2"'] & M_2 \arrow[r, "g_2"'] & M_2'' & \end{tikzcd}$$

w/ exact rows

$\Longrightarrow$ $\exists$ exact sequence

$$\ker(\varphi') \xrightarrow{f_0} \ker(\varphi) \xrightarrow{g_0} \ker(\varphi'') \xrightarrow{\exists\,\delta} \operatorname{cok}(\varphi') \xrightarrow{f_3} \operatorname{cok}(\varphi) \xrightarrow{g_3} \operatorname{cok}(\varphi'')$$

making the diagram

$$\begin{tikzcd} & \ker\varphi' \arrow[r] \arrow[d, "i'"'] & \ker\varphi \arrow[r] \arrow[d, "i"'] & \ker\varphi'' \arrow[d, "i''"'] \arrow[lldddd, rounded corners, "\delta"] & \\ & M_1' \arrow[r] \arrow[d] & M_1 \arrow[r] \arrow[d] & M_1'' \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & M_2' \arrow[r] \arrow[d, "p'"'] & M_2 \arrow[r] \arrow[d, "p"'] & M_2'' \arrow[d, "p''"'] & \\ & \operatorname{cok}\varphi' \arrow[r] & \operatorname{cok}\varphi \arrow[r] & \operatorname{cok}\varphi'' & \end{tikzcd}$$

[i', i, i'': the natural inclusions

p', p, p'': the natural quotient maps]

commute. Moreover, f_0 is mono if f_1 is so, and g_3 is epi if g_2 is so.

Pf.

① Construction of f_0, g_0 & exactness at $\ker(\varphi)$:

- For f_0, apply universal property of $\ker(\varphi)$ to $N := \ker(\varphi')$:

$$\operatorname{Hom}(N, \ker(\varphi)) \xrightarrow[i\circ(-)]{\sim} \{ f \in \operatorname{Hom}_R(N, M_1) \mid \varphi \circ f = 0 \}$$

$$\exists!\, f_0 \longmapsto f := f_1 \circ i'$$

because

$$\varphi \circ f = \varphi \circ f_1 \circ i' = f_2 \circ \underbrace{\varphi' \circ i'}_{=0} = 0$$

By construction $i \circ f_0 = f_1 \circ i'$.

- Similarly get a unique g_0 with $i'' \circ g_0 = g_1 \circ i$.

- Exactness at $\ker(\varphi)$:

Clearly $g_0 \circ f_0 = 0$ because $i'' \circ g_0 \circ f_0 = \underbrace{g_1 \circ f_1}_{=0} \circ i' = 0$,

so $\operatorname{im}(f_0) \subseteq \ker(g_0)$.

Conversely: Let $k_0 \in \ker(g_0)$

$\Longrightarrow$ $i(k_0) \in \ker(g_1) = \operatorname{im}(f_1)$,

say $i(k_0) = f_1(m_1')$ with $m_1' \in M_1'$

Want: $\varphi'(m_1') = 0$,

which follows from $f_2(\varphi'(m_1')) = \varphi(\underbrace{f_1(m_1')}_{\substack{= i(k_0) \\ \in \ker(\varphi)}}) = 0$

(using that f_2 is mono!)

② Construction of f_3, g_3 & exactness at $\mathrm{cok}(\varphi)$:

Dual argument, apply universal property of $\mathrm{cok}\,\varphi$ to $N := \mathrm{cok}\,\varphi''$:

$$\mathrm{Hom}(\mathrm{cok}\,\varphi, N) \xrightarrow[(-)\circ p]{\sim} \{ g \in \mathrm{Hom}_R(M_2, N) \mid g \circ \varphi = 0 \}$$

$$\exists!\, g_3 \longmapsto g := p'' \circ g_2$$

because

$$g \circ \varphi = p'' \circ g_2 \circ \varphi = \underbrace{p'' \circ \varphi''}_{=0} \circ g_1 = 0$$

Get unique f_3, g_3

with $f_3 \circ p' = p \circ f_2$

$g_3 \circ p = p'' \circ g_2$

& exactness $\ker(g_3) = \mathrm{im}(f_3)$ follows from g_1 being epi (exercise).

③ The "connecting map" δ:

Given $k'' \in \ker(\varphi'')$,

write $i''(k'') = g_1(m_1)$ w/ $m_1 \in M_1$ (using that g_1 is epi)

$\Rightarrow g_2(\varphi(m_1)) = \varphi''(g_1(m)) = \varphi''(i''(k'')) \underset{\uparrow}{=} 0$

$(\varphi'' \circ i'' = 0)$

$\Rightarrow \varphi(m_1) \in \ker(g_2) = \mathrm{im}(f_2)$,

Say $\varphi(m_1) = f_2(m_2')$ w/ $m_2' \in M_2'$

uniquely determined since f_2 is mono!

We put $\delta(k'') := p'(m_2') \in \mathrm{cok}(\varphi')$.

Check this is well-defined:

Let $\tilde{m}_1 \in M_1$ be another lift of $i''(k'')$,

i.e. $g_1(\tilde{m}_1) = g_1(m_1)$

$\Rightarrow \tilde{m}_1 - m_1 \in \ker(g_1) = \mathrm{im}(f_1)$

$\Rightarrow \tilde{m}_1 = m_1 + f_1(m_1')$ w/ $m_1' \in M_1'$

$\Rightarrow \varphi(\tilde{m}_1) = \varphi(m_1) + \underbrace{\varphi(f_1(m_1'))}_{= f_2(\varphi'(m_1'))}$

$\Rightarrow$ the unique $\tilde{m}_2' \in M_2'$

with $\varphi(\tilde{m}_1) = f_2(\tilde{m}_2')$

satisfies $\tilde{m}_2' = m_2' + \varphi'(m_1')$

$\Rightarrow p'(\tilde{m}_2') = p'(m_2')$ because $p' \circ \varphi' = 0$

④ Exactness at $\ker(\varphi'')$ & $\mathrm{cok}(\varphi')$: Exercise. $\square$

2. Finitely presented modules

<u>Recall</u> $M \in \mathrm{Mod}(R)$ is <u>finitely generated</u> if $\exists$ epi $R^n \overset{p}{\twoheadrightarrow} M$ for some $n \in \mathbb{N}$.

We then also say M is <u>of finite type</u> as an R-module.

⚠ It does NOT follow that $\ker(p)$ is of finite type, think of $M := R/\mathfrak{a}$ for a not fin gen ideal $\mathfrak{a} \trianglelefteq R$.

<u>Def</u> M is <u>of finite presentation</u> if $\exists$ exact sequence

$$R^m \longrightarrow R^n \overset{p}{\longrightarrow} M \longrightarrow 0$$

with $m, n \in \mathbb{N}$ (ie an epi p w/ $\ker(p)$ fin.gen).

<u>Lemma.</u> Consider an exact sequence $0 \to M' \overset{f}{\to} M \overset{g}{\to} M'' \to 0$.

a) M fin gen. $\Longrightarrow$ M'' fin gen.

b1) M', M'' both fin gen. $\Longrightarrow$ M fingen.

b2) — " — fin. pres. $\Longrightarrow$ M fin. pres.

Pf. a) Obvious: $R^n \overset{p}{\twoheadrightarrow} M \overset{g}{\twoheadrightarrow} M''$ is epi

b1)

$$(*)\quad \begin{tikzcd} 0 \arrow[r] & R^{n'} \arrow[r, "\tilde f"] \arrow[d, two heads, "p'"'] & R^{n'+n''} \arrow[r, "\tilde g"] \arrow[d, dashed, "\exists p"] & R^{n''} \arrow[r] \arrow[d, two heads, "p''"] & 0 \\ 0 \arrow[r] & M' \arrow[r, "f"'] & M \arrow[r, "g"'] & M'' \arrow[r] & 0 \end{tikzcd}$$

$\tilde f(e_i) := e_i$, $1 \le i \le n'$

$\tilde g(e_j) := \begin{cases} 0, & j \le n' \\ e_{j-n'}, & j > n' \end{cases}$

To define p, choose any lifts $\begin{array}{ccc} m_j & \longmapsto & p''(e_{j-n'}), \quad j > n' \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ M & \longrightarrow & M'' \end{array}$

Put $m_i := p'(e_i)$, $i \le n'$,

and define

$$p: R^{n'+n''} \longrightarrow M$$

by $e_k \longmapsto m_k$ for $k = 1, \dots, n'+n''$.

$\Longrightarrow$ Diagram $(*)$ commutes & rows are exact,

and p epi by snake lemma.

b2) Choose p', p'' with fingen kernel.

Snake lemma: $0 \to \ker(p') \longrightarrow \ker(p) \longrightarrow \ker(p'') \longrightarrow \underset{\mathrm{cok}(p')}{\overset{0}{\|}}$

$\Longrightarrow$ $\ker(p)$ fin. gen. by an application of b1) w/ $\ker(p'), \ker(p'')$ fingen. $\square$

Rem. Part a) does NOT hold for "fin. pres."

e.g. suppose $\mathfrak{a} \trianglelefteq R$ is not fin. gen.

and put

$$
\begin{aligned}
&M := R \quad (\text{fin. pres.})\\
&\quad \downarrow\!\!\downarrow\\
&M'' := R/\mathfrak{a} \quad (\text{NOT fin. presented, see next proposition with})
\end{aligned}
$$

Prop A module $N \in \mathrm{Mod}(R)$ is fin. pres.

iff
- N is fin. gen., and
- for every epi $f : M \twoheadrightarrow N$ w/ M fin. gen, the kernel $\ker(f)$ is fin. gen.

Pf. "$\Leftarrow$" trivial.

"$\Rightarrow$": Fix a presentation $R^m \xrightarrow{q} R^n \xrightarrow{p} N \to 0$.

Given $f : M \twoheadrightarrow N$,

consider the diagram

$$
\begin{tikzcd}
 & R^m \arrow[r, "q"] \arrow[d, dashed, "\alpha"] & R^n \arrow[r, "p"] \arrow[d, dashed, "\beta"] & N \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \ker(f) \arrow[r] & M \arrow[r, "f"] & N \arrow[r] & 0
\end{tikzcd}
$$

where $\beta(e_i) := (\text{any lift of } p(e_i)) \in M$

$\alpha(e_j) := (\text{any lift of } \beta(q(e_j))) \in \ker(f)$

(using that R^m and R^n are free).

Snake lemma gives exact sequence

(using that f is epi)

$$
\begin{tikzcd}
0 \arrow[r] \arrow[d, equal] & \mathrm{cok}(\alpha) \arrow[r] & \mathrm{cok}(\beta) \arrow[r] & 0 \arrow[d, equal] \\
\ker(\mathrm{id}_N) & & & \mathrm{cok}(\mathrm{id}_N)
\end{tikzcd}
$$

$\Longrightarrow$ $\mathrm{cok}(\alpha) \simeq \mathrm{cok}(\beta)$,

and the latter is fin. gen. (being a quotient of the fin. gen. module M)

Now look at

$$
\begin{tikzcd}
0 \arrow[r] & \mathrm{im}(\alpha) \arrow[r] \arrow[d, phantom, "\rotatebox{90}{$\leadsto$}"] & \ker(f) \arrow[r] & \mathrm{cok}(\alpha) \arrow[r] \arrow[d, phantom, "\rotatebox{90}{$\leadsto$}"] & 0 \\
 & \text{fin. gen. (as quotient of } R^m) & & \text{fin. gen. (see above)} &
\end{tikzcd}
$$

$\underset{\text{previous lemma b1)}}{\Longrightarrow}$ $\ker(f)$ fin. gen. $\square$

3. Noetherian rings and modules

Have seen:
- "fin. gen" is not preserved under taking submodules
- "fin. pres." —— $\shortparallel$ —— submodules / quotients (in general)

Def A module $M \in Mod(R)$ is Noetherian if every submodule $N \subseteq M$ is fin. gen.

Lemma M is Noetherian if it satisfies the "ascending chain condition (acc)":
$\forall$ submodules $M_1 \hookrightarrow M_2 \hookrightarrow \cdots \hookrightarrow M$,
$\exists\, n \in \mathbb{N}$ with $M_n = M_{n+1} = M_{n+2} = \cdots$

Pf. "$\Leftarrow$": Let $N \subseteq M$ not fin. gen.

Pick $n_1 \in N$ and set $M_1 := Rn_1$

$\vdots$ $\qquad\qquad\qquad\qquad\qquad \vdots$

$n_i \in N \setminus M_{i-1}$, set $M_i := M_{i-1} + R \cdot n_i$

Since N is NOT fin. gen., we have $M_i \overset{\neq}{\hookrightarrow} N \;\; \forall i$, so this doesn't terminate.

$\Longrightarrow M_1 \overset{\neq}{\hookrightarrow} M_2 \overset{\neq}{\hookrightarrow} \cdots \hookrightarrow M$ doesn't stabilize

"$\Rightarrow$" Given $M_1 \hookrightarrow M_2 \hookrightarrow \cdots \hookrightarrow M$

consider the R-submodule

$$N := \bigcup_{n \in \mathbb{N}} M_n \hookrightarrow M.$$

If M is Noetherian, then N is fin. gen, say $N = \sum_{i=1}^{k} Rm_i$

$\Longrightarrow \exists\, n: \quad m_1, \ldots, m_k \in M_n$

$\Longrightarrow \quad M_n = M_{n+1} = \cdots = M$ $\square$

The property "Noetherian" behaves much nicer than "fin gen" or "fin pres":

Lemma For a short exact sequence $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ we have:

M Noetherian $\iff$ M' and M'' Noetherian.

Pf. "$\Rightarrow$"

M Noetherian $\Rightarrow$
- M' Noetherian because $N \subseteq M'$ implies $N \subseteq M$.
- M'' Noetherian because for $N \subseteq M''$ the submodule $g^{-1}(N) \subseteq M$ is fin gen so that its image $N = g(g^{-1}(N))$ is fin gen.

"$\Leftarrow$" Given $N \subseteq M$,

have exact sequence

$$0 \to f^{-1}(N) \to N \to g(N) \to 0$$

$f^{-1}(N)$: fingen since $\subseteq M'$ and M' Noetherian

$g(N)$: fin.gen. since $\subseteq M''$ and M'' Noetherian

$\Longrightarrow N$ fin. gen. $\square$

<u>Lemma</u> Let $M \in \mathrm{Mod}(R)$.

(a) If $M_1, M_2 \subseteq M$ are Noetherian submodules,

then so are $M_1 \cap M_2 \subseteq M$

$M_1 + M_2 \subseteq M$.

(b) If M is Noetherian as an R-module and $S \subseteq R$ is a multiplicative subset, then the localization $M_S \simeq M \otimes_R R_S$ is Noetherian as an R_S-module.

Pf.

(a) $$0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$$

$\Longrightarrow M_1 \oplus M_2$ Noetherian by previous lemma.

Similarly, $0 \to \ker(\mathrm{sum}) \to M_1 \oplus M_2 \xrightarrow{\mathrm{sum}} M_1 + M_2 \to 0$

$\Longrightarrow M_1 + M_2$ and $\ker(\mathrm{sum}) \simeq M_1 \cap M_2$ Noetherian by previous lemma.

(b) Consider the localization map $\alpha : M \longrightarrow M_S$, $m \longmapsto \frac{m}{1}$.

For an R_S-submodule $N \subseteq M_S$, the preimage $\tilde{N} := \alpha^{-1}(N) \subseteq M$ is an R-submodule, hence fingen as an R-module.

$\Longrightarrow N = \tilde{N}_S$ fin gen as R_S-module. $\square$

⚠ In general, for a ring homom. $R \to T$, $M \in \mathrm{Mod}(R)$ Noetherian does <u>NOT</u> imply $M \otimes_R T \in \mathrm{Mod}(T)$ to be Noetherian, (think of $M = R$ ...)!

Anyway: Get many Noetherian modules from any given one. via ker, coke, $\oplus$, $+$, $\cap$, localization... How to get started?

<u>Def</u> A ring R is <u>Noetherian</u> if it is so as an R-module, ie. if any ideal $\mathfrak{a} \trianglelefteq R$ is fin. gen. ($\Leftrightarrow$ acc for ideals).

<u>Ex</u> a) $R := \mathbb{Q}[X_n \mid n \in \mathbb{N}]$ is not Noetherian

since $\mathfrak{a} := (X_n \mid n \in \mathbb{N}) \trianglelefteq R$ is not fin gen.

b) For k a field,

$R := \{ a + x \cdot f(x,y) \mid a \in k,\ f \in k[x,y] \}$ is not Noetherian

since $\mathfrak{a} := (x, xy, xy^2, xy^3, \dots) \trianglelefteq R$ is not fin gen.

c) $R := \mathcal{C}([0,1], \mathbb{R}) := \{$continuous fct^s $f : [0,1] \to \mathbb{R}\}$

is not Noetherian (exercise).

d) Any PID R <u>is</u> Noetherian

(as we've seen in proving PID $\Rightarrow$ UFD, see § I.3).

e) Quotients and localizations of Noetherian rings are Noetherian

f) Fin. gen. modules over Noetherian rings are Noetherian.

<u>Hilbert's basis thm</u> R Noetherian

$\Rightarrow R[X_1, \dots, X_n]$ Noetherian $\forall n \in \mathbb{N}$

Pf. Wlog $n = 1$ by induction.

Let $\mathfrak{a} \trianglelefteq R[X]$.

Put $\mathfrak{a}_0 := \{$ leading coeff^s of polynomials in $\mathfrak{a} \} \trianglelefteq R$.

R Noetherian $\Rightarrow$ $\mathfrak{a}_0$ fin. gen., say $\mathfrak{a}_0 = (a_1, \dots, a_m) \trianglelefteq R$.

Pick $f_i \in \mathfrak{a}$ w/ $f_i = a_i X^{n_i}$ + lower order terms

and let $\mathfrak{b} := (f_1, \dots, f_m) \trianglelefteq R[X]$.

Given $f = a x^n$ + lower order terms $\in \mathfrak{a}$,

write $a = \sum_{i=1}^m r_i a_i$ w/ $r_i \in R$ (since $a \in \mathfrak{a}_0$)

If $n \geq n_0 := \max\{n_1, \dots, n_m\}$,

then $g := f - \underbrace{\sum_{i=1}^m r_i f_i X^{n-n_i}}_{\in \mathfrak{b}} \in \mathfrak{a}$

has $\deg(g) < n$.

$\Rightarrow$ Proceeding like this,

find $b \in \mathfrak{b}$ sth $f - b \in \mathfrak{a} \cap M \qquad (*)$

for $M := (1, X, X^2, \dots, X^{n_0 - 1})$

M fingen module over the Noetherian ring $R \Rightarrow$ Noetherian

$\Rightarrow$ any submodule $\mathfrak{a} \cap M \subseteq M$ is fin gen

Thus:

$$\mathfrak{a} \overset{\text{by } (*)}{=} \underbrace{(\mathfrak{a} \cap M)}_{\text{fin.gen.}} + \underbrace{\mathfrak{b}}_{\text{fin.gen.}} \qquad \Rightarrow \quad \mathfrak{a} \trianglelefteq R[X] \text{ fin. gen.}$$

$\square$

<u>Cor</u> If R is a Noetherian ring,

then so is any fin.gen. R-algebra.

i.e. any quotient of $R[X_1, \dots, X_n]$, $n \in \mathbb{N}$.

<u>Recall</u> An <u>R-algebra</u> is a ring S w/ a ring homom. $\varphi : R \to S$.

It is called <u>fin.gen. as an R-algebra</u> if $\exists\, s_1, \dots, s_n \in S$ sth every $s \in S$ is a polynomial in $s_1, \dots, s_n$ with coefficients in $\varphi(R)$.

<u>NB</u> Don't confuse this with the much more restrictive notion of S being fingen as an R-module, which allows only $\varphi(R)$-linear combinations of $s_1, \dots, s_n$.

In that case $\varphi : R \to S$ is a so-called <u>integral</u> ring extension, these are very special (see later).

<u>Upshot</u> "Almost all rings in algebraic geometry are Noetherian"

This simplifies life:

<u>Remark</u> Let R be a Noetherian ring, then for $M \in \mathrm{Mod}(R)$ TFAE:

a) M fin.gen.

b) M fin. pres.

c) M Noetherian.

Pf. a) $\Rightarrow$ c) already noted above
(R Noeth $\Rightarrow R^n$ Noeth $\Rightarrow$ quotients of R^n Noeth.)

c) $\Rightarrow$ b) M Noeth $\Rightarrow$ fingen, say $R^n \overset{p}{\twoheadrightarrow} M$
$\Rightarrow \ker(p) \subseteq R^n$ also fingen as R^n Noeth

b) $\Rightarrow$ a) trivial.

$\square$

4. Artinian rings and modules

Def $M \in \mathrm{Mod}(R)$ is <u>Artin(ian)</u> if it satisfies the "descending chain condition (dcc)":

$\forall$ submodules $\cdots \; M_3 \subseteq M_2 \subseteq M_1 \subseteq M$

$\exists\, n \in \mathbb{N}$ with $M_n = M_{n+1} = M_{n+2} = \cdots$

Def A ring R is <u>Artin(ian)</u> if it is so as an R-module.

⚠ MUCH more restrictive than Noetherian!

We'll see: "Artin rings are the simplest ones next to fields."

Ex

- Any field is an Artin ring.
- $\mathbb{Z}/n\mathbb{Z}$ is an Artin ring iff $n \neq 0$.
- a <u>fin.gen.</u> abelian gp $M \in \mathrm{Mod}(\mathbb{Z})$ is an Artinian module iff M is finite.

  [NB: "Fin.gen." cannot be dropped in "$\Rightarrow$" see the example b) on p. 63]
- for any field k and $n \in \mathbb{N}$, the ring $k[t]/(t^n)$ is Artin (its Spec is a "fat point")

Lemma For a short exact sequence $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ we have:

$$M \text{ Artin} \iff M' \text{ and } M'' \text{ Artin}.$$

Pf. "$\Leftarrow$" Given $\cdots \subseteq M_n \subseteq M_{n-1} \subseteq \cdots \subseteq M_1 \subseteq M$,

consider $M'_n := f^{-1}(M_n) \subseteq M'$

$M''_n := g(M_n) \subseteq M''$.

If M', M'' are Artin, then $\exists n$: $M'_n = M'_{n+1} = \cdots$

$M''_n = M''_{n+2} = \cdots$,

hence $M_n = M_{n+1} = \cdots$

"$\Rightarrow$" Given $\cdots \subseteq M''_n \subseteq M''_{n-1} \subseteq \cdots \subseteq M''_1 \subseteq M''$

put $M_n := g^{-1}(M_n)$.

