Commutative algebra lecture 1

Examples of commutative rings

Number theory: $\mathbb{Z}$, $\mathbb{Z}[i] = \{m+ni \mid m,n \in \mathbb{Z}\}$, $\mathbb{Z}[\zeta]$ $\zeta = e^{2\pi i/23}$ $\zeta^{23}=1$

Is this ring a UFD? — $\mathbb{Z}$: yes, $\mathbb{Z}[i]$: yes, $\mathbb{Z}[\zeta]$: no

Invariant: Ideal class group $Pic(R)$ — how far from UFD

Alg Geo: Coordinate ring of a variety

$k[x,y]$ $\mathbb{Z}[x,y]$

$y^2 = x^3 - x$

$R := K[x,y]/(y^2 - x^3 + x)$

how are points of this curve related to R

Points $\Leftrightarrow$ $hom: R \to K$ $\Leftrightarrow$ ideal of R

Invariant theory

icosahedron $\leq \mathbb{R}^3$

Symmetry: 120

$I \subset \mathbb{R}^3$, so on $\mathbb{R}[x,y,z]$

Invariants = polynomials fixed by symmetries

$x^2 + y^2 + z^2$

Form invariant ring → what is the structure?

$\mathbb{R}[a,b,c]$ deg 2, 6, 10 — is the ring finitely generated? sometimes... ↓ it looks this

---

Course: mainly follow Eisenbud, readings + exercises may be in description

Atiyah + Macdonald

Zariski vol 1

More advanced: Zariski vol 1

Serre local algebra ← must read

Nagata local rings "examples of bad noetherian rings"

↳ lots of counter examples

Commutative Algebra → Matsumura

Commutative Algebra → Bourbaki

Elements of Algebraic Geometry → Grothendieck

Modern Syntax → Macaulay

Stacks Project → online

Lecture 2 Rings, Ideals, & Modules

Def: Ring R = set, $+, \times$

abelian group under $+$

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$

$(a+b)c = ac + bc$

$a(b+c) = ab + ac$

commutative: $ab = ba$

Identity: $1a = a = a1$

Examples of noncommutative rings:

Matrix Rings $M_n(R)$

Quaternions $a + bi + cj + dk$

Group Rings: G group $\mathbb{Z}[G]$ basis $g_i \in G$

$\times$: $gh = gh$ (ring prod, group prod)

Rings of differential operators: $\sum a_{ij} x^i \left(\frac{d}{dx}\right)^j \quad a_{ij} \in R$

$\frac{d}{dx} \cdot x - x \cdot \frac{d}{dx} = 1$

($\frac{d}{dx}$: differentiate; x: multiply by x)

$ab - ba$ simplifies a, b would be zero if commutative

$K[x,y]$ commutative basis x, y

non-commutative poly-rings

$K\{x,y\}$, $xy \neq yx$

basis words in x, y

lie, clifford algebras

Do rings have an identity? for us, yes!
rngs useful in analysis

Ex: $f: G \to \mathbb{R}$ G abelian

$f * g(b) = \sum_{a \in G} f(a)\, g(b-a)$

$G = \mathbb{R}$?

f, g continuous $\rightarrow$ $f*g(b) = \int_{a \in \mathbb{R}} f(a) g(b-a)$

converges if f, g continuous + compact support

↳ no identity

X = locally compact topological space

$C_0(X)$ vanish at ∞

↳ no identity unless X is compact

Rings without 1 $\Leftrightarrow$ locally compact spaces

Rings with 1 $\Leftrightarrow$ compact

↓ ↓ 1-point compactification

$R \to \mathbb{R} \oplus R$ $C_0(X \cup \infty) = \mathbb{R} \oplus C_0(X)$

$X = (0,1)$ $C_0(X)$

$X \cup \infty =$ ○—○ $C_0((0,1))$ continuous functions on $[0,1]$

$X \cup X =$ ○ ○

$\mathbb{R} \oplus C_0(X \cup X)$

$= \mathbb{R} \oplus (C_0(X) \times C_0(X)) \cong \mathbb{R} \times (C_0(X))$

$\not\cong \mathbb{R} \oplus (C_0(X) \times C_0(X) \times C_0(X))$

Recall: hom of rings $f: R \to S$

$f(a+b) = f(a) + f(b)$

$f(ab) = f(a) f(b)$

$f(1) = 1$ easy to forget!