If M is Artin, then $\exists n$: $M_n = M_{n+1} = \cdots$

and so $\underset{M''_n}{\underset{\parallel}{g(M_n)}} = \underset{M''_{n+1}}{\underset{\parallel}{g(M_{n+1})}} = \cdots \Rightarrow M''$ Artin

& similarly for M'

$\square$

Lemma Let $M \in \mathrm{Mod}(R)$.

(a) If $M_1, M_2 \subseteq M$ are Artin submodules,

so are $\quad M_1 \cap M_2 \subseteq M$

$\quad M_1 + M_2 \subseteq M$.

(b) If M is Artin as an R-module

and $S \subseteq R$ is multiplicative,

then $M_S \simeq M \otimes_R R_S$ is Artin as R_S-module.

$\square$

Pf. Exercise.

Cor R Artin and $M \in \mathrm{Mod}(R)$ fingen $\Rightarrow$ M Artin.

Want to build up Artinian modules from simple pieces:

Def A composition series for a module $M \in \mathrm{Mod}(R)$

is a chain $\quad 0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$

which cannot be refined,

i.e. for which each M_i / M_{i-1} is simple.

(has no submodules other than 0 & itself)

The M_i / M_{i-1} are called composition factors

and n is called the length of the series.

We say M has finite length if it admits a composition series.

Thm (Jordan-Hölder) Assume $M \in \mathrm{Mod}(R)$ has finite length.

Then a) any chain can be refined into a compos. series,

b) any two compos. series have the same length and isomorphic compos. factors up to permutation.

Pf.

a) Let $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ be any chain

and $0 = N_0 \subset N_1 \subset \cdots \subset N_m = M$ a compos series.

Put $\quad M_{i,j} := M_{i-1} + M_i \cap N_j \quad$ for $\quad i = 1, \dots, n$
$j = 1, \dots, m$.

$\Rightarrow \cdots \subseteq M_{i-1} = M_{i-1,0} \subseteq M_{i-1,1} \subseteq \cdots \subseteq M_{i-1,m} = M_i \subseteq \cdots$

This is a composition series refining the given chain,

since each $\quad M_{i-1,j} / M_{i-1,j-1} \hookrightarrow \underbrace{N_j / N_{j-1}}_{\text{simple by assumption!}}$ is either zero or simple.

b) Now assume $0 = M_0 \subset \cdots \subset M_n = M$ is also a composition series (not just a chain).

Then each M_i / M_{i-1} is simple

$\Rightarrow \exists!\, J(i)$ with

$$(*) \quad M_{i,j}/M_{i,j-1} \simeq \begin{cases} M_i/M_{i-1} & \text{if } j = J(i) \\ 0 & \text{else.} \end{cases}$$

Similarly, put $N_{j,i} := N_{j-1} + N_j \cap M_i$,
then $\forall j\ \exists!\, I(j)$ with

$$(**) \quad N_{j,i}/N_{j,i-1} \simeq \begin{cases} N_j/N_{j-1} & \text{if } i = I(j) \\ 0 & \text{else.} \end{cases}$$

$\Rightarrow$ Suffices to show that $(*) \simeq (**)$ $\forall i,j$.

Indeed

$$\begin{tikzcd} (*) = \dfrac{M_{i-1} + M_i \cap N_j}{M_{i-1} + M_i \cap N_{j-1}} \arrow[rr, dashed, leftrightarrow, "\sim"] & & \dfrac{N_{j-1} + N_j \cap M_i}{N_{j-1} + N_j \cap M_{i-1}} = (**) \\ & \dfrac{M_i \cap N_j}{M_i \cap N_{j-1} + M_{i-1} \cap N_j} \arrow[ul, "\sim"] \arrow[ur, "\sim"'] & \end{tikzcd}$$

$\square$

Def $\ell(M) := n$ is called the <u>length</u> of M.

Cor. $M \in \mathrm{Mod}(R)$ has finite length iff M is both Artinian & Noetherian.

Pf. "$\Rightarrow$" by Jordan-Hölder thm, any chain has length $\leq \ell(M)$, so acc + dcc hold.

"$\Leftarrow$" Pick a maximal submodule $M_1 \subsetneq M$ (M Noetherian)

— 〃 — $\quad M_2 \subsetneq M_1$ (M^0 — 〃 —)

$\vdots$

Get chain $M = M_0 \supseteq M_1 \supseteq \cdots$ with each M_i/M_{i+1} simple or zero

M Artin $\Rightarrow \exists n : M_n = M_{n+1} = \cdots = \{0\}$
so we get a composition series of length n. $\square$

Ex Need both dcc & acc: Put $R = \mathbb{Z}$.

a) $M = \mathbb{Z}$ Noetherian but NOT Artinian.

b) $M = \mathbb{Z}[\frac{1}{p}]/\mathbb{Z} = \{ \frac{a}{p^n} \in \mathbb{Q}/\mathbb{Z} \mid a \in \mathbb{Z}, n \in \mathbb{N} \}$

Exercise: All proper subgp^s of M are $M_n := \frac{1}{p^n}\mathbb{Z}/\mathbb{Z}$, $n \in \mathbb{N}$.

$\Rightarrow$ M Artinian but NOT Noetherian:

$$M_1 \subsetneq M_2 \subsetneq M_3 \subsetneq \cdots \subseteq M.$$

Ex If $R = k$ is a field, TFAE for $M \in \mathrm{Mod}(R)$:

a) M Noetherian

b) M Artinian

c) $\dim_k(M) < \infty$

and in this case $\ell(M) = \dim_k(M)$.

5. The Structure of Artinian rings

Let's take a closer look at Artin rings (not modules).

Lemma Let R be a ring s.th. $m_1 \cdots m_n = (0)$ for suitable $m_i \in \mathrm{Spm}(R)$ (not necessarily distinct).

Then: R Noetherian $\Leftrightarrow$ R Artinian

Pf. Put $M_i := m_1 \cdots m_i \subseteq R$

$\Rightarrow R = M_0 \supset M_1 \supset \cdots \supset M_n = \{0\}$

Each $Q_i := M_{i-1}/M_i \in \mathrm{Mod}(R/m_i)$ is a vector space over the field $k_i := R/m_i$.

Previous ex. gives: Q_i Noetherian in $\mathrm{Mod}(k_i)$ (or in $\mathrm{Mod}(R)$) $\Longleftrightarrow$ Q_i Artinian in $\mathrm{Mod}(k_i)$ (or in $\mathrm{Mod}(R)$)

But by ind^n R is Artin/Noeth iff all Q_i are so. $\square$

Does this always apply?

Prop Let R be an Artin ring. Then:

a) $\mathrm{Spm}(R) = \mathrm{Spec}(R)$ and this is a finite set.

b) $\exists n \in \mathbb{N}$: $\mathrm{Jac}(R)^n = (0)$.

c) R is Noetherian.

Pf. a1) Assume $m_1, m_2, \ldots \in \mathrm{Spm}(R)$ all distinct

R Artin $\Rightarrow$ the chain $m_1 \supseteq m_1 \cap m_2 \supseteq m_1 \cap m_2 \cap m_3 \supseteq \cdots$ stabilizes

$\Rightarrow \exists n$: $m_1 \cap \cdots \cap m_n \subseteq \wp := m_{n+1}$

hence $m_1 \cdots m_n \subseteq \wp$

$\Rightarrow \exists i \in \{1, \ldots, n\}$: $m_i \subseteq \wp$ (since $\wp$ prime).

$\Rightarrow \mathrm{Spm}\, R = \{m_1, \ldots, m_n\}$. finite set

a2) Let $\wp \in \mathrm{Spec}\, R$

$\Rightarrow K := R/\wp$ is both Artin & integral domain, hence a field

(for $a \in K \setminus \{0\}$, $\exists n$: $(a^n) = (a^{n+1}) = \cdots$, so $a^n = c \cdot a^{n+1}$ (some $c \in K$) and hence $1 = ca$ because K integral)

$\Rightarrow \wp$ maximal

b) Put $J := \mathrm{Jac}(R)$.

R Artin $\Rightarrow \exists n$: $J^n = J^{n+1} = \cdots$

Put $\mathfrak{a} := \mathrm{Ann}(J^n) := \{a \in R \mid a \cdot J^n = (0)\}$.

Want: $\mathfrak{a} = (1)$ (then $J^n = 1 \cdot J^n = (0)$).

If $\mathfrak{a} \neq (1)$, exists since $R/\mathfrak{a}$ is an Artinian module!

pick a simple submodule $\mathfrak{b}/\mathfrak{a} \subsetneq R/\mathfrak{a}$ $\quad (\mathfrak{b} \trianglelefteq R)$.

$J = \mathrm{Jac}(R)$ annihilates all simple R-modules

$\Longrightarrow J \cdot \mathfrak{b}/\mathfrak{a} = \{0\}$

$\Longrightarrow J \cdot \mathfrak{b} \subseteq \mathfrak{a} = \mathrm{Ann}(J^n)$

$\Longrightarrow \mathfrak{b} \subseteq \mathrm{Ann}(J^{n+1}) \underset{\uparrow}{=} \mathrm{Ann}(J^n) =: \mathfrak{a}$ $\lightning$

(recall $J^{n+1} = J^n$)

c) Combining a) & b),

$\exists\, \mathfrak{m}_1, \dots, \mathfrak{m}_n \in \mathrm{Spm}(R)$ with $\mathfrak{m}_1 \cdots \mathfrak{m}_n = (0)$

Hence R Artinian $\Longrightarrow$ R Noetherian by previous lemma. $\square$

Cor For any ring R, TFAE:

a) R is Artin.

b) R is Noetherian and $\underline{\mathrm{Spec}\, R = \mathrm{Spm}\, R}$.

i.e. "$\dim R = 0$"
where we define
$\dim R := \sup \{ n \mid \exists\, \mathfrak{p}_0 \overset{\neq}{\subset} \mathfrak{p}_1 \overset{\neq}{\subset} \cdots \mathfrak{p}_n$ with $\mathfrak{p}_i \in \mathrm{Spec}\, R \}$
$\in \mathbb{N}_0 \cup \{\infty\}$

Pf. a) $\Rightarrow$ b) by previous proposition.

b) $\Rightarrow$ a):

FACT: Any Noetherian ring R has only finitely many minimal prime ideals
($\hat{=}$ irred. cpt^s of $\mathrm{Spec}\, R$, see next section)

If $\dim R = 0$, these are all the prime ($=$ maximal $=$ minimal) ideals,

say $\mathrm{Spec}\, R = \{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$.

$\Longrightarrow \mathrm{Rad}\, R = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_m$

But $\mathrm{Rad}\, R$ is fin. gen. (R Noetherian) & all its elements are nilpotent $\Bigg\} \Longrightarrow \exists n: (\mathrm{Rad}\, R)^n = (0)$

$\Longrightarrow \mathfrak{p}_1^m \cdots \mathfrak{p}_n^m = (0)$,

hence R Noetherian implies R Artinian by previous lemma. $\square$

Cor A ring R is Artin iff it is of finite length over itself.

Pf. For R-modules we know: Finite length $\Longleftrightarrow$ Artin + Noetherian, so previous corollary applies. $\square$

... geometric interpretation?

Rem. Let R be a ring and $J \trianglelefteq R$ an ideal w/ $J \subseteq \operatorname{Rad} R$

$\Rightarrow$ The quotient map $R \twoheadrightarrow R/J$ induces a bijection

$$\{\text{idempotents of } R\} \xrightarrow{\sim} \{\text{idempotents of } R/J\}.$$

(i.e. elements $e \in R$ with $e^2 = e$)

Pf 1. Check by hand that $\forall k$, idempotents of R/J^k can be lifted to idempotents of R/J^{k+1} (exercise, slightly messy). $\square$

Pf 2 (better). Use geometry:

- $\operatorname{Spec}(R/J) \xrightarrow{\sim} \operatorname{Spec}(R)$ as top. spaces (since $J \subseteq \operatorname{Rad} R$)
- $\{\text{idempotents of } R\} \xrightarrow{\sim} \left\{\begin{array}{l}\text{subsets of } \operatorname{Spec}(R) \\ \text{which are both open \& closed}\end{array}\right\}$

$$\begin{array}{ccc} \psi & & \psi \\ e & \longmapsto & V(e) \end{array}$$

(closed by def^n of Zariski top, open since $(\operatorname{Spec} R) \setminus V(e) = V(1-e)$)

(see next section) $\square$

Prop Let R be a ring with $\operatorname{Spm} R = \{m_1, \dots, m_n\}$ finite (pairwise distinct) & $\operatorname{Jac} R = \operatorname{Rad} R$.

Then $R \xrightarrow{\sim} R_{m_1} \times \dots \times R_{m_n}$ (a product of local rings).

Pf. By maximality $m_i + m_j = (1) \quad \forall i \neq j$

$\Rightarrow$ Chinese Remainder Thm gives

$$R/_{\operatorname{Jac} R} \xrightarrow{\sim} \prod_{i=1}^n R/m_i \quad \text{since } \operatorname{Jac} R = m_1 \cap \dots \cap m_n.$$

$\Longrightarrow$ $\exists$ idempotents $\bar{e}_i \in R/_{\operatorname{Jac} R}$ with $\bar{e}_i \equiv \begin{cases} 1 \bmod m_i \\ 0 \bmod m_j \ \forall j \neq i \end{cases}$

By previous remark, these lift to idempotents $e_i \in R$.

Note:

- For $i \neq j$ we have $e_i \cdot e_j = 0$ (indeed $e_i \cdot e_j$ is both idempotent and $\in \bigcap_{i=1}^n m_i = \operatorname{Rad} R$) nilpotent elt^s!
- Similarly $e_1 + \dots + e_n = 1$ (indeed $1 - e_1 - \dots - e_n$ is idempotent and $\in \operatorname{Rad} R$).

$$\Longrightarrow \begin{array}{ccc} R & \xrightarrow{\sim} & Re_1 \times \dots \times Re_n \\ a & \longmapsto & (ae_1, \dots, ae_n) \\ b_1 + \dots + b_n & \longleftarrow & (b_1, \dots, b_n) \end{array}$$

By construction, each Re_i has a unique max. ideal and it maps to m_i so that $Re_i \simeq R_{m_i}$. $\square$

Cor. ("Structure thm for Artin rings")

A ring R is Artin iff $R \simeq R_1 \times \cdots \times R_n$ with local Artin rings R_i.

The rings R_i are uniquely determined up to iso, they are the localizations of R at its maximal ideals.

Pf. Only remains to check uniqueness.

Given an iso $\varphi : R \xrightarrow{\sim} R_1 \times \cdots \times R_n$ w/ $\mathrm{Spm}\, R_i =: \{\bar{m}_i\}$,

put
$$m_i := \varphi^{-1}(\bar{m}_i)$$

via
$$\mathrm{Spm}(R_1 \times \cdots \times R_n) \simeq \mathrm{Spm}(R_1) \times \cdots \times \mathrm{Spm}(R_n).$$

$$\Longrightarrow \quad \mathrm{Spm}(R) = \{m_1, \dots, m_n\}$$

and
$$R_{m_i} \xrightarrow[\varphi]{\sim} R_{i,\bar{m}_i} \underset{\uparrow}{=} R_i.$$

(since R_i is local)

Note: By construction the m_i are pairwise distinct because the $\bar{m}_i$ live in different factors of $R_1 \times \cdots \times R_n$.

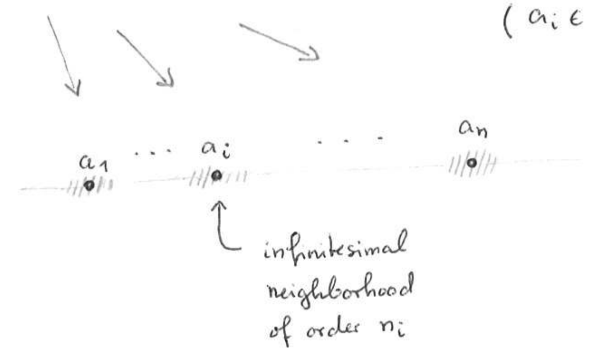
$\square$

Rem. A local ring R w/ max. ideal $m \trianglelefteq R$ is Artin iff $m^n = (0)$ for some $n \in \mathbb{N}$ (use that $\mathrm{Jac}\, R = m$).

We then think of $\mathrm{Spec}\, R$ as a "fat point", so in general spectra of Artin rings are unions of such:

$$\mathrm{Spec}\left(k[X]/(f(X))\right), \qquad f(X) = \prod_{i=1}^{n} (X - a_i)^{e_i}$$

($a_i \in k$ pairwise distinct)



Caution For arbitrary rings R,

$\mathrm{Spec}(R)$ = finite union of closed points

does NOT imply that R is Artin:

e.g. take k a field and $V \in \mathrm{Vect}(k)$

then $R := k \oplus V$ as a k-algebra

with multiplication defined by $V \cdot V := \{0\}$

has $\mathrm{Spec}\, R$ = a single pt, but R is Noetherian only if $\dim_k V < \infty$.

This example was artificial as we made $\mathrm{Rad}(R)$ huge.
But we need to be careful even in reduced cases:

<u>Ex</u> Let $R = \prod_{i=1}^{\infty} k_i$ be an infinite product of fields k_i.

$\Rightarrow$ R is not Noetherian but $\dim R = 0$.

Pf. Consider the following property of rings S:

$(*)$ $\forall\, s \in S$, the element s^2 divides s in S

("von Neumann rings")

Then:

- fields satisfy $(*)$
- $(*)$ is stable under arbitrary products & quotients

In our case we get: For any $\mathfrak{p} \in \mathrm{Spec}(R)$,
the integral domain $S := R/\mathfrak{p}$ has $(*)$

But an integral domain with $(*)$ is necessarily a field:
For $s \in S \setminus \{0\}$ write $s = s^2 t$ with $t \in S$ by $(*)$,
then we get $st = 1$ since S is an integral domain.

Conclusion: Any $\mathfrak{p} \in \mathrm{Spec}\, R$ is maximal, ie $\dim R = 0$. $\square$

6. Connected components

Let R be a ring.

The top. space $\mathrm{Spec}\, R$ doesn't have to be connected,
ie. it may be a disjoint union of two closed subsets:

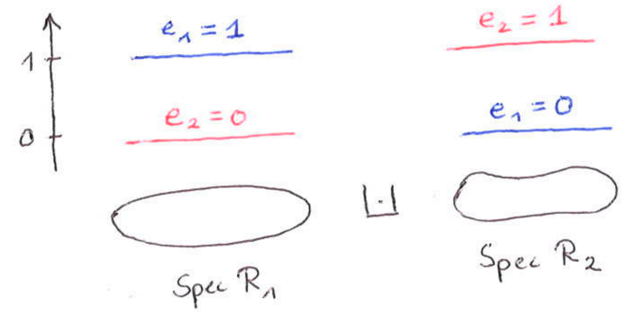
<u>Ex</u> $R = R_1 \times R_2$ product of two rings

$\Longrightarrow$ $\mathrm{Spec}\, R = V_1 \sqcup V_2$ with $V_i := \mathrm{Spec}\, R_i$

(disjoint union)

The $V_i \subset \mathrm{Spec}\, R$ are closed since $V_i = V(e_i)$
for the "basis vectors" $e_1 = (1,0)$, $e_2 = (0,1)$ $\in R_1 \times R_2$.

This is like a "partition of unity":



<u>More precisely:</u> e_1 and e_2 are idempotent, $e_1 e_2 = 0$
and $e_1 + e_2 = 1$.

Def • An element $e \in R$ is called *idempotent* if $e^2 = e$.

• For a topological space X, a subset $Y \subseteq X$ is called <u>clopen</u> if it is both closed & open ($\Leftrightarrow$ Y and $X \setminus Y$ are both closed).

<u>Lemma</u> For any ring R, $\exists$ bijection

$$\begin{array}{ccc} \{\text{idempotents } e \in R\} & \xrightarrow{\sim} & \{\text{clopen subsets of } \operatorname{Spec} R\} \\ & & \text{(in the Zariski topology)} \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ e & \longmapsto & V(e) \subseteq \operatorname{Spec} R \end{array}$$

Pf.

① For $e \in R$ idempotent, also $f := 1 - e$ is idempotent

$$(f^2 = 1 - 2e + e^2 = 1 - 2e + e = f)$$

We have

- $e \cdot f = 0 \implies \operatorname{Spec} R = V(e) \cup V(f)$
- $e + f = 1 \implies V(e) \cap V(f) = \emptyset$

Thus both $V(e)$ & its complement $\operatorname{Spec} R \setminus V(e) = V(f)$ are closed, ie. $V(e)$ is clopen.

② Conversely, assume $V = V(\tilde{I}) \subseteq \operatorname{Spec} R$ clopen for some $\tilde{I} \trianglelefteq R$.

Write $W = \operatorname{Spec} R \setminus V(\tilde{I}) = V(\tilde{J})$ with $\tilde{J} \trianglelefteq R$ (as W is also closed).

• Now $V(\tilde{I}) \cap V(\tilde{J}) = \emptyset$

$\implies$ the ideal $\tilde{I} + \tilde{J}$ is not contained in any prime ideal

$\implies \tilde{I} + \tilde{J} = (1)$

$\implies \exists\, \check{e} \in \tilde{I},\ \check{f} \in \tilde{J} : \quad \check{e} + \check{f} = 1.$

$\implies \begin{array}{l} V(\check{e}) \supseteq V(\tilde{I}) \\ V(\check{f}) \supseteq V(\tilde{J}) \end{array}$ and $V(\check{e}) \cap V(\check{f}) = \emptyset$

Since $\operatorname{Spec} R = V(\tilde{I}) \sqcup V(\tilde{J}) \subseteq V(\check{e}) \sqcup V(\check{f}) \subseteq \operatorname{Spec} R$ it follows that "$=$" holds everywhere.

$\implies$ Wlog $\begin{array}{l} \tilde{I} = (\check{e}) \\ \tilde{J} = (\check{f}) \end{array}$ without changing vanishing loci V, W.

• Now if we knew $\check{e}\check{f} = 0$ then $\check{e}, \check{f}$ would be idempotent since $\check{f} = 1 - \check{e}$, so we'd be done.

This doesn't always work.

However, $V(\tilde{I}) \cup V(\tilde{J}) = \operatorname{Spec} R$

$\implies \tilde{I}\tilde{J} \subseteq \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p} = \operatorname{Rad} R$

$\implies \exists\, n \in \mathbb{N} : (\check{e}\check{f})^n = 0$

$\implies IJ = 0$ for the ideals $I = (\check{e}^n),\ J = (\check{f}^n) \trianglelefteq R.$

Now $V = V(I) = V(\tilde{I})$ since $\sqrt{I} = \sqrt{\tilde{I}}$
$W = V(J) = V(\tilde{J})$ $\sqrt{J} = \sqrt{\tilde{J}}$

$\Rightarrow$ same argument as before gives $e \in I$, $f \in J$ with $e + f = 1$

but now also $ef \in IJ = (0)$, so $ef = 0$.

$\Rightarrow$ $e \in R$ idempotent with $V = V(e)$.

③ So we've shown every clopen $V \subseteq \operatorname{Spec} R$ has the form $V = V(e)$ with $e \in R$ idempotent.

Remains to check uniqueness:

Let $e_1 \neq e_2 \in R$ be distinct idempotents.
Put $f_i := 1 - e_i \in R$, again idempotent w/ $e_i f_i = 0$.

$$\Rightarrow 0 \neq e_1 - e_2 = e_1 \cdot \underbrace{(e_2 + f_2)}_{=1} - \underbrace{(e_1 + f_1)}_{=1} \cdot e_2 = e_1 f_2 - f_1 e_2.$$

$\Rightarrow$ $e_1 f_2 \neq 0$ or $f_1 e_2 \neq 0$. Say $e_1 f_2 \neq 0$.

Nonzero idempotents are not nilpotent, so $e_1 f_2 \notin \operatorname{Rad} R$

$\Rightarrow$ $\exists\, \wp \in \operatorname{Spec} R : e_1 f_2 \notin \wp$

$\Rightarrow$ $e_1 \notin \wp$ and $f_2 \notin \wp$, but the latter implies $e_2 \in \wp$ because $e_2 f_2 = 0$.

$\Rightarrow$ $V(e_1) \neq V(e_2)$. $\square$

<u>Cor.</u> Spec R is connected iff the only idempotents in R are $e = 0, 1$.

<u>Ex.</u> If R is an integral domain, then Spec R is connected (even irreducible, see below).

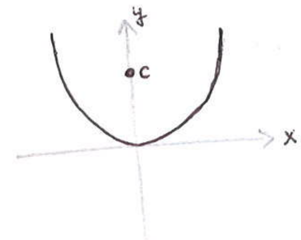
<u>Rem.</u> If $e \in R$ is idempotent and $f := 1 - e$, then

$$R \xrightarrow{\sim} R_1 \times R_2 \quad \text{with} \quad R_1 := R \cdot e, \quad R_2 := R \cdot f$$
$$a \longmapsto (ae, af)$$

$\Rightarrow$ $V(e) = \operatorname{Spec}(R_1)$, $V(f) = \operatorname{Spec}(R_2)$ & the example from the beginning covers all cases.

<u>Ex</u> $R = k[x, y]/\mathfrak{a}$ for k a field,

$$\mathfrak{a} := \underbrace{(y - x^2)}_{I} \cdot \underbrace{(x, y - c)}_{J}$$



Look for $e \in I$, $f \in J$ with $e + f = 1$:

For $c \neq 0$, can take

$e := \frac{1}{c} \cdot (y - x^2) \in I$

$f := \frac{1}{c} \cdot (x^2 - (y - c)) \in J$.

Then put $R_1 := Re \simeq k[x, y]/(x, y-c) \simeq k$
$R_2 := Rf \simeq k[x, y]/(y - x^2) \simeq k[x]$

$\Rightarrow$ $R \xrightarrow{\sim} R_1 \times R_2 \simeq k \times k[x]$ via $a \mapsto (a, a)$, $a \in k$
$x \mapsto (0, x)$,
$y \mapsto (c, x^2)$.

Do you see what happens for $c = 0$?

7. Irreducible components

Recall: Any top space X is the disjoint union of its connected components (= max. clopen subsets).

Q: When $X = \operatorname{Spec} R$,

a) can we refine this decomposition;

b) and find conditions under which it is finite?

Def A top space X is *irreducible* if it cannot be written as $X = X_1 \cup X_2$ w/ $X_1, X_2 \overset{\neq}{\hookrightarrow} X$ proper closed subsets.

Ex
- $X = \operatorname{Spec} k[t]$ is irreducible (its proper closed subsets are finite)
- $X = \operatorname{Spec} k[s,t]/(st) = \underset{\uparrow \text{ not disjoint}}{V(s) \cup V(t)}$

is not irreducible,

it decomposes in two irreducible closed subsets

$V(s) \simeq \operatorname{Spec} k[t]$

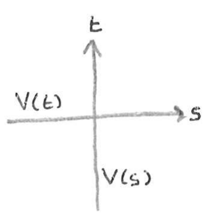
$V(t) \simeq \operatorname{Spec} k[s]$.

However, X is connected:

$\bar{e} \in k[s,t]/(st)$ idempotent $\iff e \in k[s,t]$ with $e(e-1) \in (st)$

$\iff e \in (st)$ or $e - 1 \in (st)$ (exercise)

$\iff \bar{e} \in \{0,1\}$.



Lemma $X = \operatorname{Spec} R$ is irreducible iff $\operatorname{Rad}(R) \trianglelefteq R$ is a prime ideal.

Pf. X is irreducible iff $X = V(\mathfrak{a}) \cup V(\mathfrak{b})$ w/ $\mathfrak{a}, \mathfrak{b} \trianglelefteq R$ implies that $X = V(\mathfrak{a})$ or $X = V(\mathfrak{a})$.

Since $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cdot \mathfrak{b})$, it is equivalent to require:

" $\mathfrak{a} \cdot \mathfrak{b} \subseteq \operatorname{Rad} R$ implies $\mathfrak{a} \subseteq \operatorname{Rad} R$ or $\mathfrak{b} \subseteq \operatorname{Rad} R$."

But this is equivalent to $\operatorname{Rad} R$ being prime. $\square$

Cor. A closed subset $V(\mathfrak{a}) \subseteq \operatorname{Spec} R$ is irreducible iff $\sqrt{\mathfrak{a}} \trianglelefteq R$ is prime. $\square$

Pf. $V(\mathfrak{a}) = \operatorname{Spec}(R/\mathfrak{a})$ and $\operatorname{Rad}(R/\mathfrak{a}) = \sqrt{\mathfrak{a}}/\mathfrak{a}$.

Def By an *irreducible component* of a top space X we mean a maximal irreducible closed subset.

By the above,

$$\left\{ \begin{matrix} \text{minimal prime} \\ \text{ideals } \mathfrak{p} \in \operatorname{Spec} R \end{matrix} \right\} \xleftrightarrow{1:1} \left\{ \begin{matrix} \text{irreducible cpts} \\ \text{of } X = \operatorname{Spec} R \end{matrix} \right\}$$

... are there only finitely many?

Def A top space X is <u>Noetherian</u> if it satisfies dcc for closed subsets: Any chain

$$X = X_0 \supseteq X_1 \supseteq X_2 \supseteq \cdots$$

stabilizes, ie $\exists n \in \mathbb{N}$ with $X_n = X_{n+1} = X_{n+2} = \cdots$

Ex R Noetherian ring $\Rightarrow$ Spec R Noetherian

(as descending chains of closed subsets in Spec R correspond to ascending chains of vanishing ideals)

Note Converse is NOT true in general:

e.g. take $R = k[x_n \mid n \in \mathbb{N}] / (x_n^2 \mid n \in \mathbb{N})$

$\Rightarrow$ every x_n is nilpotent, hence contained in all primes of R

$\Rightarrow$ $\mathfrak{p} := (x_n \mid n \in \mathbb{N}) \trianglelefteq R$ is the only prime ideal

$\Rightarrow$ Spec $R = \{\mathfrak{p}\}$ is a singleton space, clearly Noetherian

but R is NOT Noetherian since $\mathfrak{p}$ is not fin. gen.

Lemma. Every Noetherian top space X is the union of finitely many irreducible components.

Pf. We show that any closed subset of X is a finite union of irreducibles.

Put $\mathcal{S} := \{$ closed subsets $Z \subset X$ that are not finite unions of irreducible closed subsets $\}$

Then $\mathcal{S}$ is partially ordered by "$\subseteq$".

If $\mathcal{S} \neq \emptyset$, then $\exists$ a minimal element $Z \in \mathcal{S}$ (since X Noetherian)

Since $Z \in \mathcal{S}$, in particular Z is not irreducible,

so $Z = Z_1 \cup Z_2$ with $Z_i \overset{\neq}{\hookrightarrow} Z$ closed.

By minimality $Z_1, Z_2 \notin \mathcal{S}$, so both Z_i are finite unions of irreducible closed subsets & then so is $Z = Z_1 \cup Z_2$ $\lightning$

$\square$

Cor For any Noetherian ring R,

a) the spectrum $X = $ Spec R is a finite union of irred components,

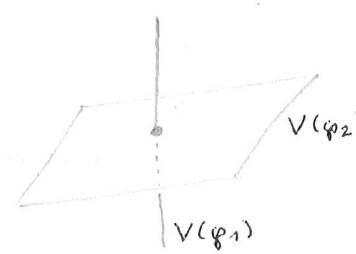
b) hence R has finitely many minimal prime ideals.

Ex $R = k[x, y, z] / (xz, yz)$

minimal primes:

$\mathfrak{p}_1 = (x, y) \trianglelefteq R$

$\mathfrak{p}_2 = (z) \trianglelefteq R$



Spec (R)

8. Primary ideals

R ring, $\mathfrak{a} \trianglelefteq R$

"irreducible cpt^s"

Have seen: If R is Noetherian,

then $V(\mathfrak{a}) = \operatorname{Spec}(R/\mathfrak{a}) = V(\mathfrak{p}_1) \cup \dots \cup V(\mathfrak{p}_n)$

for the finitely many minimal prime ideals $\mathfrak{p}_i \supseteq \mathfrak{a}$.

Equivalently: $\sqrt{\mathfrak{a}} = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_n$,

Cor. In a Noetherian ring R,

any radical ideal is a finite intersection of prime ideals.

Q: What about non-radical ideals?

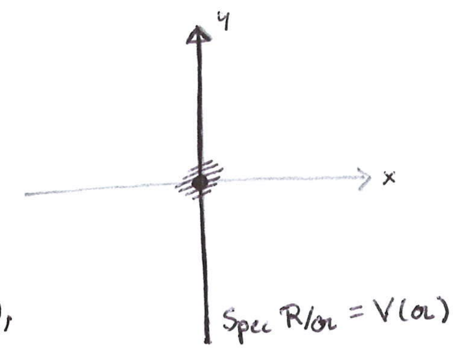
Ex a) $R = \mathbb{Z}$, $\mathfrak{a} = (a)$, $a = \pm p_1^{e_1} \cdots p_n^{e_n}$ prime factorizat^n

$$\left.\begin{aligned} R &= \mathbb{Z} \\ \mathfrak{a} &= (a) \\ a &= \pm p_1^{e_1}\cdots p_n^{e_n} \\ &\text{prime factorizat}^n \end{aligned}\right\} \quad \begin{aligned} \sqrt{\mathfrak{a}} &= (p_1 \cdots p_n) \\ &= (p_1) \cap \dots \cap (p_n) \\ \text{but} \quad \mathfrak{a} &= (p_1)^{e_1} \cap \dots \cap (p_n)^{e_n} \end{aligned}$$

$\Rightarrow$ Want to allow powers of prime ideals $\mathfrak{p} \supseteq \mathfrak{a}$ ("fat points")

b) $R = k[X, Y]$ (k a field)

$\mathfrak{a} = (XY, X^2)$



There is a unique smallest prime $\mathfrak{p} \supseteq \mathfrak{a}$, namely $\mathfrak{p} = (x)$

($\mathrel{\hat{=}}$ the unique irred. cpt. of $\operatorname{Spec} R/\mathfrak{a}$),

but clearly $\mathfrak{a} \neq \mathfrak{p}^n \ \forall n \in \mathbb{N}$!

However,

$$\mathfrak{a} = \left\{ \begin{array}{l} \text{fct}^s \text{ vanishing along the } y\text{-axis} \\ \& \text{ vanishing to order} \geq 2 \text{ at the origin} \end{array} \right\} = \mathfrak{p}_1 \cap \mathfrak{p}_2^2$$

where
$\mathfrak{p}_1 := (x)$
$\mathfrak{p}_2 := (x, y)$

Note: Here $V(\mathfrak{p}_2) \subseteq V(\mathfrak{p}_1)$, since $\mathfrak{p}_2 \subseteq \mathfrak{p}_1$ is not minimal containing $\mathfrak{a}$.

$\Rightarrow$ Want to consider not only minimal primes $\supseteq \mathfrak{a}$

($\mathrel{\hat{=}}$ irred. cpt^s of $V(\mathfrak{a})$)

but also other "associated primes"

($\mathrel{\hat{=}}$ "embedded cpt^s of $V(\mathfrak{a})$")

c) $R = k[X,Y]$

$\mathfrak{a} = (X, Y^2)$ is NOT an intersection of prime powers:

Indeed, if $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cap \dots \cap \mathfrak{p}_n^{e_n}$

then $\mathfrak{a} \subseteq \mathfrak{p}_i \ \forall i$, so $X, Y \in \mathfrak{p}_i$,

hence $(X,Y) \hookrightarrow \mathfrak{p}_i$ & equality holds by maximality,

i.e. $n = 1$ and $\mathfrak{p}_1 = (X,Y)$, but $\mathfrak{a} \neq \mathfrak{p}_1^{e_1} \ \forall e_1 \in \mathbb{N}$ ↯

But: Here $R/\mathfrak{a} \simeq k[Y]/(Y^2)$, although not integral,
becomes integral when dividing out its radical...

$\Rightarrow$ Want to relax the notion of prime ideal
to "primary ideal":

Def An ideal $\mathfrak{q} \ntrianglelefteq R$ is primary if it satisfies the following equivalent conditions:

(i) Every zero divisor of $R/\mathfrak{q}$ is nilpotent.

(ii) $ab \in \mathfrak{q} \implies a \in \mathfrak{q}$ or $b^n \in \mathfrak{q}$ for some $n \in \mathbb{N}$.

(iii) $ab \in \mathfrak{q}$ but $a, b \notin \mathfrak{q} \Rightarrow \exists m, n \in \mathbb{N}: a^m, b^n \in \mathfrak{q}$.

Rem. Imposing just "$ab \in \mathfrak{q} \Rightarrow \exists n: a^n \in \mathfrak{q}$ or $b^n \in \mathfrak{q}$"
would be strictly weaker:
e.g. $\mathfrak{q} := (XY, Y^2) \trianglelefteq k[X,Y]$ satisfies this condition but is not primary,
since $XY \in \mathfrak{q}$, $Y \notin \mathfrak{q}$ but $X^n \notin \mathfrak{q} \ \forall n \in \mathbb{N}$.
Thus the order of a, b in condition (ii) matters,
we require (ii) not only for (a,b) but also for (b,a).

Ex. If R is a PID, then

$\mathfrak{q} \trianglelefteq R$ is primary iff $\mathfrak{q} = \mathfrak{p}^n$ for some $\mathfrak{p} \in \operatorname{Spec} R$, $n \in \mathbb{N}$.

Pf. Write $\mathfrak{q} = (c)$ for some $c \in R$.

Then: $\mathfrak{q} \neq \mathfrak{p}^n$ for all $\mathfrak{p} \in \operatorname{Spec} R$, $n \in \mathbb{N}$

$\Leftrightarrow$ $c = ab$ with $a, b \notin R^*$ and $\gcd(a,b) = 1$.

In that case, $c \nmid a^m$, $c \nmid b^n$ $\forall m,n$ but $c \mid ab$,

hence $\mathfrak{q} = (c)$ is not primary (and vice versa). □

Back to arbitrary rings R:

<u>Lemma</u> a) Every prime ideal is primary.

b) If $\mathfrak{q} \trianglelefteq R$ is primary, then $\mathfrak{p} := \sqrt{\mathfrak{q}}$ is prime.

Pf. a) Obvious: Integral domains have no zero divisors $\neq 0$.

b) Let $ab \in \sqrt{\mathfrak{q}}$

$\Rightarrow \exists N: \ (ab)^N \in \mathfrak{q}$

If $a^N \in \mathfrak{q}$ then $a \in \sqrt{\mathfrak{q}}$, similarly for b.

$\Longrightarrow$ wlog $a^N, b^N \notin \mathfrak{q}$

$\Longrightarrow \exists m, n: \ a^{mN}, b^{nN} \in \mathfrak{q}$ since $\mathfrak{q}$ is primary $\square$

$\Longrightarrow a, b \in \sqrt{\mathfrak{q}}$

<u>Cor.</u> For $\mathfrak{q} \trianglelefteq R$ primary,

$\mathfrak{p} := \sqrt{\mathfrak{q}}$ is the unique smallest prime ideal $\supseteq \mathfrak{q}$. $\square$

Pf. Any prime ideal containing $\mathfrak{q}$ must contain $\sqrt{\mathfrak{q}}$.

<u>Def</u> We say that $\mathfrak{q}$ is <u>$\mathfrak{p}$-primary</u> if it is primary with $\mathfrak{p} = \sqrt{\mathfrak{q}}$.

<u>Warning</u> In general,

a) primary $\not\Rightarrow$ prime power,

e.g. $\mathfrak{q} := (X, Y^2) \trianglelefteq R := k[X,Y]$

is a primary ideal but not a power of any prime ideal.

b) prime power $\not\Rightarrow$ primary,

e.g. $\mathfrak{p} := (X, Z) \trianglelefteq R := k[X,Y,Z]/(XY - Z^2)$

is a prime ideal but $\mathfrak{p}^2$ is not primary

(exercise).

However, we do have:

<u>Lemma</u> If $\mathfrak{q} \trianglelefteq R$ is an ideal sth $\mathfrak{m} := \sqrt{\mathfrak{q}}$ is maximal, then $\mathfrak{q}$ is primary. In particular, powers of maximal ideals are primary.

Pf. Consider the epi $R/\mathfrak{q} \twoheadrightarrow K := R/\mathfrak{m}$.

If $a \in R/\mathfrak{q}$ is a zero divisor which is not nilpotent, then it maps to a zero divisor $\neq 0$ in K, $\square$

but K is a field $\lightning$

9. Primary decomposition

Goal: Decompose arbitrary ideals into their "irreducible" pieces.

Def A primary decomposition of an ideal $\mathfrak{a} \trianglelefteq R$ is a representation as an intersection

$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ of primary ideals $\mathfrak{q}_i \trianglelefteq R$.

Two questions: Existence? Uniqueness?

Let's start with existence.

Def An ideal $\mathfrak{q} \trianglelefteq R$ is called irreducible if it cannot be written as $\mathfrak{q} = \mathfrak{q}_1 \cap \mathfrak{q}_2$ with $\mathfrak{q}_1, \mathfrak{q}_2 \neq \mathfrak{q}$.

Thm If R is Noetherian, then

a) every ideal $\mathfrak{a} \ntrianglelefteq R$ is a finite intersection of irreducibles,

b) every irreducible ideal $\mathfrak{q} \trianglelefteq R$ is primary

Pf. a) Put $\mathcal{S} := \{$ proper ideals $\mathfrak{a} \ntrianglelefteq R$ that are not finite intersections of irreducibles $\}$.

If $\mathcal{S} \neq \emptyset$,

we could find a maximal element $\mathfrak{a} \in \mathcal{S}$ (since R Noetherian).

$\Rightarrow$ $\mathfrak{a}$ not irreducible, say $\mathfrak{a} = \mathfrak{a}_1 \cap \mathfrak{a}_2$ w/ $\mathfrak{a}_1, \mathfrak{a}_2 \neq \mathfrak{a}$

$\Rightarrow$ by maximality both $\mathfrak{a}_i$ are finite intersections of irred.

$\Rightarrow$ so is $\mathfrak{a}$, ie. $\mathfrak{a} \notin \mathcal{S}$ $\lightning$

b) Let $\mathfrak{q} \trianglelefteq R$ be irreducible.

Passing to $R/\mathfrak{q}$ we may assume $\mathfrak{q} = (0)$.

Want: $(0) \trianglelefteq R$ irreducible $\Rightarrow$ every zero divisor $b \in R$ is nilpotent.

Assume $ab = 0$ but $a \neq 0$.

Consider the chain

$$\mathrm{Ann}(b) \subseteq \mathrm{Ann}(b^2) \subseteq \mathrm{Ann}(b^3) \subseteq \cdots \trianglelefteq R.$$

R Noetherian $\Rightarrow \exists n \in \mathbb{N}$: $\mathrm{Ann}(b^n) = \mathrm{Ann}(b^{n+1})$.

We want to show $(a) \cap (b^n) = (0)$

(then $b^n = 0$ by irreducibility of $(0) \trianglelefteq R$).

Indeed, let

$$\lambda a = \mu b^n \in (a) \cap (b^n) \quad \text{w/ } \lambda, \mu \in R$$

$$\Longrightarrow \mu b^{n+1} = \lambda a b = \lambda \cdot 0 = 0$$

$$\Longrightarrow \mu \in \mathrm{Ann}(b^{n+1}) = \mathrm{Ann}(b^n)$$

$$\Longrightarrow \mu b^n = 0 \quad \text{as required.}$$

$\square$

Caution: The converse to b) does NOT hold:

e.g. take $R = k[X,Y]$ for a field k,

then $\mathfrak{q} := (x^2, xy, y^2) = (x,y)^2$

is primary (being a power of a max. ideal)

but not irreducible since

$$\mathfrak{q} = (x, y^2) \cap (y, x^2).$$

$\Longrightarrow$ In particular, primary decompositions are not unique!

Imposing irreducibility of the factors doesn't help:

e.g. $(x,y^2) \cap (y,x^2) = (x, \check{y}^2) \cap (\check{y}, x^2)$ for $\check{y} := y + x$

Exercise: These four ideals are all irreducible, but looking at linear terms shows $(y,x^2) \neq (x,\check{y}^2), (\check{y},x^2)$.

So let's try to be more economic:

Lemma: If $\mathfrak{q}_1, \dots, \mathfrak{q}_n \trianglelefteq R$ are $\mathfrak{p}$-primary for the same prime $\mathfrak{p} \in \mathrm{Spec}(R)$, then so is $\mathfrak{q} := \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n$.

Pf. By def^n of the radical,

$$\sqrt{\mathfrak{q}} = \sqrt{\mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n} \overset{!}{=} \sqrt{\mathfrak{q}_1} \cap \dots \cap \sqrt{\mathfrak{q}_n} = \mathfrak{p} \cap \dots \cap \mathfrak{p} = \mathfrak{p}.$$

To check $\mathfrak{q}$ is primary, assume $ab \in \mathfrak{q}$ but $a \notin \mathfrak{q}$.

$\Longrightarrow \exists i \in \{1, \dots, n\}: \; a \notin \mathfrak{q}_i$

But $ab \in \mathfrak{q}_i$ & $\mathfrak{q}_i$ is primary $\Longrightarrow b \in \sqrt{\mathfrak{q}_i} = \mathfrak{p} = \sqrt{\mathfrak{q}}$,

ie $\exists m: \; b^m \in \mathfrak{q}$.

$\square$

Cor / Def: Any primary decomposition of an ideal $\mathfrak{a} \trianglelefteq R$ can be changed (applying the lemma & removing terms) to a primary decomposition $\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n$ which is minimal in the sense that

- $\sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j} \quad \forall i \neq j$,
- none of the $\mathfrak{q}_i$ can be removed: $\bigcap_{j \neq i} \mathfrak{q}_j \not\subseteq \mathfrak{q}_i \quad \forall i \in \{1, \dots, n\}$.

... still not unique:

Ex The ideal $\mathfrak{a} := (x^2, xy) \trianglelefteq R = k[x,y]$ has the minimal primary decompositions

$$\mathfrak{a} = (x) \cap (x,y)^2 = (x) \cap (x^2, y).$$

Note: The two decompositions differ, but they share the set of radicals: (X) and (X,Y).

Thm ("1st uniqueness thm for primary decomposition")

Let $\mathfrak{a} \trianglelefteq R$ have a minimal primary decomposition

$$\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n.$$

Then up to permutation the radicals $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$ only depend on $\mathfrak{a}$: They are precisely the prime ideals of the form $\mathfrak{p} = \sqrt{(\mathfrak{a} : x)}$ with $x \in R$

and $(\mathfrak{a} : x) := \mathrm{Ann}(\bar{x} \in R/\mathfrak{a})$

$:= \{ a \in R \mid ax \in \mathfrak{a} \}$.

Pf. Step ①:

- $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i \implies (\mathfrak{a} : x) = \bigcap_{i=1}^n (\mathfrak{q}_i : x)$

$$\implies \sqrt{(\mathfrak{a} : x)} = \bigcap_{i=1}^n \sqrt{(\mathfrak{q}_i : x)}$$

$$= \bigcap_{\mathfrak{q}_i \not\ni x} \sqrt{(\mathfrak{q}_i : x)}$$

(if $x \in \mathfrak{q}_i$ then $(\mathfrak{q}_i : x) = R$)

- $\mathfrak{q}_i$ primary with $x \notin \mathfrak{q}_i$ $\implies \sqrt{(\mathfrak{q}_i : x)} = \sqrt{\mathfrak{q}_i}$

- Conclusion: $\sqrt{(\mathfrak{a} : x)} = \bigcap_{\mathfrak{q}_i \not\ni x} \sqrt{\mathfrak{q}_i}$ $(*)$

$\implies$ If $\mathfrak{p} := \sqrt{(\mathfrak{a} : x)}$ is prime, then $\exists i$ with $\mathfrak{p} = \sqrt{\mathfrak{q}_i}$

Step ②: Conversely, $\forall i \in \{1, \dots, n\}$ $\exists x \in \bigcap_{j \neq i} \mathfrak{q}_j \setminus \mathfrak{q}_i$

(since the primary decomposition is minimal)

$(*) \implies \sqrt{\mathfrak{q}_i} = \sqrt{(\mathfrak{a} : x)}$ $\square$

Rem. If R is Noetherian, then the $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$ can also be characterized as being precisely those ideals $(\mathfrak{a} : y)$ that are prime ($y \in R$).

(without taking the radical)

Pf. Given $x \in R$ with $\sqrt{(\mathfrak{a}:x)} = \sqrt{\mathfrak{q}_i}$,

$\exists N \in \mathbb{N}$: $\sqrt{\mathfrak{q}_i}^{\,N} \subseteq \mathfrak{q}_i$ (because R is Noetherian)

$$\Rightarrow \Big(\bigcap_{j \neq i} \mathfrak{q}_j\Big) \cdot \sqrt{\mathfrak{q}_i}^{\,N} \subseteq \mathfrak{a} = \bigcap_{k=1}^{n} \mathfrak{q}_k \qquad (**)$$

Fix N minimal with $(**)$

$$\Rightarrow \exists\, y \in \Big(\bigcap_{j \neq i} \mathfrak{q}_j\Big) \cdot \sqrt{\mathfrak{q}_i}^{\,N-1} \text{ with } y \notin \mathfrak{a}$$

i.e. $y \notin \mathfrak{q}_i$.

But

$$\sqrt{\mathfrak{q}_i} \underset{\text{by } (**)}{\subseteq} (\mathfrak{a} : y) \underset{\text{trivial}}{\subseteq} \sqrt{(\mathfrak{a}:y)} \;=\; \sqrt{\mathfrak{q}_i}$$

by $(*)$ from previous proof, since $y \in \mathfrak{q}_j \;\forall j \neq i$

$\Rightarrow$ equality holds & we're done. $\square$

Def In the above setup, the $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i} \in \operatorname{Spec}(R)$ are called the <u>primes associated to</u> $\mathfrak{a} \trianglelefteq R$.

We divide them in two types:

a) The minimal ones among the $\mathfrak{p}_i$ are called <u>isolated primes</u>,

b) the others are <u>embedded primes</u>.

These terms come from geometry:

Lemma Let $\mathfrak{a} \trianglelefteq R$ have associated primes $\underbrace{\mathfrak{p}_1, \dots, \mathfrak{p}_m}_{\text{isolated}}, \underbrace{\mathfrak{p}_{m+1}, \dots, \mathfrak{p}_n}_{\text{embedded}}$

Then

$$V(\mathfrak{a}) = \bigcup_{i=1}^{m} V(\mathfrak{p}_i)$$

is the decomposition of $V(\mathfrak{a})$ in irreducible cpt^s, while each $V(\mathfrak{p}_j)$ with $j > m$ is embedded as a proper closed subset in one of these cpt^s (we also say that $V(\mathfrak{p}_j)$ is an "embedded cpt" of $V(\mathfrak{a}) = \operatorname{Spec} R/\mathfrak{a}$).

Pf. Pick a primary decomposition

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n \quad \text{with} \quad \mathfrak{p}_i = \sqrt{\mathfrak{q}_i}.$$

$$\Rightarrow \sqrt{\mathfrak{a}} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$$

$$= \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m \quad (\text{as each } \mathfrak{p}_j,\ j > m, \text{ is } \subseteq \mathfrak{p}_i \text{ for some } i \le m)$$

$$\Rightarrow V(\mathfrak{a}) = \bigcup_{i=1}^{m} V(\mathfrak{p}_i)$$

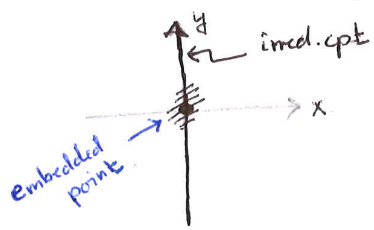
irreducible, closed, and none of them contained in another one.

$\square$

Ex a) $R := k[X,Y]$ (k a field)

$\triangledown \! |$

$\mathfrak{a} := (XY, X^2)$



Spec $R/\mathfrak{a}$

We've already seen the primary decomposition

$$\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \quad \text{where}$$

where $\mathfrak{q}_1 := \mathfrak{p}_1 = (X) = (\mathfrak{a} : Y)$ (isolated)

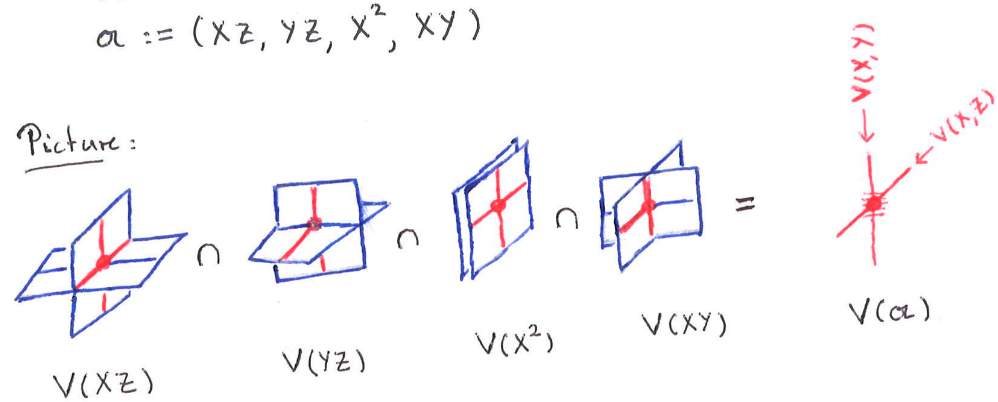
$\mathfrak{q}_2 := \mathfrak{p}_2^2$ with $\mathfrak{p}_2 := (X,Y) = (\mathfrak{a} : X)$ (embedded)

b) $R := k[X,Y,Z]$

$\triangledown \! |$

$\mathfrak{a} := (XZ, YZ, X^2, XY)$

Picture:



$\Rightarrow$ Spec $(R/\mathfrak{a})$ should be the union of the Y-axis & Z-axis but with a "fat point at the origin" ($\hat{=}$ tangent direction to X-axis at origin).

A primary decomposition:

$$\mathfrak{a} = \underbrace{(X,Z)}_{\mathfrak{q}_1} \cap \underbrace{(X,Y)}_{\mathfrak{q}_2} \cap \underbrace{(X^2,Y,Z)}_{\mathfrak{q}_3}$$

Indeed:
- $\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3$ are primary (exercise)
- $\mathfrak{q}_1 \cap \mathfrak{q}_2 = (X, YZ) \Rightarrow \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \mathfrak{q}_3 = \mathfrak{a}$.

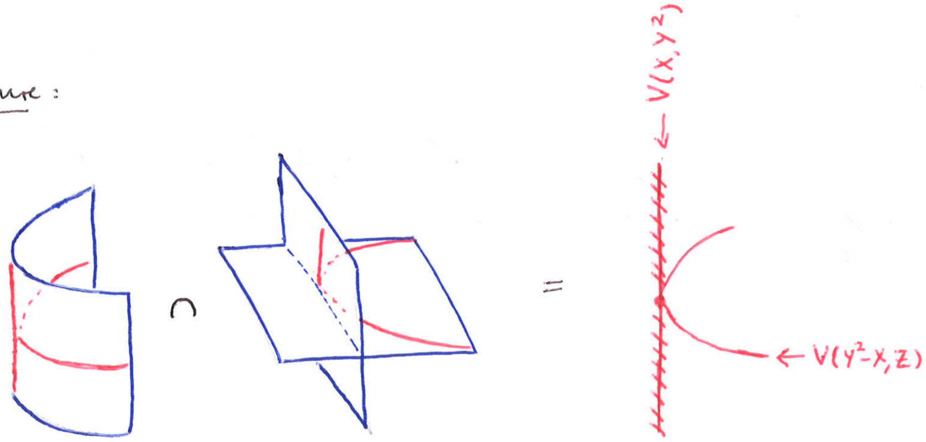
Associated primes:

$$\left.\begin{aligned} \mathfrak{p}_1 &= (X,Z) \\ \mathfrak{p}_2 &= (X,Y) \end{aligned}\right\} \text{(isolated)}$$

$\mathfrak{p}_3 = (X,Y,Z)$ (embedded)

c) $k[X,Y,Z]$
$\trianglerighteq$
$\mathfrak{a} := (Y^2 - X, XZ)$

Picture:



$V(Y^2-X) \qquad \cap \qquad V(XZ) \qquad = \qquad V(\mathfrak{a})$

$\Rightarrow$ Spec$(R/\mathfrak{a})$ should be the union of the parabola $V(Y^2-X, Z)$ with the Z-axis, but the Z-axis with "multiplicity two" ($\hat{=}$ tangents in Y-direction along the X-axis)

A primary decomposition:

$$\mathfrak{a} = \underbrace{(X, Y^2)}_{\mathfrak{q}_1} \cap \underbrace{(Y^2-X, Z)}_{\mathfrak{q}_2}$$

Associated primes:

$\mathfrak{p}_1 = (X, Y)$ (both are isolated)
$\mathfrak{p}_2 = (Y^2 - X, Z)$

Rem In the last example $\mathfrak{q}_1 \neq \mathfrak{p}_1$ although $\mathfrak{p}_1$ was isolated.

Q: Are primary cpt^s $\mathfrak{q}_i$ of isolated primes $\mathfrak{p}_i$ unique (all previous cases of non-uniqueness were about embedded primes)?

Idea: Trivially true if $\exists!$ primary cpt. In general, can "zoom in" to kill all other primary cpt^s by localizing!

Lemma. Let $S \subset R$ be a multiplicative subset and $\mathfrak{p} \in \operatorname{Spec} R$.

a) If $\mathfrak{p} \cap S \neq \emptyset$, then $\mathfrak{q} \cdot R_S = (1)$ $\forall$ $\mathfrak{p}$-primary ideal $\mathfrak{q} \trianglelefteq R$.

b) If $\mathfrak{p} \cap S = \emptyset$, then the localizat^n $\varphi: R \to R_S$ induces a bijection

$$\left\{ \begin{array}{c} \mathfrak{p}\text{-primary ideals} \\ \text{in } R \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \mathfrak{p}R_S\text{-primary} \\ \text{ideals in } R_S \end{array} \right\}$$

$$\begin{tikzcd} \mathfrak{q} \arrow[r, mapsto] & \mathfrak{q}R_S \arrow[l, bend left, "\varphi^{-1}"] \end{tikzcd}$$

Pf. a) Recall $\mathfrak{p} = \sqrt{\mathfrak{q}}$ if $\mathfrak{q}$ is $\mathfrak{p}$-primary.

Thus: $s \in S \cap \mathfrak{p} \Rightarrow \exists n : s^n \in S \cap \mathfrak{q} \Rightarrow \frac{s^n}{1} \in \mathfrak{q} R_S \cap R_S^*$

$$\Rightarrow \mathfrak{q} R_S = (1)$$

b) Let $S \cap \mathfrak{p} = \emptyset$.

If $\mathfrak{q}$ is $\mathfrak{p}$-primary, then $\mathfrak{q} R_S$ is $\mathfrak{p} R_S$-primary:

- $\mathfrak{q} R_S$ is primary: $\frac{a}{s}, \frac{b}{t} \in R_S$ with $\frac{a}{s}\frac{b}{t} \in \mathfrak{q} R_S$ but $\frac{a}{s} \notin \mathfrak{q} R_S$

  $\Rightarrow \exists u \in S : \; uab \in \mathfrak{q}$

  but $va \notin \mathfrak{q} \; \forall v \in S$

  In particular $ua \notin \mathfrak{q}$, so $\exists n : b^n \in \mathfrak{q}$
  since $\mathfrak{q}$ primary

  $\Rightarrow \left(\frac{b}{t}\right)^n \in \mathfrak{q} R_S$

- $\sqrt{\mathfrak{q} R_S} = \sqrt{\mathfrak{q}} \cdot R_S = \mathfrak{p} R_S$

Conversely, if $\mathfrak{q}_S \trianglelefteq R_S$ is $\mathfrak{p} R_S$-primary,
then $\varphi^{-1}(\mathfrak{q}_S)$ is $\mathfrak{p}$-primary (exercise).

Finally, these assignments are mutually inverse:

- $\varphi^{-1}(\mathfrak{q}_S) \cdot R_S = \mathfrak{q}_S$ (true for all ideals in a localization)
- $\varphi^{-1}(\mathfrak{q} \cdot R_S) = \mathfrak{q}$ ($\frac{a}{1} \in \mathfrak{q} R_S \Rightarrow \exists s \in S : s \cdot a \in \mathfrak{q} \underset{\substack{s \notin \mathfrak{q} \; \& \\ \mathfrak{q} \text{ primary}}}{\Rightarrow} \exists n : a^n \in \mathfrak{q} \underset{\mathfrak{q} \text{ primary}}{\Rightarrow} a \in \mathfrak{q}$) $\square$

Prop Let $S \subset R$ be multiplicative,

$\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n$ a minimal primary decomposition

with $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$ disjoint from S for $i = 1, \dots, m$
but not for $i = m+1, \dots, n$.

$\Rightarrow$ Have minimal primary decompositions

- $\mathfrak{a} R_S = \bigcap_{i=1}^{m} \mathfrak{q}_i R_S$ in R_S
- $\varphi^{-1}(\mathfrak{a} R_S) = \bigcap_{i=1}^{m} \mathfrak{q}_i$ in R

Pf. $\mathfrak{a} R_S = (\mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n) R_S$

$= \bigcap_{i=1}^{n} \mathfrak{q}_i R_S$ as localization commutes w/ finite intersections

$= \bigcap_{i=1}^{m} \mathfrak{q}_i R_S$ as $\mathfrak{q}_i R_S = (1)$ for $i > m$,

and this is a minimal primary decomposition
by previous lemma.

$\square$

Now apply φ^{-1} and use the lemma again.

Cor. ("2nd uniqueness thm for primary decomposition")

Let $\mathfrak{a} \trianglelefteq R$ have a minimal primary decomposition

$$\mathfrak{a} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_n,$$

labelled such that among the associated primes $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$, precisely $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ are isolated (ie minimal).

$\Rightarrow$ Up to permutation $\mathfrak{q}_1, \dots, \mathfrak{q}_m \trianglelefteq R$ are determined uniquely by the ideal $\mathfrak{a}$.

Pf. The set of isolated primes $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ only depends on $\mathfrak{a}$.
For $i = 1, \dots, m$ the proposition gives

$$\mathfrak{q}_i = \varphi^{-1}(\mathfrak{a} R_S) \quad \text{for } S := R \setminus \mathfrak{p}_i,$$

because $\mathfrak{p}_j \cap S \neq \emptyset$ for all $j \neq i$ (using minimality of $\mathfrak{p}_i$). $\square$

Application For R Noetherian, $\mathfrak{p} \in \operatorname{Spec} R$, $n \in \mathbb{N}$, have $V(\mathfrak{p}^n) = V(\mathfrak{p})$ irreducible

$\Rightarrow \exists!$ primary component $\mathfrak{q} = \mathfrak{q}_1$ of $\mathfrak{p}^n = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_m$ corresponding to the unique isolated prime $\mathfrak{p} = \sqrt{\mathfrak{q}_1}$.

Def We call $\mathfrak{p}^{(n)} := \mathfrak{q}$ the n-th symbolic power of $\mathfrak{p}$.

Rem $\mathfrak{p}^n \subseteq \mathfrak{p}^{(n)}$ with "=" iff $\mathfrak{p}^n$ is primary.

Thm (Zariski-Nagata) Let $R = k[X_1, \dots, X_N]$ w/ k an alg closed field. For $\mathfrak{p} \in \operatorname{Spec} R$ put $Z = V(\mathfrak{p}) \subseteq k^N$

$$\Rightarrow \mathfrak{p}^{(n)} = \{ f \in R \mid f \text{ vanishes to order} \geq n \text{ at every } z \in Z \}$$

$\left(:= \bigcap_{z \in Z} \mathfrak{m}_z^n \text{ for the maximal ideal } \mathfrak{m}_z \trianglelefteq R \right)$

... proof uses Hilbert's Nullstellensatz.

III. Integrality and the Nullstellensatz

1. Finite and integral extensions

Def Let A be a ring.

By an A-algebra we mean a ring B together with a ring homomorphism $\varphi : A \to B$

(not required to be injective)

We call B finitely generated as an A-algebra if $\exists$ epi $\tilde{\varphi} : A[X_1, \dots, X_n] \twoheadrightarrow B$ extending φ,

i.e. if $\exists\, b_1, \dots, b_n \in B$ sth $B = A[b_1, \dots, b_n]$

$:= \operatorname{im}(A[X_1, \dots, X_n] \xrightarrow{\text{extending } \varphi} B)$

$X_i \longmapsto b_i$

Want a much stronger notion:

We call B finite over A if B is fin. gen. as an A-module (!).

Abuse of notation: We then also say "B/A is a finite ring extension" even though φ needn't be injective ...

Prop Let B be an A-algebra. For $b \in B$ the following are equivalent:

a) The subring $A[b] \subseteq B$ is finite over A.

b) $\exists$ fin.gen. A-submodule $M \subseteq B$ with $1 \in M$ and $b \cdot M \subseteq B$.

c) $\exists\, a_1, \ldots, a_n \in A$ s.th.

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

Def We then say that b is <u>integral</u> over A. We say that B is <u>integral</u> over A iff all $b \in B$ are.

Pf of the prop.

(a) $\Rightarrow$ (b): trivial with $M := A[b]$.

(c) $\Rightarrow$ (a): trivial since (c) implies $A[b] = \sum_{i=0}^{n-1} A \cdot b^i$ is generated as an A-module by $1, b, b^2, \ldots, b^{n-1}$.

(b) $\Rightarrow$ (c): Pick generators $m_i \in M$, say $M = Am_1 + \cdots + Am_n$ w/ $m_1 := 1$.

Then $b \cdot M \subseteq M$ gives a system of equations

$$\begin{aligned} bm_1 &= c_{11} m_1 + \cdots + c_{1n} m_n \\ &\vdots \\ bm_n &= c_{n1} m_1 + \cdots + c_{nn} m_n \end{aligned}$$

with $c_{ij} \in A$ (not necessarily unique but that doesn't matter).

$\Longrightarrow$ the matrix $\Delta := (\delta_{ij} \cdot b - c_{ij})_{1 \le i,j \le n} \in \mathrm{Mat}_{n \times n}(A[b])$

satisfies $\Delta \cdot v = 0$ for $v := \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$ $(*)$

By Cramer's rule

$$\Delta^{ad} \cdot \Delta = \det(\Delta) \cdot \mathbb{1} \qquad (**)$$

for the adjoint matrix Δ^{ad} whose (i,j)-entry is

$$(-1)^{i+j} \cdot \det(\Delta^{(ij)})$$

Δ with row j & column i deleted

NB: $(**)$ is a polynomial identity in the entries of Δ, hence it holds over any ring if it does so over $\mathbb{Z}$. But over $\mathbb{Z}$ it is true since it is so over $\mathbb{Q} = \mathrm{Quot}(\mathbb{Z})$.

$(*) + (**) \implies \quad \det(\Delta)\cdot\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0$

$\implies \det(\Delta)\cdot m_i = 0 \quad \forall i$

$\implies \det(\Delta) = 0 \quad$ since $m_1 = 1 \in B$.

In other words: $\quad \det(\delta_{ij}\cdot b - \underset{\substack{\uparrow \\ \in A}}{c_{ij}}) = 0$

Expanding this gives an equation

$$b^n + a_1 b^{n-1} + \dots + a_n = 0 \quad \text{w/ } a_1, \dots, a_n \in A.$$

$\square$

<u>Ex</u> If a ring extension $A \to B$ is finite, then it is integral.
The converse does not hold:

e.g. an extension of fields $A = k \hookrightarrow B = K$ is

- finite iff $\dim_k(K) < \infty$
- integral iff K/k is an <u>algebraic</u> extension,
  ie. a (possibly infinite) union of finite ones.

<u>In general</u>: B/A integral $\iff$ union of finite subextensions B_i/A

(e.g. $B_i := A[i] \ \forall i \in B$).

<u>Lemma</u> If $A \xrightarrow[\varphi]{} B$ is an integral (resp. finite) extension, then so are

a) $A/\mathfrak{a} \xrightarrow{\varphi} B/\mathfrak{b} \quad \forall\, \mathfrak{a} \trianglelefteq A,\ \mathfrak{b} \trianglelefteq B$ w/ $\varphi(\mathfrak{a}) \subseteq \mathfrak{b}$,

b) $C = A \otimes_A C \xrightarrow{\varphi} B \otimes_A C$ for any A-algebra C,

c) $A_S \xrightarrow{\varphi} B_{\varphi(S)}$ for any multiplicative subset $S \subseteq A$,

d) $A[X] \xrightarrow{\varphi} B[X]$.

Pf. Part d) follows from b) with $C := A[X]$.

Part c) —— " —— $C := A_S$

using $B \otimes_A A_S \simeq B_{\varphi(S)}$.

Part a), b) are trivial if B/A is finite.

If B/A is integral, write $B = \bigcup_{i \in I} B_i$ with B_i/A finite A-subalgebra.

$$\implies B/\mathfrak{b} = \bigcup_{i \in I} B_i / \mathfrak{b} \cap B_i \longleftarrow \text{finite}/A \ \forall i$$

$$B \otimes_A C = \bigcup_{i \in I} \underbrace{\mathrm{im}\,(\underset{\substack{\uparrow \\ \text{finite}/C}}{B_i \otimes_A C} \to B \otimes_A C)}_{\text{hence finite}/C}$$

$\square$

Lemma If $A \xrightarrow[\varphi]{} B$ & $B \xrightarrow[\psi]{} C$ are integral (resp. finite), then so is $A \xrightarrow[\psi\circ\varphi]{} C$.

Pf. For "finite" this is obvious:

$$B = \sum_{i=1}^{m} A \cdot b_i \qquad C = \sum_{j=1}^{n} B \cdot c_j \quad \Longrightarrow \quad C = \sum_{i=1}^{m} \sum_{j=1}^{n} A \cdot c_{ij}$$

w/ $c_{ij} := b_i c_j$.

For "integral" let $c \in C$.

C/B integral $\Longrightarrow$ $\exists\, b_1, \dots, b_n \in B$:

$$c^n + b_1 c^{n-1} + \dots + b_n = 0 \qquad (*)$$

(proposition, part c))

B/A integral $\Longrightarrow$ $A[b_1]$ finite $/A$ (proposition, part a))

$A[b_2]$ finite $/A$, so $A[b_1, b_2]$ finite $/ A[b_1]$

$\vdots$

$A[b_1, \dots, b_n]$ finite $/ A[b_1, \dots, b_{n-1}]$

$\Longrightarrow A[b_1, \dots, b_n]$ finite $/A$ $\qquad (**)$

$\xrightarrow{(*)+(**)}$ $A[b_1, \dots, b_n, c]$ finite $/A$ $\Longrightarrow$ c integral $/A$

(by proposition, part b)) $\square$

2. The integral closure

Lemma. For any A-algebra B, the set

$$\bar{A} := \{ b \in B \mid b \text{ integral over } A \} \subseteq B$$

is a subring.

Pf.

$b_1, b_2 \in \bar{A} \Longrightarrow A[b_1, b_2]$ finite $/A$ by previous lemma (or its proof)

$\Longrightarrow b_1 + b_2 \in \bar{A}$

$b_1 \cdot b_2 \in \bar{A}$ by proposition, part c). $\square$

Def We call $\bar{A}$ the <u>integral closure</u> (or "<u>normalization</u>") of A in B.

We always have $\varphi(A) \subseteq \bar{A}$ for the structure map $\varphi : A \to B$.

If $\bar{A} = \varphi(A)$ we say that A is <u>integrally closed</u> in B.

When A is an integral domain and $B := \mathrm{Quot}(A)$, then we also drop the phrase "in B" and just talk about "the integral closure / normalization of A" resp about A being "integrally closed / normal".

Remark For any $\varphi : A \to B$, the integral closure $\bar{A} \subseteq B$ is integrally closed in B.

Pf. If $b \in B$ is integral over $\bar{A}$, then it is so over A because the extension $\bar{A}/A$ is integral. $\square$

Ex Any UFD is normal (exercise).

Ex Taking $B = \mathbb{C}$ we get

$$\pi \notin \bar{\mathbb{Q}} = \{ b \in \mathbb{C} \mid \exists \text{ monic } p \in \mathbb{Q}[X] \text{ w/ } p(b) = 0 \} \quad \text{"algebraic numbers"}$$

$\ni 1/\sqrt{2},\ i/2, \ldots$

$$\bar{\mathbb{Z}} = \{ b \in \mathbb{C} \mid \exists \text{ monic } p \in \mathbb{Z}[X] \text{ w/ } p(b) = 0 \} \quad \text{"algebraic integers"}$$

$\ni \sqrt{2},\ i, \ldots$

Too big?

Def A number field is a finite field extension $K/\mathbb{Q}$. Its ring of integers is defined to be

$$\mathcal{O}_K := (\text{integral closure of } \mathbb{Z} \text{ in } K) = \bar{\mathbb{Z}} \cap K$$

for any embedding $K \hookrightarrow \bar{\mathbb{Q}}$.

$$\Longrightarrow \bar{\mathbb{Q}} = \bigcup_{\substack{K \subset \bar{\mathbb{Q}} \\ \text{number field}}} K \supset \bar{\mathbb{Z}} = \bigcup_{\substack{K \subset \bar{\mathbb{Q}} \\ \text{number field}}} \mathcal{O}_K .$$

How to compute these?

Lemma Let A be a normal integral domain, K/k a finite extension field of $k = \mathrm{Quot}(A)$ and $B :=$ integral closure of A inside K.

Then

a) $B = \{ b \in K \mid$ the (normed) minimal polynomial of b over k lies in $A[X] \subset k[X] \}$

$= \{ b \in K \mid$ the (normed) characteristic polynomial of b for the extension K/k lies in $A[X] \}$

b) $K = \{ \frac{b}{a} \mid b \in B,\ a \in A \setminus \{0\} \}$.

Pf. a) If the min./char. polynomial of b lies in $A[X]$, then b satisfies a monic polynomial eq^n over A, $\Longrightarrow b \in B$.

Conversely, if $b \in B$, consider an algebraic closure $\bar{k}/k$ & fix an embedding $K \hookrightarrow \bar{k}$. Put $\bar{A} :=$ int. closure of A in $\bar{k}$:

$$\begin{tikzcd}
\bar{A} \arrow[r, hook] \arrow[d, dash] & \bar{k} \arrow[d, dash] \\
B \arrow[r, hook] \arrow[d, dash] & K \arrow[d, dash] \\
A \arrow[r, hook] & k
\end{tikzcd}$$

$\Rightarrow$ $\mathrm{Gal}(\bar{k}/k)$ acts on $\bar{k}$

& this action preserves the subring $\bar{A} \hookrightarrow \bar{k}$

(since it is trivial on $A \hookrightarrow k$)

$\Rightarrow$ Since $b \in B \subseteq \bar{A}$,

we have $\sigma(b) \in \bar{A}$ $\forall\, \sigma \in \mathrm{Gal}(K/k)$

But these $\sigma(b)$ are precisely the zeroes of the min/char polynomial $p_b(X) \in k[X]$

$\Rightarrow$ $p_b(X)$ has coeff^s in $k \cap \bar{A} \underset{\uparrow}{=} A$

A int. closed in k

b) Let $x \in K$

$\Rightarrow$ x algebraic $/k$, say $a_0 x^n + a_1 x^{n-1} + \dots + a_n = 0$

with $a_0, \dots, a_n \in k$, $a_0 \neq 0$

Multiply by common denominator $\Rightarrow$ wlog all $a_i \in A$

Multiply by $a := a_0^{n-1}$

$\Rightarrow$ monic equation for $b := a \cdot x$ w/ coeff^s in A,

hence $x = \frac{b}{a}$ with $b \in B$. $\square$

Ex $A = \mathbb{Z} \subset k = \mathbb{Q}$

$\Rightarrow$ for any number field K,

get $\mathcal{O}_K = \{ c \in K \mid \mathrm{minpol}(c) \in \mathbb{Z}[X] \}$

Special case:

$K = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ squarefree

has $\mathcal{O}_K = \mathbb{Z}[\alpha]$, $\alpha := \begin{cases} \sqrt{d} & \text{if } d \equiv 2,3 \bmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \bmod 4. \end{cases}$

Pf. Let $c = a + b\sqrt{d} \in K$ $(a, b \in \mathbb{Q}$, wlog $b \neq 0)$

$\Rightarrow$ $\mathrm{minpol}(c) = X^2 - 2aX + (a^2 - b^2 d)$

$\Rightarrow$ $c \in \mathcal{O}_K$ iff $\begin{cases} 2a \in \mathbb{Z} \\ \text{and } a^2 - b^2 d \in \mathbb{Z} \end{cases}$

This is equivalent to $\begin{cases} a, b \in \mathbb{Z} & \text{if } d \equiv 2,3 \bmod 4 \\ a, b \in \frac{1}{2}\mathbb{Z} \ \& \ a - b \in \mathbb{Z} & \text{else} \end{cases}$

(exercise). $\square$

Geometrically, for an integral domain A, being normal ($=$ integrally closed in $K = \mathrm{Quot}(A)$) is a kind of "nonsingularity condition" on Spec A:

Ex Let $A := \mathbb{R}[X,Y]/(Y^2 - X^2(X+1))$,

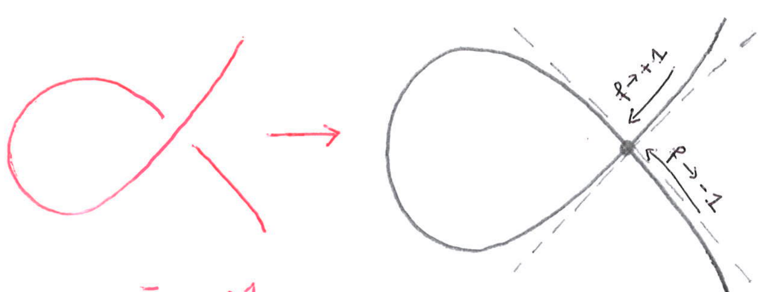
$$\left.\begin{array}{l} x := \text{image}(X) \\ y := \text{image}(Y) \end{array}\right\} \in A$$

$\Rightarrow$ $f := \dfrac{y}{x} \in \mathrm{Quot}(A) = K$

is a rational fct^n on Spec A

well-defined on the complement of $(0,0)$.

The problem at $(0,0)$ is not a pole but that f approaches two different values along the two branches as $(x,y) \to (0,0)$:



Spec $\bar{A} \cong \mathbb{A}^1_{\mathbb{R}}$ Spec A

We have $f^2 \to +1$ as $(x,y) \to (0,0)$ on both branches, and indeed

$$f^2 = \frac{y^2}{x^2} = x + 1 \in A$$

$\Rightarrow$ $f \in K$ is integral over A but $f \notin A$

$\Rightarrow$ A is not normal

Claim: Its normalization is $\bar{A} = A[f] \simeq k[z]$ with the map $A \hookrightarrow k[z]$ given by $x \mapsto z^2 - 1$, $y \mapsto z\cdot(z^2-1)$

Pf. Since f is integral over A, we know $A[f] \hookrightarrow \bar{A}$.

$\Rightarrow$ equality if we can show $A[f] \simeq k[z]$, since $k[z]$ is a normal domain.

Indeed:

$$A[f] = k[X, Y, \tfrac{Y}{X}]/(Y^2 - X^2(X+1)) \xrightarrow{\varphi} k[z]$$

$$X \longmapsto z^2 - 1$$

$$Y \longmapsto z\cdot(z^2-1)$$

is
- well-defined
- iso w/ inverse given by $z \mapsto \frac{y}{x} = f$. $\square$

3. Going up & down

Q: Given an integral ring extension $A \hookrightarrow B$, how do prime ideals in B relate to those in A?

Prop ("lying over") Let $A \hookrightarrow B$ be integral. Then $\operatorname{Spec} B \to \operatorname{Spec} A$ is onto, ie $\forall\, \mathfrak{p} \in \operatorname{Spec} A\ \exists\, \mathfrak{q} \in \operatorname{Spec} B$ with $\mathfrak{p} = \mathfrak{q} \cap A$.

Pf. Localize at $S := A \setminus \mathfrak{p}$.

Then $A_\mathfrak{p} := A_S \longrightarrow B_\mathfrak{p} := B_S$ is still integral and we get a commutative diagram

$$\begin{tikzcd} B \arrow[r, "\varphi"] & B_\mathfrak{p} \\ A \arrow[u] \arrow[r] & A_\mathfrak{p} \arrow[u] \end{tikzcd}$$

Note: $B_\mathfrak{p} \neq \{0\}$ because $A \hookrightarrow B$ is injective !!!

$A_\mathfrak{p}$ is local!

Pick any $\mathfrak{m} \in \operatorname{Spm}(B_\mathfrak{p}) \overset{(*)}{\Rightarrow} \mathfrak{m} \cap A_\mathfrak{p} \in \operatorname{Spm}(A_\mathfrak{p}) = \{\mathfrak{p}A_\mathfrak{p}\}$

$\Rightarrow \mathfrak{q} := \varphi^{-1}(\mathfrak{m}) \in \operatorname{Spec} B$ has $\mathfrak{q} \cap A = \mathfrak{p}$. $\square$

(*): Use integrality (see below)!

For (*) we've used:

Rem Let $A \hookrightarrow B$ be integral.

a) If B (hence A) is a domain, then A is a field iff B is a field.

b) $\mathfrak{q} \in \operatorname{Spec} B$ is maximal iff $\mathfrak{p} = \mathfrak{q} \cap A \in \operatorname{Spec} A$ is so.

Pf. a) A field

$b \in B \setminus \{0\}$, say $b^n + a_1 b^{n-1} + \dots + a_n = 0$ w/ $a_i \in A$

If B is a domain, then wlog $a_n \neq 0$ (take n minimal)

$\Rightarrow b^{-1} = -\underbrace{\tfrac{1}{a_n}}_{\in A} \underbrace{(b^{n-1} + a_1 b^{n-2} + \dots + a_{n-1})}_{\in B} \in B \Rightarrow B$ field

Conversely: B field

$a \in A \setminus \{0\}$, say $b := a^{-1}$ satisfies $b^n + a_1 b^{n-1} + \dots + a_n = 0$ w/ $a_i \in A$

Multiply eqn by a^{n-1}

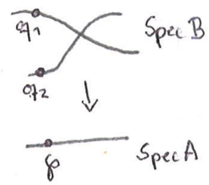
$\Rightarrow a^{-1} = -a_1 - a_2 a - \dots - a_n a^{n-1} \in A \Rightarrow A$ field $\square$

b) Apply a) to $A/\mathfrak{p} \hookrightarrow B/\mathfrak{q}$.

Def If $\mathfrak{q} \in \operatorname{Spec} B$ and $\mathfrak{q} \cap A = \mathfrak{p}$ we say $\mathfrak{q}$ lies over $\mathfrak{p}$ and write

$$\begin{tikzcd} \mathfrak{q} \arrow[r, hook] \arrow[d, dash] & B \arrow[d, dash] \\ \mathfrak{p} \arrow[r, hook] & A. \end{tikzcd}$$

Rem Usually $\exists$ more than one q over the same p, ie $\operatorname{Spec} B \to \operatorname{Spec} A$ needn't be injective: Consider $A = k[t] \hookrightarrow B := k[\sqrt{t}]$ ...



But:

Prop ("Incomparability") If $A \hookrightarrow B$ is integral and $q_1 \neq q_2 \in \operatorname{Spec} B$ lie over the same $p \in \operatorname{Spec} A$, then $q_1 \not\subseteq q_2 \not\subseteq q_1$.

Pf. Assume $q_1 \overset{\neq}{\hookrightarrow} q_2$ with $q_1 \cap A = q_2 \cap A = p$.

The extension $\bar{A} := A/p \hookrightarrow \bar{B} := B/q_1$ is integral.

For $b \in q_2 \setminus q_1$ and $\bar{b} := \text{image}(b) \in \bar{B}$,

have $\bar{b}^n + \bar{a}_1 \bar{b}^{n-1} + \dots + \bar{a}_n = 0$ w/ $a_1, \dots, a_n \in B$.

Assume n minimal $\Rightarrow$ $\bar{a}_n \neq 0$ as $\bar{B}$ is a domain

Eq^n gives $\bar{a}_n = -\bar{b}^n - \dots - \bar{a}_{n-1}\bar{b} \in \bar{q}_2 := q_2 \cdot \bar{B} = q_2/q_1$

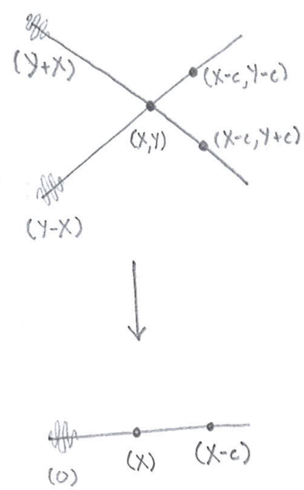
But also $a_n \in A$, so $a_n \in q_2 \cap A = p = q_1 \cap A$

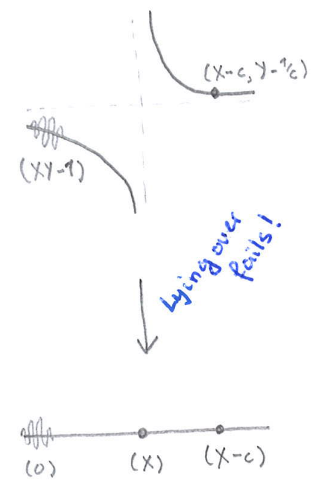
$\Longrightarrow \bar{a}_n = 0$ ↯ $\square$

A geometric example: Let k be an alg closed field

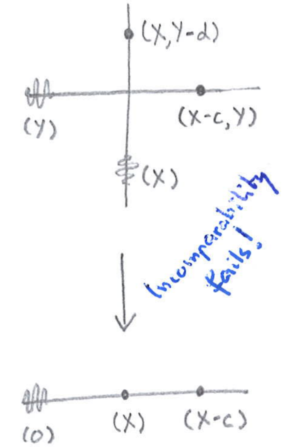
$$A := k[X] \longrightarrow B := k[X,Y]/(f)$$

$f = Y^2 - X^2$	$f = XY - 1$	$f = XY$
$A \to B$ integral since $Y \in B$ is integral over A $(Y^2 - \underset{\substack{\cap \\ A}}{X^2} = 0)$	$A \to B$ not integral, indeed $B \simeq k[X, X^{-1}]$ and X^{-1} is not integral over $A = k[X]$	$A \to B$ not integral, indeed $Y \in B$ generates the A-algebra $B \simeq A \oplus \bigoplus_{i \geq 1} \underbrace{Y^i \cdot k}_{\text{w/ X acting by zero}}$, which is not fin gen as an A-module.
$\operatorname{Spec} B \to \operatorname{Spec} A$ onto:	$\operatorname{Spec} B \to \operatorname{Spec} A$ not onto:	$\operatorname{Spec} B \to \operatorname{Spec} A$ onto but has a fiber of dim >0:





No prime in Spec B lies over $p = (X)$!



Here $(X) \overset{\neq}{\hookrightarrow} (X, Y-d)$ in Spec B both lie over the same $p = (X)$!

Goal: Want to apply "lying over" inductively for chains of prime ideals: Given $\mathfrak{p}_1 \subset \mathfrak{p}_2$ in Spec A and $\mathfrak{q}_i \in \operatorname{Spec} B$ over $\mathfrak{p}_i$ for one $i \in \{1,2\}$, want to find $\mathfrak{q}_j$ over $\mathfrak{p}_j$ for the other $j \in \{1,2\}$ fitting in the diagram

$$\begin{tikzcd} \mathfrak{q}_1 \arrow[r, hook] \arrow[d, dash] & \mathfrak{q}_2 \arrow[d, dash] \arrow[r, phantom, "\triangleleft"] & B \arrow[d, dash] \\ \mathfrak{p}_1 \arrow[r, hook] & \mathfrak{p}_2 \arrow[r, phantom, "\triangleleft"] & A \end{tikzcd}$$

Two cases:
- $i=1,\ j=2$: Going up $\longrightarrow$
- $i=2,\ j=1$: Going down $\longleftarrow$

(very different!)

Rem $\exists$ topological interpretation:

Let X be a top space and $p, q \in X$.

We call p a specialization of q and q a generization of p if $p \in \overline{\{q\}}$ closure

Then going up / down for $A \hookrightarrow B$ means:

"Given $\operatorname{Spec} B \to \operatorname{Spec} A$, $\mathfrak{q} \mapsto \mathfrak{p}$, any specialization / generization of $\mathfrak{p}$ lifts to one of $\mathfrak{q}$"

Thm ("Going up") If $A \hookrightarrow B$ is an integral extension, then for any $\mathfrak{p}_1 \hookrightarrow \mathfrak{p}_2$ in Spec A and any $\mathfrak{q}_1 \in \operatorname{Spec} B$ over $\mathfrak{p}_1$, $\exists\, \mathfrak{q}_2 \in \operatorname{Spec} B$ over $\mathfrak{p}_2$ with $\mathfrak{q}_1 \hookrightarrow \mathfrak{q}_2$:

$$\begin{tikzcd} \mathfrak{q}_1 \arrow[r, hook] \arrow[d, dash] & \mathfrak{q}_2 \arrow[d, dash] \\ \mathfrak{p}_1 \arrow[r, hook] & \mathfrak{p}_2 \end{tikzcd}$$

Pf. Consider the integral extension

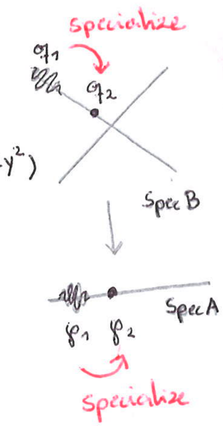
$$\bar{A} := A/\mathfrak{p}_1 \hookrightarrow \bar{B} := B/\mathfrak{q}_1.$$

By "lying over", $\exists\, \bar{\mathfrak{q}}_2 \in \operatorname{Spec} \bar{B}$ over $\bar{\mathfrak{p}}_2 := \mathfrak{p}_2/\mathfrak{p}_1 \in \operatorname{Spec} \bar{A}$

$\Longrightarrow \mathfrak{q}_2 := (\text{preimage of } \bar{\mathfrak{q}}_2) \in \operatorname{Spec} B$ does the job. $\square$

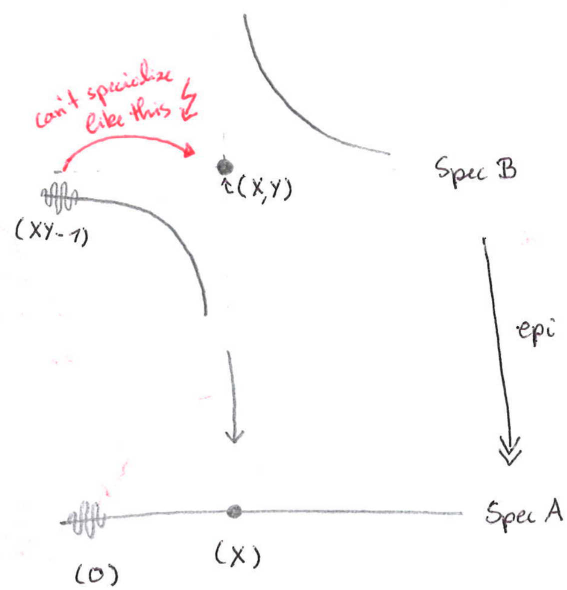
Ex a)

$$\begin{tikzcd} (Y+X) \arrow[d, equal] & (X-c, Y+c) \arrow[d, equal] & \\ \mathfrak{q}_1 \arrow[r, hook] \arrow[d, dash] & \mathfrak{q}_2 \arrow[r, hook] \arrow[d, dash] & B = k[X,Y]/(X^2-Y^2) \arrow[d, dash, "\text{integral}"] \\ \mathfrak{p}_1 \arrow[r, hook] \arrow[d, equal] & \mathfrak{p}_2 \arrow[r, hook] \arrow[d, equal] & A = k[X] \\ (0) & (X-c) & \end{tikzcd}$$



Ex b)

$$\begin{tikzcd}
(XY-1) \arrow[d, phantom, "\shortparallel"] & & \\
\mathfrak{q}_1 \arrow[r, hook] \arrow[d, dash] & ? \arrow[r, hook] \arrow[d, dash] & B = k[X,Y]/(XY-1)\cap(X,Y) \arrow[d, dash, "\text{not integral}"] \\
\mathfrak{p}_1 \arrow[r, hook] \arrow[d, phantom, "\shortparallel"] & \mathfrak{p}_2 \arrow[r, hook] \arrow[d, phantom, "\shortparallel"] & A = k[X] \\
(0) & (X) &
\end{tikzcd}$$



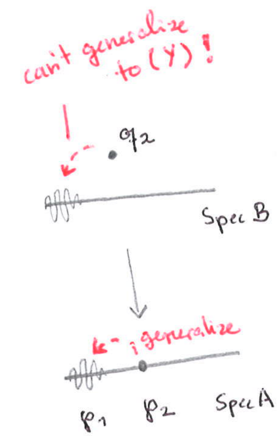
$\Rightarrow$ The only prime ideal over $(X) \in \operatorname{Spec} A$ is $(X,Y) \in \operatorname{Spec} B$ but that one doesn't contain $(XY-1)$.

Thus: Going up says something about "continuity in fibers" under specialization...

For "going down" we need more care:

Ex c) Trivial counterexample:

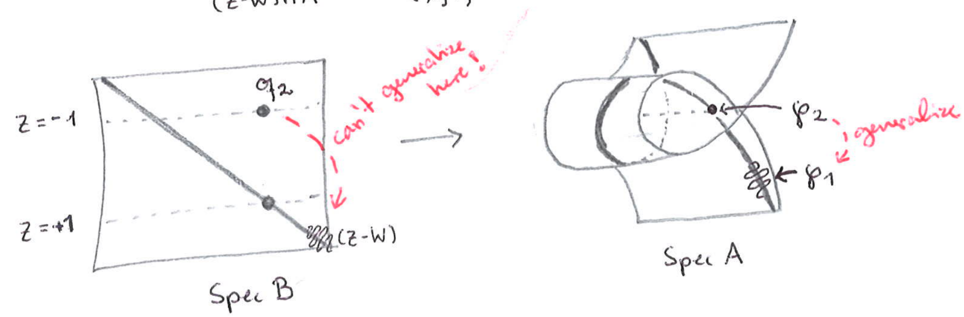
$$\begin{tikzcd}
 & (X,Y-1) \arrow[d, phantom, "\shortparallel"] & \\
? \arrow[r, dash] \arrow[d, dash] & \mathfrak{q}_2 \arrow[r, hook] \arrow[d, dash] & B = k[X,Y]/(Y)\cap(X,Y-1) \arrow[d, dash, "\text{integral}"] \\
\mathfrak{p}_1 \arrow[r, hook] \arrow[d, phantom, "\shortparallel"] & \mathfrak{p}_2 \arrow[r, hook] \arrow[d, phantom, "\shortparallel"] & A = k[X] \\
(0) & (X) &
\end{tikzcd}$$



d) In the previous example Spec B was disconnected.

But even assuming B to be an integral domain won't help:

$$\begin{tikzcd}
 & (Z+1,W-1) \arrow[d, phantom, "\shortparallel"] & \\
? \arrow[r, hook] \arrow[d, dash] & \mathfrak{q}_2 \arrow[r, hook] \arrow[d, dash] & B = k[Z,W] \arrow[d, dash, "\text{integral}"] \\
\mathfrak{p}_1 \arrow[r, hook] \arrow[d, phantom, "\shortparallel"] & \mathfrak{p}_2 \arrow[r, hook] \arrow[d, phantom, "\shortparallel"] & A = k[X,Y,W]/(Y^2-X^2(X+1)) \\
(Z-W)\cap A & (X,Y,W-1) &
\end{tikzcd}$$



<u>Guess</u>: Problem comes from A not being normal. Indeed:

<u>Thm</u> ("Going down") Let $A \hookrightarrow B$ be an integral extension with A normal and B a domain. Then for any $\mathfrak{p}_1 \hookrightarrow \mathfrak{p}_2$ in $\operatorname{Spec} A$ and any $\mathfrak{q}_2 \in \operatorname{Spec} B$ over $\mathfrak{p}_2$, $\exists\, \mathfrak{q}_1 \in \operatorname{Spec} B$ over $\mathfrak{p}_1$ with $\mathfrak{q}_1 \hookrightarrow \mathfrak{q}_2$:

$$\begin{tikzcd}
\mathfrak{q}_1 \arrow[r, hook] \arrow[d, dash] & \mathfrak{q}_2 \arrow[d, dash] \\
\mathfrak{p}_1 \arrow[r, hook] & \mathfrak{p}_2
\end{tikzcd}$$

Pf. ① Main idea: Localize at $S := \{uv \mid u \in A \setminus \mathfrak{p}_1,\ v \in B \setminus \mathfrak{q}_2\}$

$$= (A \setminus \mathfrak{p}_1) \cdot (B \setminus \mathfrak{q}_2)$$

$\downarrow$ get ideals over $\mathfrak{p}_1$ $\qquad$ $\downarrow$ get ideals inside $\mathfrak{q}_2$

$$\begin{tikzcd}
\mathfrak{p}_1 B_S \arrow[d, phantom, "\cap"] & & \\
\exists ?\ \tilde{\mathfrak{q}}_1 \arrow[rr, hook] \arrow[d, dash] & & B_S \arrow[d, dash] \\
\exists ?\ \mathfrak{q}_1 \arrow[r, hook] \arrow[d, dash] & \mathfrak{q}_2 \arrow[r, hook] \arrow[d, dash] & B \arrow[d, dash] \\
\mathfrak{p}_1 \arrow[r, hook] & \mathfrak{p}_2 \arrow[r, hook] & A
\end{tikzcd}$$

$\Longrightarrow$ enough to show $\quad \mathfrak{p}_1 B \cap S = \emptyset$

[Since then $\mathfrak{p}_1 B_S \neq (1)$,
so $\exists\, \tilde{\mathfrak{q}}_1 \in \operatorname{Spec} B_S$ with $\mathfrak{p}_1 B_S \subseteq \tilde{\mathfrak{q}}_1$
and then $\mathfrak{q}_1 := \tilde{\mathfrak{q}}_1 \cap B \in \operatorname{Spec} B$
satisfies $\mathfrak{p}_1 B \subseteq \mathfrak{q}_1$ and $\mathfrak{q}_1 \cap S = \emptyset$,
whence $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$ and $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$.]

② Preliminary reduction:

Assume $\mathfrak{p}_1 B \cap S \neq \emptyset$, say $x \in \mathfrak{p}_1 B \cap S$

$$\Longrightarrow \quad x = \sum_{i=1}^{n} a_i b_i \qquad (a_i \in \mathfrak{p}_1,\ b_i \in S)$$

$$= u \cdot v \qquad (u \in A \setminus \mathfrak{p}_1,\ v \in B \setminus \mathfrak{q}_2).$$

Replace B by $B' := A[v, b_1, \dots, b_n]$,
$\mathfrak{q}_2$ by $\mathfrak{q}_2' := \mathfrak{q}_2 \cap B'$
S by $S' := S \cap B'$

$\Longrightarrow$ Wlog may assume B is fin. gen. as an A-algebra, hence as an A-module (by integrality).

③ Consider minpols : finite field ext^n by ②

Put $K = \mathrm{Quot}(A) \hookrightarrow L = \mathrm{Quot}(B)$,

$$f(Z) := \mathrm{minpol}_K(v)(Z)$$
$$= Z^d + c_1 Z^{d-1} + \dots + c_d \in K[Z]$$

Note: A normal and $v \in L$ integral over A

$\Longrightarrow$ all $c_i \in A$, ie $f \in A[Z]$ (see §2)

On the other hand $u \in K^*$,

so

$$g(Z) := \mathrm{minpol}_K(uv)(Z)$$
$$= u^d \cdot \mathrm{minpol}_K(v)\left(\tfrac{Z}{u}\right)$$
$$= u^d \cdot f\left(\tfrac{Z}{u}\right)$$
$$= Z^d + uc_1 Z^{d-1} + \dots + u^d c_d$$

Note: $A \hookrightarrow B$ finite extension of domains & $uv \in \mathfrak{p}_1 \cdot B$

$\Longrightarrow$ all non-leading coefficients of $g = \mathrm{minpol}_K(uv)$ are $\in \mathfrak{p}_1$

(add-on to §2, see below)

$\Longrightarrow u^i \cdot c_i \in \mathfrak{p}_1 \quad \forall i$

$\Longrightarrow$ all $c_i \in \mathfrak{p}_1$ (since $u \notin \mathfrak{p}_1$ & $\mathfrak{p}_1$ prime)

But then $f(v) = v^d + c_1 v^{d-1} + \dots + c_d = 0$

implies $\quad v^d \in \mathfrak{p}_1 B \subseteq \mathfrak{q}_2$,

whence $\quad v \in \mathfrak{q}_2 \quad ↯$ $\quad \square$

In the proof we've used:

<u>Add-on to §2</u> Let $A \hookrightarrow B$ be a finite extension of domains, where A is normal and $K := \mathrm{Quot}(A)$.

If $\mathfrak{p} \in \mathrm{Spec}\, A$, then for any $x \in \mathfrak{p}B$, writing

$$\mathrm{minpol}_K(x)(Z) = Z^d + a_1 Z^{d-1} + \dots + a_d$$

we have $a_i \in \mathfrak{p}$ for $i = 1, \dots, d$.

Pf. Put $L :=$ normal closure of $\mathrm{Quot}(B)$ in $\overline{K}$ ← algebraic closure

$:= K(\text{all conjugates of elt's of } \mathrm{Quot}(B))$.

Replacing B by the subring of L generated by $\sigma(B)$ $\forall \sigma \in \mathrm{Aut}(L/K)$

we still have $A \hookrightarrow B$ finite

$\Rightarrow$ wlog $\mathrm{Aut}(L/K)$ acts on B (and fixes A)

$\Rightarrow$ $x \in \wp B$ implies $\sigma(x) \in \wp B$ $\forall \sigma \in \mathrm{Aut}(L/K)$

$\Rightarrow$ Writing $\mathrm{minpol}_K(x)(Z) = \prod_{i=1}^{d} (Z - x_i)$ w/ $x_i \in L$, $x_1 = x$,

have $x_i \in \wp B$ $\forall i$

A normal, x integral over A

$\Rightarrow$ all non-leading coeff's of $\mathrm{minpol}_K(x)(Z) \in A[Z]$

are $\in \wp B \cap A = \wp$

since $A \hookrightarrow B$ integral (use lying over ...)

$\square$

4. Noether normalization

Fix a field k

Q Inside $\mathbb{A}_k^{n+1} := \mathrm{Spec}\ k[x_1, \dots, x_{n+1}]$,

consider a hypersurface

$$Y = V(f) \subset \mathbb{A}_k^{n+1} \qquad (f \in k[x_1, \dots, x_{n+1}] \text{ non-constant polynomial})$$

Can we find a coordinate change

$$k[x_1, \dots, x_{n+1}] \simeq k[y_1, \dots, y_{n+1}]$$

s.th. the projection

$$\mathbb{A}_k^{n+1} \xrightarrow{pr} \mathbb{A}_k^n = \mathrm{Spec}\ k[y_1, \dots, y_n]$$
$$(y_1, \dots, y_{n+1}) \longmapsto (y_1, \dots, y_n)$$

restricts to a <u>finite morphism</u> $Y \longrightarrow \mathbb{A}_k^n$

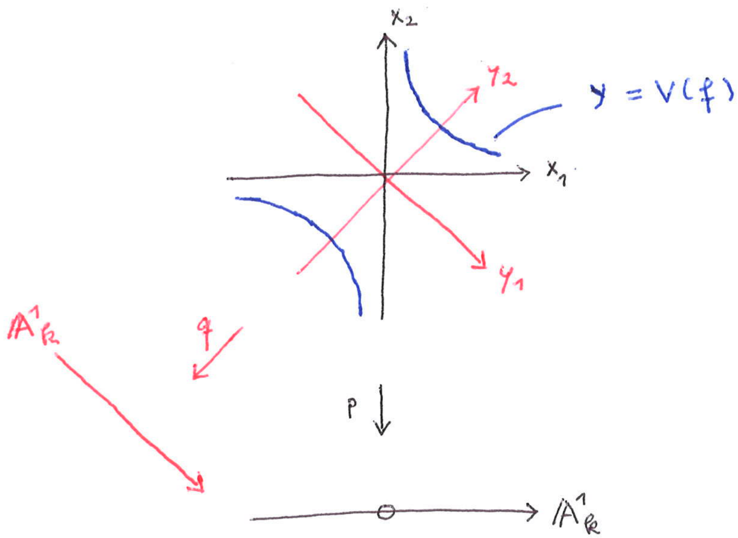
in the sense that the composite

$$k[y_1, \dots, y_n] \hookrightarrow k[x_1, \dots, x_{n+1}] \twoheadrightarrow k[x_1, \dots, x_{n+1}]/(f)$$

is a finite ring extension?

Ex $n = 1$

$f(x_1, x_2) = x_1 x_2 - 1$



$\Rightarrow$ In the coordinates (x_1, x_2), the projection $p : Y \longrightarrow \mathbb{A}^1_k$, $(x_1, x_2) \mapsto x_1$ is not finite.

But in the coordinates (y_1, y_2),

$q : Y \longrightarrow \mathbb{A}^1_k$, $(y_1, y_2) \mapsto y_1$ is finite if char $k \neq 2$:

Write $\begin{array}{l} x_1 = y_2 + y_1 \\ x_2 = y_2 - y_1 \end{array}$ $\Big|$ $\leftarrow$ (coordinate trafo since char $k \neq 2$)

then $f(y_1, y_2) = (y_2 + y_1)(y_2 - y_1) - 1 = \underbrace{y_2^2 - y_1^2 - 1}_{\text{monic eq}^n \text{ for } y_2 \bmod f \text{ over } k[y_1]\,!}$

$\Rightarrow$ $k[y_1, y_2]/(f)$ finite over $k[y_1]$.

Rem For char $k = 2$ this doesn't work but we can instead take the coordinate trafo $\begin{array}{l} x_1 = z_1 + z_2 \\ x_2 = z_2 \end{array}$ that works for all k (exercise).

Expect that for arbitrary $V(f) \subset \mathbb{A}^{n+1}_k$, a "sufficiently general" coordinate change will make $p : V(f) \to \mathbb{A}^n_k$ finite.

Indeed as in previous remark:

Exercise Assume k is an infinite field. Then for any $f \in k[x_1, \dots, x_{n+1}] \setminus k$, $\exists\, c_1, \dots, c_n \in k$ sth for the new coordinates

$$\begin{cases} y_1 := x_1 - c_1 x_{n+1} \\ \vdots \\ y_n := x_n - c_n x_{n+1} \\ y_{n+1} := x_{n+1} \end{cases}$$

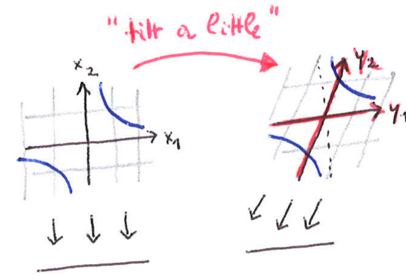
the eq^n $f(y_1 + c_1 y_{n+1}, \dots, y_n + c_n y_{n+1}, y_{n+1}) = 0$ is monic, hence

$V(f) \longrightarrow \mathbb{A}^n_k$

$(y_1, \dots, y_{n+1}) \mapsto (y_1, \dots, y_n)$

is a finite morphism.

(ie $k[y_1, \dots, y_n] \hookrightarrow k[x_1, \dots, x_{n+1}]/(f)$ finite ring extension)

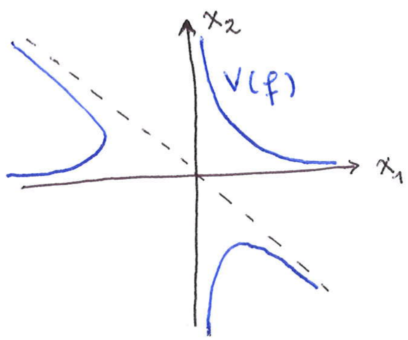


Caution If k is finite this may fail:

eg let $k = \mathbb{F}_2$,

$n = 1$,

$f = x_1 x_2 (x_1 + x_2) - 1$:



Over $\mathbb{F}_2$ we have only 3 linear forms in (x_1, x_2):

$y_1 = x_1$ or $y_1 = x_2$ or $y_1 = x_1 + x_2$

In the above real picture all three corresponding lines $\{y_1 = 0\}$ are asymptotes to $V(f)$.

And indeed: The extension

$k[y_1] \hookrightarrow k[x_1, x_2]/(f)$ is integral for none of them!

(exercise)

But a slightly more general coordinate trafo (nonlinear) will work also over finite fields:

Prop Let k be an arbitrary field & $B = k[b_1, \dots, b_{n+1}]$ a fingen k-algebra.

Assume $\exists f \in k[x_1, \dots, x_{n+1}] \setminus \{0\}$ w/ $f(b_1, \dots, b_{n+1}) = 0$.

$\Longrightarrow \exists a_1, \dots, a_n \in B$

sth
- b_{n+1} is integral over $A := k[a_1, \dots, a_n]$
- $B = A[b_{n+1}]$.

Pf. (Nagata 1950's)

Ansatz: $a_i := b_i - b_{n+1}^{r_i}$ with $r_i \in \mathbb{N}$

(our previous tilt would have $r_i = 1$).

Correspondingly, define $g \in k[y_1, \dots, y_{n+1}] \setminus \{0\}$

by

$$g(y_1, \dots, y_{n+1}) := f(y_1 + y_{n+1}^{r_1}, \dots, y_n + y_{n+1}^{r_n}, y_{n+1}),$$

so that $\boxed{g(a_1, \dots, a_n, b_{n+1}) = 0.}$

Goal: Choose the r_i so that $g \in (k[y_1, \dots, y_n])[y_{n+1}]$ has leading coefficient $\in k$

$\hookrightarrow$ (as polynomial in y_{n+1})

Using multiindex notation,

put $f = \sum_{\underline{m}} c_{\underline{m}} \cdot \prod_{i=1}^{n+1} x_i^{m_i}$ w/ $\underline{m} = (m_1, \dots, m_{n+1})$, $c_{\underline{m}} \in k$

$$\Rightarrow \quad g = \sum_{\underline{m}} \underbrace{c_{\underline{m}}}_{\in k} \cdot \underbrace{\prod_{i=1}^{n} (y_i + y_{n+1}^{r_i})^{m_i} \cdot y_{n+1}^{m_{n+1}}}$$

leading term wrt y_{n+1} is $= y_{n+1}^{\underline{r}\cdot\underline{m}}$, $\underline{r}\cdot\underline{m} := \sum_{i=1}^{n+1} r_i m_i$.

$\Rightarrow$ Enough to show:

(*) Given any finite collection of multiindices $\mathcal{M} \subset \mathbb{N}_0^{n+1}$
$\exists\, \underline{r} = (r_1, \dots, r_{n+1}) \in \mathbb{N}^{n+1}$ with $r_{n+1} = 1$
sth
$$\delta : \mathcal{M} \longrightarrow \mathbb{N}, \quad \underline{m} \longmapsto \underline{r}\cdot\underline{m}$$
is injective

Indeed then the leading term of g wrt y_{n+1} will be $\underbrace{c_{\underline{m}}}_{\in k^*} \cdot y_{n+1}^{\underline{r}\cdot\underline{m}}$ for the unique $\underline{m}$ with $\delta(\underline{m})$ maximal.

Pf of (*) works by induction:

$n = 0$ trivial.

$n-1 \to n$:

By induction $\exists\, \underline{r}' = (r_2, \dots, r_{n+1} = 1)$

w/ $\delta' : \mathcal{M}' := \{ \underline{m}' := (m_2, \dots, m_{n+1}) \mid \underline{m} \in \mathcal{M} \} \longrightarrow \mathbb{N}_0$, $\underline{m}' \longmapsto \underline{r}'\cdot\underline{m}'$

injective.

Then take $r_1 > \max\{ \delta(\underline{m}') \mid \underline{m}' \in \mathcal{M}' \}$.

$\Rightarrow \underline{r} := (r_1, r_2, \dots, r_{n+1})$ works. $\square$

Let's reformulate this in a convenient way:

<u>Def</u> For a k-algebra B, elements $a_1, \dots, a_n \in B$ are called <u>algebraically independent</u> (over the field k) if the natural homomorphism $k[x_1, \dots, x_n] \longrightarrow k[a_1, \dots, a_n]$ is an isomorphism.

abstract polynomial ring

subalgebra of B

Thm ("Noether normalization") For any fin.gen. k-algebra B, $\exists$ alg. independent $a_1, \dots, a_n \in B$ (some $n \in \mathbb{N}_0$) sth

$$A := k[a_1, \dots, a_n] \hookrightarrow B$$

is a finite extension.

(ie. $\operatorname{Spec}(B) \xrightarrow{\exists} \mathbb{A}^n_k$ finite morphism).

Pf. Let $B = k[b_1, \dots, b_m]$ with $b_i \in B$, $m \in \mathbb{N}$.

$m = 0$: Trivial (take $n := 0$).

$m-1 \to m$: If $b_1, \dots, b_m$ are alg. independent, we're done (take $n := m$ & $a_i := b_i$).

So wlog $\exists f \in k[x_1, \dots, x_m] \setminus \{0\}$ w/ $f(b_1, \dots, b_m) = 0$.

Prop $\Rightarrow \exists \tilde{a}_1, \dots, \tilde{a}_{m-1} \in B$

w/ • b_m integral over $\tilde{A} := k[\tilde{a}_1, \dots, \tilde{a}_{m-1}]$

• $B = \tilde{A}[b_m]$

By induction $\exists a_1, \dots, a_n \in \tilde{A}$ w/ $k[a_1, \dots, a_n] \hookrightarrow \tilde{A}$ finite

$\Rightarrow$ claim. $\square$

5. Hilbert's Nullstellensatz

Recall our geometry $\leftrightarrow$ algebra dictionary:

$$\left\{ \begin{array}{c} \text{Zariski closed} \\ \text{subsets } V \subset \operatorname{Spec} R \end{array} \right\} \overset{1:1}{\longleftrightarrow} \left\{ \begin{array}{c} \text{radical ideals} \\ \mathfrak{a} \trianglelefteq R \end{array} \right\}$$

$$V \longmapsto \mathcal{J}(V) := \bigcap_{\mathfrak{p} \in V} \mathfrak{p}$$

$$V(\mathfrak{a}) := \{\mathfrak{p} \mid \mathfrak{a} \subseteq \mathfrak{p}\} \longleftarrow \mathfrak{a}$$

(see § I.5)

Goal: If $R = k[x_1, \dots, x_n]$ w/ k algebraically closed, then

a) $k^n \simeq \operatorname{Spm} R$ via $\underline{a} \mapsto \mathfrak{m}_{\underline{a}} := (x_1 - a_1, \dots, x_n - a_n)$

b) above correspondence works more naively w/ $\operatorname{Spm} R$ in place of $\operatorname{Spec} R$

$V(\mathfrak{a}) := \{\underline{a} \in k^n \mid f(\underline{a}) = 0 \ \forall f \in \mathfrak{a}\}$,

$\mathcal{J}(V) := \{f \in R \mid f(\underline{a}) = 0 \ \forall \underline{a} \in V\}$.

Main point is Noether normalization:

Thm (Nullstellensatz, version 1) Let k be any field.
If K/k is a field extension which is fin gen. as a k-algebra, then it is finite: $[K:k] < \infty$.
($\Rightarrow K = k$ in case k is alg closed)

Pf. Noether normalization $\Rightarrow$ K is finite over a polynomial ring $k[x_1,\dots,x_n]$, $n \in \mathbb{N}_0$

So $k[x_1,\dots,x_n] \hookrightarrow K$ integral
But K is a field $\Rightarrow$ $k[x_1,\dots,x_n]$ is a field
(see remark after "lying over" in §3)

$\Rightarrow n = 0$, ie. $k \hookrightarrow K$ is finite $\square$

Cor (Nullstellensatz, version 2) For k alg. closed,

(Goal a) from above)

$$\mathrm{Spm}\, k[x_1,\dots,x_n] = \{ m_{\underline{a}} \mid \underline{a} \in k^n \}$$

where $m_{\underline{a}} := (X_1 - a_1, \dots, X_n - a_n)$.

Pf. $\wp \trianglelefteq R := k[x_1,\dots,x_n]$ maximal

$\Rightarrow R/\wp$ a field & fin gen k-algebra

$\Rightarrow k \xrightarrow[\varphi]{\sim} R/\wp$ iso by previous thm

Put $a_i := \varphi^{-1}(x_i \bmod \wp)$

$\Rightarrow x_i - a_i \in \wp \;\forall i$

$\Rightarrow m_{\underline{a}} \subseteq \wp$, hence "=" since $m_{\underline{a}}$ is maximal. $\square$

Cor (Nullstellensatz, version 3) Let k be alg closed,
$J \trianglelefteq k[x_1,\dots,x_n]$,
$V := \{ \underline{a} \in k^n \mid f(\underline{a}) = 0 \;\forall f \in J \}$
a Zariski closed subset of k^n.

(Goal a) for any fin gen k-algebra R)

$\Rightarrow \exists$ bijection
$$V \xrightarrow{\sim} \mathrm{Spm}(R), \quad R := \frac{k[x_1,\dots,x_n]}{J}$$
$$\underline{a} \longmapsto (m_{\underline{a}} \bmod J)$$

Pf. $\mathrm{Spm}\, R \cong \{ m \in \mathrm{Spm}\, k[x_1,\dots,x_n] \mid J \subseteq m \}$

$\overset{\text{(Nullstellensatz version 2)}}{\cong} \{ \underline{a} \in k^n \mid J \subseteq m_{\underline{a}} \} \overset{(*)}{=} V$

(*) see overleaf

For (*) note: "$\subseteq$" obvious

"$\supseteq$": $\underline{a} \in V \Rightarrow \underset{\overset{\cup|}{J}}{J(V)} \subseteq \underset{\overset{||}{m_{\underline{a}}}}{J(\underline{a})} \Rightarrow J \subseteq m_{\underline{a}}$. $\square$

Rem. In particular, for k alg closed & $\mathfrak{a} \subsetneqq k[x_1, .., x_n]$,

one has $V(\mathfrak{a}) \neq \emptyset$.

(For k non-closed this fails, think of $\mathfrak{a} = (x^2+1) \subsetneqq \mathbb{R}[x] ...$)

Cor (Nullstellensatz, version 4) Let k be a field.

$\Rightarrow$ any fingen k-algebra R is Jacobson,

ie. $\underset{\overset{\cdot\cdot}{||}}{\sqrt{\mathfrak{a}}} = \underset{\overset{\cdot\cdot}{||}}{\mathrm{Jac}(\mathfrak{a})} \quad \forall \mathfrak{a} \trianglelefteq R$.

$\bigcap_{\substack{\mathfrak{p} \supseteq \mathfrak{a} \\ \text{prime}}} \mathfrak{p} \qquad \bigcap_{\substack{m \supseteq \mathfrak{a} \\ \text{maximal}}} m$

Pf. "$\subseteq$" obvious.

"$\supseteq$": Let $f \in R \setminus \sqrt{\mathfrak{a}}$. Want to find $m \supseteq \mathfrak{a}$ maximal w/ $f \notin m$.

$f \notin \sqrt{\mathfrak{a}} \Rightarrow f^n \notin \mathfrak{a} \ \forall n \in \mathbb{N} \Rightarrow \mathfrak{a} \cdot R_f \neq (1) \Rightarrow \exists\, m \in \mathrm{Spec}\, R$
w/ $\mathfrak{a} \subseteq m$

and $m R_f \in \mathrm{Spm}\, R_f$.

Claim: This $m \trianglelefteq R$ must be maximal.

Indeed:

$$k \hookrightarrow R/m \hookrightarrow (R/m)_f \simeq R_f / m R_f$$

this is
- a field since $m R_f \in \mathrm{Spm}(R_f)$
- a fingen. k-algebra since it is generated by $1/f$ & generators of R

$\Rightarrow \dim_k R_f / m R_f < \infty$

(Nullstellensatz, version 1)

Thus

$k \hookrightarrow R_f / m R_f$ finite

$\Rightarrow k \hookrightarrow R/m$ finite

But k is a field

& R/m a domain

$\Longrightarrow R/m$ is a field

$\Longrightarrow m \in \mathrm{Spm}\, R$ maximal. $\square$

Cor (Nullstellensatz, version 5) (Goals a) and b) for any fingen k-algebra R)

Let $J \trianglelefteq k[x_1,\dots,x_n]$ w/ k alg. closed,

and $R := k[x_1,\dots,x_n]/J$

$V := V(J) := \{\underline{a} \in k^n \mid f(\underline{a}) = 0 \ \forall f \in J\}$.

$\Rightarrow$ $\exists$ bijection

$$\left\{\begin{array}{c}\text{Zariski closed} \\ \text{subsets } W \subseteq V\end{array}\right\} \overset{1:1}{\longleftrightarrow} \left\{\begin{array}{c}\text{radical ideals} \\ \mathfrak{a} \trianglelefteq R\end{array}\right\}$$

$$W \longmapsto J(W) := \{f \bmod J \mid f(\underline{a}) = 0 \ \forall f \in W\}$$

$$V(\mathfrak{a}) := \{\underline{a} \in k^n \mid f(\underline{a}) = 0 \ \forall (f \bmod J) \in \mathfrak{a}\} \longleftarrow \mathfrak{a}$$

Pf.
- $J(W)$ always radical because defined "pointwise"
- $V(\tilde{\mathfrak{a}}) \subseteq W$ for $\tilde{\mathfrak{a}} \supseteq J$ because $V = V(J)$
- $W = V(J(W))$ always (see chapter 0, p. 2)

Main point: $J(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$ $\forall \mathfrak{a} \trianglelefteq R$.

"$\supseteq$": $f \in \sqrt{\mathfrak{a}} \Rightarrow \exists n \in \mathbb{N}: f^n \in \mathfrak{a}$

(always)

$\Rightarrow \forall \underline{a} \in V(\mathfrak{a}): f(\underline{a})^n = 0$

i.e. $f(\underline{a}) = 0$

$\Rightarrow f \in J(V(\mathfrak{a}))$

"$\subseteq$": $f \notin \sqrt{\mathfrak{a}} \Rightarrow$ By Nullstellensatz, version 4

(k alg. closed)

$\exists \mathfrak{m} \in \operatorname{Spm}(R)$

w/
- $\mathfrak{a} \subseteq \mathfrak{m}$
- $f \notin \mathfrak{m}$

Nullstellensatz, version 3: $\mathfrak{m} = \mathfrak{m}_{\underline{a}} \bmod J$

for some $\underline{a} \in V$

$\Rightarrow$ $\mathfrak{a} \subseteq \mathfrak{m}$ implies $\underline{a} \in V(\mathfrak{a})$

$f \notin \mathfrak{m}$ implies $f(\underline{a}) \neq 0$

$\Rightarrow f \notin J(V(\mathfrak{a}))$ $\square$

IV. Dimension

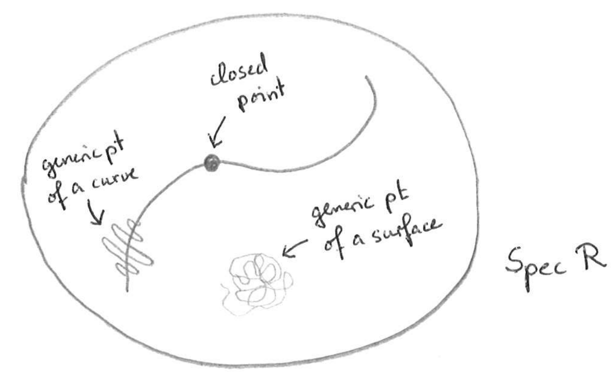
1. Krull dimension

Let R be a ring.

Intuitive idea: Spec R has

- dim $= 0$ if it consists only of closed pt^s
- dim ≥ 1 if it contains "generic pt^s of curves"
  (non-closed pt^s all of whose specializations are closed)
- dim ≥ 2 if it contains "generic pt^s of surfaces"
  (pt^s specializing (only) to generic pt^s of curves & to closed pt^s)

⋮



Ex $R = k[X,Y]$

∇ I

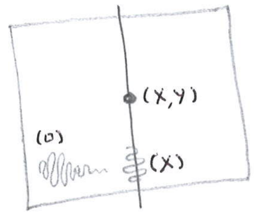
(X,Y) closed pt

$\cup$

(X) generic pt of the Y-axis

$\cup$

(0) generic pt of the plane



Def The <u>Krull dimension</u> (or simply <u>dimension</u>) of R is

$$\dim R := \sup \{ n \in \mathbb{N}_0 \mid \exists \text{ chain of prime ideals } \mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_n \subsetneqq R \}$$

$$= \sup \{ n \in \mathbb{N}_0 \mid \exists \text{ chain of irreducible closed subsets } \operatorname{Spec} R \supsetneqq V_0 \supsetneqq V_1 \supsetneqq \cdots \supsetneqq V_n \neq \emptyset \}$$

$$\in \mathbb{N}_0 \cup \{\infty\}.$$

The <u>codimension</u> (or <u>height</u>) of $\mathfrak{p} \in \operatorname{Spec} R$ is

$$\operatorname{codim} \mathfrak{p} := \operatorname{ht} \mathfrak{p} := \sup \{ n \in \mathbb{N}_0 \mid \exists \text{ chain of prime ideals } \mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_n = \mathfrak{p} \}$$

$$= \dim R_{\mathfrak{p}}.$$

Ex a) $\dim R = 0 \iff$ every prime ideal is maximal,

ie $\operatorname{Spec} R = \operatorname{Spm} R$.

eg. fields, Artin rings (= Noetherian of dim 0)

⚠ In general, $\dim R = 0$ does NOT imply R Noetherian,

e.g. take $R = \prod_{i=1}^{\infty} k_i$ infinite product of fields...

(see §II.5)

b) If R is a domain, then

$\dim R = 1 \iff$ the max. ideals are precisely the prime ideals $\neq (0)$,

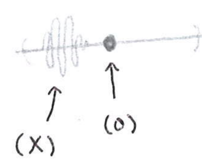
ie $\operatorname{Spec} R = \{(0)\} \sqcup \operatorname{Spm} R$.

eg. every PID R which is not a field has $\dim R = 1$,

in particular $R = \mathbb{Z}$, $k[X]$ (k a field)

but also DVR's such as $R = k[X]_{(X)}$, $\mathbb{Z}_{(p)}$ (p prime)

here $\operatorname{Spec} R = \{(0), (X)\}$ has only two points, but still (0) is the generic pt of a curve...



c) If $R = A[Y]$ where A is a PID but not a field, then we've seen in § I.3 that any $\mathfrak{p} \in \operatorname{Spec} R$ has the form

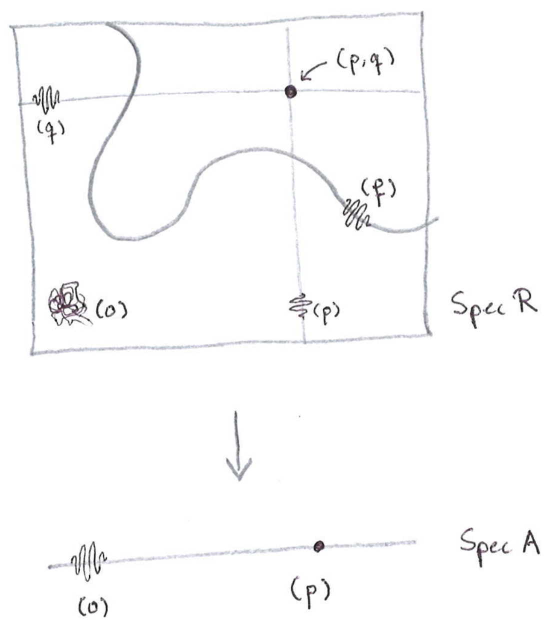
- $\mathfrak{p} = (0)$, or
- $\mathfrak{p} = (f)$ w/ $f \in R$ irreducible, or
- $\mathfrak{p} = (p, q)$ maximal w/ $p \in A$ irreducible, $q \in R$ w/ $\bar{q} \in (A/(p))[Y]$ irreducible.

generic pt of the surface, codim $\mathfrak{p} = 0$

generic pt of a curve, codim $\mathfrak{p} = 1$

closed point, codim $\mathfrak{p} = 2$

$\Longrightarrow \dim R = 2$



eg. $\dim k[X,Y] = 2$
$\dim \mathbb{Z}[Y] = 2$
$\vdots$

d) $R = k[X_n \mid n \in \mathbb{N}]$ has $\dim R = \infty$,

indeed $(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq (X_1, X_2, X_3) \subsetneq \cdots$

is a strictly ascending infinite chain of prime ideals.

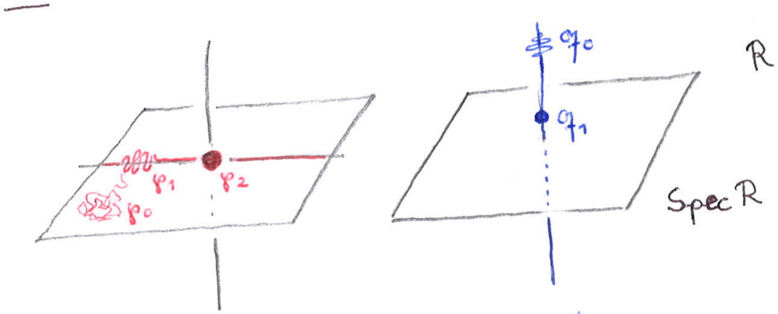
⚠ $\exists$ examples where R is Noetherian but $\dim R = \infty$ (Nagata 1962, see later)

2. Equidimensional rings

Def A chain $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n \trianglelefteq R$ of primes is maximal if it cannot be refined to a longer chain of primes.

Rem Maximal chains can have different length:

$R = \dfrac{k[X,Y,Z]}{(XZ, YZ)}$



$\mathfrak{p}_0 \overset{\neq}{\hookrightarrow} \mathfrak{p}_1 \overset{\neq}{\hookrightarrow} \mathfrak{p}_2$, with $\mathfrak{p}_0 = (z)$, $\mathfrak{p}_1 = (y,z)$, $\mathfrak{p}_2 = (x,y,z)$

$\mathfrak{q}_0 \overset{\neq}{\hookrightarrow} \mathfrak{q}_1$, with $\mathfrak{q}_0 = (x,y)$, $\mathfrak{q}_1 = (x,y,z-c)$ (any $c \in k$)

In general we only have:

Lemma a) Dimension is a "local notion":

$$\dim R = \sup\{\dim R_{\mathfrak{p}} \mid \mathfrak{p} \in \operatorname{Spm} R\}$$
$$= \sup\{\operatorname{codim} \mathfrak{p} \mid \mathfrak{p} \in \operatorname{Spm} R\}$$

("maximal codim of a closed pt")

b) For any $\mathfrak{p} \in \operatorname{Spec} R$,

$$\dim R \gneqq \dim R/\mathfrak{p} + \operatorname{codim} \mathfrak{p}.$$

Pf. a) Given a chain $\mathfrak{p}_0 \overset{\neq}{\hookrightarrow} \cdots \overset{\neq}{\hookrightarrow} \mathfrak{p}_n = \mathfrak{p}$ in $\operatorname{Spec} R$

we get a chain $\mathfrak{p}_0 R_{\mathfrak{p}} \overset{\neq}{\hookrightarrow} \cdots \overset{\neq}{\hookrightarrow} \mathfrak{p}_n R_{\mathfrak{p}}$ in $\operatorname{Spec} R_{\mathfrak{p}}$

& conversely.

b) Pick chains

$\mathfrak{p}_0 \overset{\neq}{\hookrightarrow} \cdots \overset{\neq}{\hookrightarrow} \mathfrak{p}_c = \mathfrak{p}$ w/ $c := \operatorname{codim} \mathfrak{p}$ (if $< \infty$)

$(0) = \mathfrak{q}_0 \overset{\neq}{\hookrightarrow} \cdots \overset{\neq}{\hookrightarrow} \mathfrak{q}_d \trianglelefteq R/\mathfrak{p}$ w/ $d := \dim R/\mathfrak{p}$ (if $< \infty$)

Put $\mathfrak{p}_{c+i} := (\text{preimage of } \mathfrak{q}_i) \in \operatorname{Spec} R$

$\Rightarrow$ get $\mathfrak{p}_0 \overset{\neq}{\hookrightarrow} \cdots \overset{\neq}{\hookrightarrow} \mathfrak{p}_{c+d}$ in $\operatorname{Spec} R \Rightarrow \dim R \geq c+d$. $\square$

Ex In the previous example $R = k[X,Y,Z]/(XZ,YZ)$, we have

$$\dim R = 2 > 1 = \underbrace{\dim R/\mathfrak{p}}_{=\begin{cases}1\\0\end{cases}} + \underbrace{\operatorname{codim} \mathfrak{p}}_{=\begin{cases}0\\1\end{cases}}$$

for $\mathfrak{p} := \begin{cases} (x,y) \\ (x,y,z-c) \text{ with } c \neq 0. \end{cases}$

Ex $R := A_S$ where $A := k[X,Y]$ & $S := A \setminus (\mathfrak{m} \cup \mathfrak{p})$. Here R is even a domain!

maximal, codim = 2

prime, codim = 1

Def A ring R is <u>biequidimensional</u> if all maximal chains of primes $\mathfrak{p}_0 \overset{\neq}{\hookrightarrow} \cdots \overset{\neq}{\hookrightarrow} \mathfrak{p}_n \trianglelefteq R$ have the same length n. Then in particular

a) R is <u>equidimensional</u>,

ie all minimal primes $\mathfrak{p} \in \operatorname{Spec} R$ have the same $\dim R/\mathfrak{p}$

($\hat{=}$ "all irreducible cpt^s of $\operatorname{Spec} R$ have the same dim")

b) R is <u>equicodimensional</u>,

ie all maximal ideals $\mathfrak{m} \in \operatorname{Spm} R$ have the same codim $\mathfrak{m}$

($\hat{=}$ "all closed pt^s of $\operatorname{Spec} R$ have the same codim")

c) R is <u>catenary</u>,

ie $\forall$ fixed primes $\mathfrak{p} \subseteq \mathfrak{q} \trianglelefteq R$,

all maximal chains of primes between $\mathfrak{p}$ and $\mathfrak{q}$ have the same length.

Caution: a), b), c) $\not\Longrightarrow$ biequidimensional (see later)
(this is wrong even in EGA IV)

Prop Let R be biequidimensional with $\dim R < \infty$.
For any $\mathfrak{p} \in \operatorname{Spec} R$ we have:

a) $R/\mathfrak{p}$ and $R_\mathfrak{p}$ are biequidim,

b) $\dim R = \dim R/\mathfrak{p} + \operatorname{codim} \mathfrak{p}$.

("Dimension formula")

Pf. $\dim R < \infty \Rightarrow \dim R/\mathfrak{p} < \infty$

Pick a max. chain $(0) = \mathfrak{q}_0 \overset{\neq}{\hookrightarrow} \cdots \overset{\neq}{\hookrightarrow} \mathfrak{q}_d$ in $\operatorname{Spec} R/\mathfrak{p}$

(i.e. $\nexists$ no refinement, but a priori d, e needn't be max.) (so $d \leq \dim R/\mathfrak{p}$),

and a max. chain $\mathfrak{p}_0 \overset{\neq}{\hookrightarrow} \cdots \overset{\neq}{\hookrightarrow} \mathfrak{p}_c := \mathfrak{p}$ of primes $\subseteq \mathfrak{p}$,
(so $c \leq \operatorname{codim} \mathfrak{p}$)

$\Rightarrow$ max. chain $\mathfrak{p}_0 \overset{\neq}{\hookrightarrow} \cdots \overset{\neq}{\hookrightarrow} \mathfrak{p}_{c+d}$ in $\operatorname{Spec} R$

where $\mathfrak{p}_{c+i} := (\text{preimage of } \mathfrak{q}_i) \trianglelefteq R$.

R biequidim; previous lemma

$$\Longrightarrow \quad \dim R = c + d \leq \dim R/\mathfrak{p} + \operatorname{codim} \mathfrak{p} \leq \dim R$$

$\Rightarrow$ equality holds & a), b) follow. $\square$

Appendix: Some weird examples

Ex. 1 (Katharina Heinrich 2014)

$\exists$ Noetherian ring R of $\dim R = 2$
which is equidim, equicodim, catenary,
but NOT biequidim:

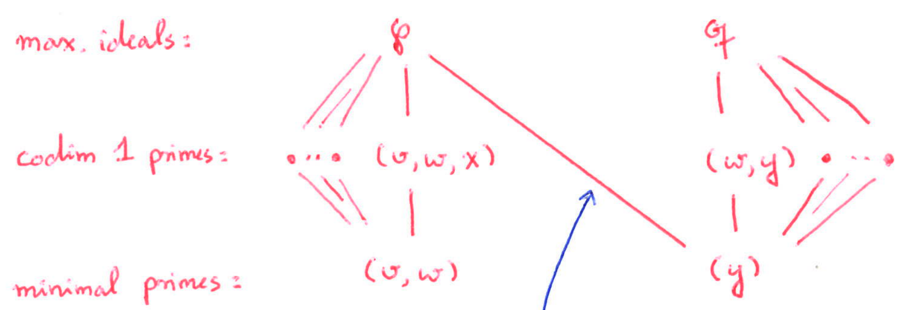
e.g. let $R := A_S$ w/ $A := k[v,w,x,y]/(vy, wy)$

$S := A \setminus (\mathfrak{p} \cup \mathfrak{q})$

$\mathfrak{p} := (v, w, x, y-1)$

$\mathfrak{q} := (v, w, y)$

$\Longrightarrow$ Spec R looks as follows:



this is a maximal chain of length $1 < 2 = \dim R$!

(exercise)

Ex. 2 (Nagata 1962)

$\exists$ Noetherian ring R w/ $\dim R = \infty$:

e.g. $R := A_S$

w/ $A := k[X_n \mid n \in \mathbb{N}]$

$S := A \setminus \bigcup_{i=1}^{\infty} \mathfrak{p}_i$

$\mathfrak{p}_i := (X_{n_i+1}, X_{n_i+2}, \dots, X_{n_{i+1}}) \trianglelefteq A$

for a sequence $0 = n_1 < n_2 < n_3 < \cdots$ in $\mathbb{N}$

$\Longrightarrow$ $\operatorname{Spm} R = \{ \mathfrak{p}_i \cdot R \mid i \in \mathbb{N} \}$

$\Longrightarrow$ $\dim R = \sup \{ n_{i+1} - n_i \mid i \in \mathbb{N} \} = \infty$

for suitable $n_1, n_2, \dots$

but one may show that R is Noetherian

(Key point: Any $a \in R$ lies in at most finitely many $\mathfrak{m} \in \operatorname{Spm} R$, & for all $\mathfrak{m} \in \operatorname{Spm} R$ the localization $R_\mathfrak{m}$ is Noetherian ...)

3. Dimension of affine varieties

Q: What's the dimension of $\mathbb{A}^n_k = \operatorname{Spec} k[x_1, \dots, x_n]$,

or more generally $\dim R$ for a fingen k-algebra R?

Idea: Use Noether normalization ...

Prop If $A \hookrightarrow B$ is an integral ring extension, then

$$\dim B = \dim A.$$

Pf.

"$\geq$": $\mathfrak{p}_0 \overset{\neq}{\hookrightarrow} \cdots \overset{\neq}{\hookrightarrow} \mathfrak{p}_n$ chain in $\operatorname{Spec} A$

$\Longrightarrow$ by "lying over" $\exists\, \mathfrak{q}_0 \in \operatorname{Spec} B$ w/ $\mathfrak{q}_0 \cap A = \mathfrak{p}$

$\Longrightarrow$ by "going up" we can extend this to a chain $\mathfrak{q}_0 \hookrightarrow \cdots \hookrightarrow \mathfrak{q}_n$ in $\operatorname{Spec} B$

w/ $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ $\forall i$ (in particular $\mathfrak{q}_i \overset{\neq}{\hookrightarrow} \mathfrak{q}_{i+1}$ are strict inclusions)

$\Longrightarrow$ $\dim B \geq \dim A$

"$\le$": If $\mathfrak{q}_0 \overset{\neq}{\hookrightarrow} \cdots \overset{\neq}{\hookrightarrow} \mathfrak{q}_n$ is a chain in $\operatorname{Spec} B$,

we get a chain $\mathfrak{p}_0 \hookrightarrow \cdots \hookrightarrow \mathfrak{p}_n$ in $\operatorname{Spec} A$

via $\mathfrak{p}_i := \mathfrak{q}_i \cap A$.

Incomparability $\Rightarrow$ $\mathfrak{p}_i \overset{\neq}{\hookrightarrow} \mathfrak{p}_{i+1}$ strict inclusion $\forall i$

$\Rightarrow$ $\dim B \le \dim A$. $\square$

By Noether normalization this reduces us to:

Thm Let $R = k[x_1, \dots, x_n]$ w/ a field k & $n \in \mathbb{N}_0$.

Then

a) R is biequidimensional

(ie all max. chains of primes have same length)

b) $\dim R = n$

(as expected, since $\operatorname{Spec} R = \mathbb{A}^n_k \dots$)

Pf. By induction on n.

$n = 0$: trivial (in fact $n = 1$ also known by ex. 1.b

$n = 2$ —"— 1.c)

Assume claim holds for $n-1$ in place of n.

Clearly $\dim R \geq n$,

as the chain $(0) \overset{\neq}{\hookrightarrow} (X_1) \overset{\neq}{\hookrightarrow} (X_1, X_2) \overset{\neq}{\hookrightarrow} \cdots \overset{\neq}{\hookrightarrow} (X_1, \dots, X_n)$

shows.

Want:

For any other chain $\mathfrak{p}_0 \overset{\neq}{\hookrightarrow} \cdots \overset{\neq}{\hookrightarrow} \mathfrak{p}_m$ in $\operatorname{Spec} R$

one has

- $m \le n$ ($\Rightarrow$ b))
- for maximal chains $m = n$ ($\Rightarrow$ a))

Wlog $\mathfrak{p}_0 = (0)$ (else extend the chain)

and $\mathfrak{p}_1 = (f)$ for some irreducible $f \in R$

(use that R is a UFD:

pick any $g \in \mathfrak{p}_1$, write $g = g_1 \cdots g_s$ w/ irreducible $g_i \in R$,

then $\exists i$ sth $f := g_i \in \mathfrak{p}_1$,

hence $(f) \subseteq \mathfrak{p}_1$ & $(f) \in \operatorname{Spec} R$ by irreducibility

$\Rightarrow$ after refinement of the chain may assume $\mathfrak{p}_1 = (f)$).

Coordinate change ("generalized tilt") $\quad x_i \mapsto x_i + x_n^{r_i} \quad (i<n)$

$$x_n \mapsto x_n$$

as in Noether normalization (proposition from §3.4)

$\Rightarrow$ wlog $f(x_1,\dots,x_n)$ is monic in x_n

(up to a scalar $\in k^*$ that doesn't affect (f))

$\Rightarrow$ $k[x_1,\dots,x_{n-1}] \longrightarrow R/(f)$ integral extension

Consider then

$$\begin{tikzcd} & R = k[x_1,\dots,x_n] \arrow[d, two heads, "\pi \;\; \text{epi}"] \\ k[x_1,\dots,x_{n-1}] \arrow[r, hook, "i"', "\text{integral}" below] & k[x_1,\dots,x_n]/\mathfrak{p}_1, \quad \mathfrak{p}_1 = (f). \end{tikzcd}$$

Note: Putting $\mathfrak{q}_i := \pi(\mathfrak{p}_{i+1})$ we get a chain

$$\mathfrak{q}_0 \overset{\neq}{\hookrightarrow} \mathfrak{q}_1 \overset{\neq}{\hookrightarrow} \dots \overset{\neq}{\hookrightarrow} \mathfrak{q}_{m-1} \quad \text{in } \operatorname{Spec} R/\mathfrak{p}_1$$

$$\Rightarrow \quad m-1 \leq \dim R/\mathfrak{p}_1 \underset{\substack{\uparrow \\ \text{previous proposition} \\ \text{using that } i \text{ is integral}}}{=} \dim k[x_1,\dots,x_{n-1}] \underset{\substack{\uparrow \\ \text{induction} \\ \text{on } n}}{=} n-1$$

$\Rightarrow$ $m \leq n$

$\Rightarrow$ $\dim R = n$ as claimed in b).

For biequidimensionality in a) we need more work:

Assume $\mathfrak{p}_0 \overset{\neq}{\hookrightarrow} \dots \overset{\neq}{\hookrightarrow} \mathfrak{p}_m$ is a maximal chain in $\operatorname{Spec} R$.

$\Rightarrow$ $\mathfrak{q}_0 \overset{\neq}{\hookrightarrow} \dots \overset{\neq}{\hookrightarrow} \mathfrak{q}_{m-1}$ is a maximal chain in $\operatorname{Spec} R/\mathfrak{p}_1$ (obvious)

We get a chain

$$i^{-1}\mathfrak{q}_0 \overset{\neq}{\hookrightarrow} \dots \overset{\neq}{\hookrightarrow} i^{-1}\mathfrak{q}_{m-1} \quad \text{in } \operatorname{Spec} k[x_1,\dots,x_{n-1}],$$

w/ strict inclusions by incomparability.

Fact: This chain is maximal ! (use exercise below)

$\Rightarrow$ By induction we get $m-1 = n-1$,

hence $m = n$ as claimed in a).

$\square$

Here we've used:

<u>Exercise</u> Let $A \hookrightarrow B$ be an integral extension w/ A a fingen. $\Bbbk$-algebra.

Suppose we have primes
$$\begin{array}{ccccc} \mathfrak{q} & \hookrightarrow & \mathfrak{q}'' & \trianglelefteq & B \\ | & & | & & | \\ \mathfrak{p} & \hookrightarrow & \mathfrak{p}'' & \trianglelefteq & A \end{array}$$

If $\exists \mathfrak{p}' \in \operatorname{Spec} A$ w/ $\mathfrak{p} \overset{\neq}{\hookrightarrow} \mathfrak{p}' \overset{\neq}{\hookrightarrow} \mathfrak{p}''$

then $\exists \mathfrak{q}' \in \operatorname{Spec} B$ w/ $\mathfrak{q} \overset{\neq}{\hookrightarrow} \mathfrak{q}' \overset{\neq}{\hookrightarrow} \mathfrak{q}''$.

(Hint: Consider the integral extension $A/\mathfrak{p} \hookrightarrow B/\mathfrak{q}$ & try "going down". Caution: $A/\mathfrak{p}$ needn't be normal, so use Noether normalization first:

$$\Bbbk[x_1,\dots,x_m] \hookrightarrow A/\mathfrak{p} \hookrightarrow B/\mathfrak{q} \quad \text{integral} \;)$$

⚠ We <u>only</u> claim $\mathfrak{q} \overset{\neq}{\hookrightarrow} \mathfrak{q}' \overset{\neq}{\hookrightarrow} \mathfrak{q}''$, in general you <u>won't</u> find $\mathfrak{q}'$ lying above $\mathfrak{p}'$.

Do you see why?

From the thm we get:

<u>Cor</u> Let R be a domain & a fingen. $\Bbbk$-algebra. Then

a) R is biequidim.

b) $\forall$ Noether normalization $\Bbbk[x_1,\dots,x_n] \hookrightarrow R$ we have
$$\dim R = n.$$

(In particular n doesn't depend on the chosen Noether normalization).

Pf. a) Write $R = \underbrace{\Bbbk[y_1,\dots,y_m]}_{\substack{\text{biequidim} \\ \text{by thm}}}/\mathfrak{a}$ for some ideal $\mathfrak{a}$

$\Longrightarrow$ R biequidim by §2

b) $\underset{\text{integral}}{\Bbbk[x_1,\dots,x_n] \hookrightarrow R}$ $\Longrightarrow$ $\dim R = \dim \Bbbk[x_1,\dots,x_n] = n$ by thm. $\square$

<u>Rem</u> The irreducible subset $\operatorname{Spec} R \hookrightarrow \mathbb{A}^m_{\Bbbk} = \operatorname{Spec} \Bbbk[y_1,\dots,y_m]$ is called an <u>affine variety</u>.

4. Transcendence degree

Another way to see dimension of affine varieties?

Recall:

Def Let $k \hookrightarrow K$ be a field extension.

A subset $\mathcal{B} \subseteq K$ is called <u>algebraically dependent</u> / k if $\exists$ distinct elements $b_1, \dots, b_n \in \mathcal{B}$ & $f \in k[x_1, \dots, x_n]$, $f \neq 0$ w/

$$f(b_1, \dots, b_n) = 0.$$

We say $\mathcal{B}$ is

- <u>alg. independent</u> / k if it is not alg dep / k
- a <u>transcendence basis</u> for K/k if it is alg indep / k and furthermore

$$\underset{\substack{\shortparallel \\ \left[\text{smallest subfield of } K \text{ containing } k \cup \mathcal{B}\right]}}{k(\mathcal{B})} \hookrightarrow K \text{ is an algebraic extension.}$$

Ex b) For singleton sets $\mathcal{B} = \{b\}$, we have:

$\mathcal{B}$ alg dep / k $\iff$ b algebraic / k $\iff$ $[k(b):k] < \infty$.

a) A subset $\mathcal{B} \subseteq k$ is alg. indep / k iff $\mathcal{B} = \emptyset$.

The empty set $\mathcal{B} = \emptyset$ is a transcendence basis for K/k iff K/k is algebraic.

c) A finite set $\mathcal{B} = \{b_1, \dots, b_n\} \subset K$ w/ $b_i \neq b_j$ $\forall i \neq j$ is alg. indep / k iff

$$\begin{aligned} k[x_1, \dots, x_n] &\hookrightarrow K \\ f &\longmapsto f(b_1, \dots, b_n) \end{aligned}$$

is an embedding. In this case it gives rise to a field extension

$$k(x_1, \dots, x_n) := \mathrm{Quot}(k[x_1, \dots, x_n]) \hookrightarrow K \qquad (*)$$

and $\mathcal{B}$ is a transcendence basis for K/k iff $(*)$ is an algebraic extension.

Thm Any field extension K/k has a (possibly infinite) transcendence basis, and any two such bases have the same cardinality.

Pf.

(1) Pick $\mathcal{A} \subseteq K$ alg. indep / k

Take $\mathcal{C} \subseteq K$ with $\mathcal{A} \subseteq \mathcal{C}$ and $K = k(\mathcal{C})$.

Claim: $\exists$ transcendence basis $\mathcal{B}$ for K/k w/ $\mathcal{A} \subseteq \mathcal{B} \subseteq \mathcal{C}$

("basis extension thm").

Indeed, let $\mathcal{S} := \{ \mathcal{B} \subseteq K \text{ alg. indep}/k \mid \mathcal{A} \subseteq \mathcal{B} \} \neq \emptyset$

partially ordered wrt "$\subseteq$" & union of any chain in $\mathcal{S}$ is again in $\mathcal{S}$

$\overset{\text{Zorn's}}{\underset{\text{lemma}}{\Longrightarrow}}$ $\exists$ max. element $\mathcal{B} \in \mathcal{S}$

Then $k(\mathcal{B}) \hookrightarrow K = k(\mathcal{C})$ is algebraic

(else $\exists\, b \in \mathcal{C} \setminus \mathcal{B}$ transcendental over $k(\mathcal{B})$, whence $\mathcal{B} \cup \{b\} \in \mathcal{S}$ $\lightning$)

$\Longrightarrow$ $\mathcal{B}$ is a transcendence basis for K/k.

(2) Now let $\mathcal{B}, \mathcal{B}' \subseteq K$ be two transcendence bases.

Wlog $|\mathcal{B}'| \leq |\mathcal{B}|$.

Distinguish 2 cases:

(2a) $\mathcal{B}$ finite:

$\Longrightarrow$ $\mathcal{B}'$ finite, say $\mathcal{B}' = \{b_1', \dots, b_m'\}$

$\mathcal{B} = \{b_1, \dots, b_n\}$ w/ $m \leq n$.

Induction on m:

$m = 0 \Rightarrow K/k$ alg $\Rightarrow n = 0$

$m > 0$: Take $f(x, y_1, \dots, y_n) \in k[x, y_1, \dots, y_n] \setminus \{0\}$ irreducible

w/ $f(b_1', b_1, \dots, b_n) = 0$ $(*)$

Since b_1' is not algebraic $/k$, may assume f involves some y_i, say y_1.

Then $\mathcal{B}'' := \{b_1', b_2, \dots, b_n\}$

is also a transcendence basis for K/k:

$$k(\mathcal{B}'') \underset{\substack{\text{algebraic}\\ \text{by } (*)}}{\hookrightarrow} k(\mathcal{B}'' \cup \{b_1\}) \underset{\substack{\text{algebraic}\\ \text{since } \mathcal{B} \subseteq \mathcal{B}'' \cup \{b_1\}}}{\hookrightarrow} K$$

If $\mathcal{B}''$ were alg. dependent / k,
then b_1' were algebraic / $k(b_2, \dots, b_n)$,
but then also b_1 would be so $\lightning$

$\Longrightarrow$ $\{b_2, \dots, b_n\}$ and $\{b_2', \dots, b_m'\}$ are transcendence bases for $K/k(b_1')$, hence $m = n$ by induction.

(2b) $\mathcal{B}$ infinite:

$\forall\, b' \in \mathcal{B}'$ $\exists$ finite subset $\mathcal{B}_{b'} \subseteq \mathcal{B}$

with b' algebraic $/\, k(\mathcal{B}_{b'})$.

Put $\mathcal{B}'' := \bigcup_{b' \in \mathcal{B}'} \mathcal{B}_{b'} \subseteq \mathcal{B}$.

Claim: Equality holds

Indeed, else $\exists\, b \in \mathcal{B} \setminus \mathcal{B}''$

But b is algebraic over $k(\mathcal{B}')$, hence over $k(\mathcal{B}'')$ ↯ (since $\mathcal{B}$ is alg. indep.)

$\Longrightarrow$ $\mathcal{B} = \bigcup_{b' \in \mathcal{B}'} \underbrace{\mathcal{B}_{b'}}_{\text{finite } \forall b'}$

$\Longrightarrow$ with $\mathcal{B}$ also $\mathcal{B}'$ has to be infinite

& in that case

$$|\mathcal{B}| = \Big|\bigcup_{b' \in \mathcal{B}'} \text{finite set}\Big| \le |\mathcal{B}' \times \mathbb{N}| = |\mathcal{B}'| \le |\mathcal{B}|$$

[set theory: Use Zorn's lemma to get a maximal $\mathcal{B}'' \subset \mathcal{B}'$ w/ $|\mathcal{B}'' \times \mathbb{N}| = |\mathcal{B}''|$ ... this works since $\mathcal{B}'$ is infinite]

by assumption

$\Longrightarrow |\mathcal{B}| = |\mathcal{B}'|$ $\square$

Def The <u>transcendence degree</u> of a field extension K/k is

$$\operatorname{trdeg}_k(K) := |\mathcal{B}|$$

for any transcendence basis $\mathcal{B}$ (all have same cardinality).

Ex
- $\operatorname{trdeg}_k(K) = 0 \iff K/k$ algebraic
- $\operatorname{trdeg}_k(k(X_1, \dots, X_n)) = n$
- $\operatorname{trdeg}_{\mathbb{Q}} \mathbb{Q}(\pi, e^{2\pi i/3}) = \operatorname{trdeg}_{\mathbb{Q}} \mathbb{Q}(\pi) = 1$

  because π is a transcendental number (Lindemann 1882)
- Schanuel's Conjecture (1960's):

  If $z_1, \dots, z_n \in \mathbb{C}$ are linearly independent $/\mathbb{Q}$,

  then $\operatorname{trdeg}_{\mathbb{Q}} \mathbb{Q}(z_1, \dots, z_n, e^{z_1}, \dots, e^{z_n}) \geqslant n$?

  e.g. are π and e alg. independent?

  (take $z_1 = 1$, $z_2 = i\pi$)

  ... still open!

(see e.g. M. Waldschmidt, Schanuel's Conjecture, Colloquium De Giorgi 2013/14 pp 129-137)

Prop Let R be a fingen k-algebra & a domain.

$$\Longrightarrow \dim R = \operatorname{trdeg}_k(K) \quad \text{with } K := \operatorname{Quot}(R).$$

Pf. Take a Noether normalization $k[x_1, \dots, x_n] \xhookrightarrow[\text{finite}]{} R$.

$$\Longrightarrow \dim R = n$$
$$= \operatorname{trdeg}_k k(x_1, \dots, x_n)$$
$$= \operatorname{trdeg}_k K$$

since $k(x_1, \dots, x_n) \hookrightarrow K$ is algebraic $\square$

Rem. "fin gen as a k-algebra" is important:

e.g. $R = k(x)$ has $\dim R = 0 < 1 = \operatorname{trdeg}_k K$

(here $K = R$).

Exercise. Show that for any k-algebra R which is a domain,

$$\dim R \leq \operatorname{trdeg}_k(K) \quad \text{with } K := \operatorname{Quot}(R).$$