Ideals: R commutative + identity from now on

kernel of ring hom $f: R \to S$

I: $a, b \in I$ $a \pm b \in I$

$a \in I$ $\forall a \in I, r \in R$

Example: $\mathbb{Z} \subseteq \mathbb{Q}$
subring, not ideal!

Ideals are examples of rngs!

$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/(n)$

$\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$

$k[x,y]/(y^2 - x^3 + x)$ = set of all functions vanishing on 

Modules: module over a ring is like a vector space over a field

M module over R

$R \times M \to M : r \mapsto rm$

$(r_1 r_2)m = r_1(r_2 m)$

$(r_1 + r_2)m = r_1 m + r_2 m$

$r(m_1 + m_2) = rm_1 + rm_2$

$1m = m$

modules are much more flexible than ideals.

Examples: $\mathbb{Z}$-module: abelian groups

k-module: vector space

$k[x]$-module: linear transformation

Submodule of R: Ideal I ⟶ module over itself → why modules are called modules

R/I : Quotient ring, still module over R

module generated by single element M.

$I = \mathrm{Ann}(M)$
$= \{r \in R \mid rm = 0 \ \forall m\}$

$n\mathbb{Z} \cong \mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ more interesting

$M \subseteq N$ N/M module

$I \subseteq J$ J/I not ideal

more complicated without commutativity

Groups	Rings
Act on set	Act on module M
G/N $N \lhd G$	R/I I ideal

G $\quad$ $\mathbb{Z}[G]$

$G \curvearrowright S$ $\quad$ M, basis of S as $\mathbb{Z}$-module

Lecture 3: What is a syzygy

Aim: Hilbert's Theorem

What is an invariant?

Example 1: rotations of $\mathbb{R}^3 \rightsquigarrow O_3(\mathbb{R})$

preserve length i.e. poly $x^2+y^2+z^2$ invariant of $O_3(\mathbb{R}) \curvearrowright \mathbb{R}^3$

($x^2+y^2+z^2$: poly on $\mathbb{R}^3$; $\mathbb{R}^3$: acted on as vector space)

How does G act on polynomials?

$V \to k$

$f: X \to Y$ $\quad$ X, Y acted on by G

$g(f) = ?$ $\quad$ $(gf)(x) = gf(g^{-1}x)$ what? why?

$(gf)(gx) = g(f(x))$

$(gf)(ggx) = gf(g^{-1}x)$

$A \times B$

$g(a \times b) = g(a) \times g(b) \to g$

$gf(x) = f(gx)$? don't!

$g_1 g_2 f(x) \to f(g_1 g_2 x)$ ✗ oops!

$\searrow g_2 f(g_1 x) = f(g_2 g_1 x)$

Example 2: $SL_n(k)$ acting on k^n

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ ↖ transitively on nonzero $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$

$SL_2(k)$ acts on $k^n \oplus k^n \oplus k^n \oplus \cdots$ (n)

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$

$\det = x_1 y_2 - x_2 y_1$ $\quad$ "determinant" invariant

$\det$ on $k^n \oplus \cdots \oplus k^n$ is invariant of $SL_n(k)$

Example 3: $G = S_n$ symmetric group

acts on $\mathbb{C}^n$

polys: $\mathbb{C}[x_1, \dots, x_n]$

invariant polynomials → poly's that say the same up to renumbering

$$e_1 = x_1 + x_2 + \cdots + x_n$$
$$e_n = x_1 x_2 x_3 \cdots$$
$$e_2 = x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n$$

$$(y - x_1)(y - x_n) \cdots (y - x_n)$$
$$= y^n - e_1 y^{n-1} + e_2 y^{n-2} \cdots \pm e_n$$

every invariant polynomial in $x_1, \dots, x_n$ is a polynomial in $e_1, \dots, e_n$

Order monomials:

$$x_1^{m_1} x_2^{m_2} \cdots > x_1^{n_1} x_2^{n_2}$$

if $m_1 > n_1$ or $m_1 = n_1$, $m_2 > n_2$ or ... (lex order)

Suppose f invariant.

Look at biggest monomial in f $\quad x_1^{n_1} x_2^{n_2} x_3^{n_3} \cdots$

Subtract $(x_1 + x_2 + \cdots)^{n_1 - n_2} \cdot (x_1 x_2 + \cdots)^{n_2 - n_3} \cdot (x_1 x_2 x_3 + \cdots)^{n_3 - n_4} \cdots$

This kills biggest monomial in f, (continue until now f is zero.

If f symmetric, then $n_1 \geq n_2 \geq n_3 \geq \cdots$

So invariants of $S_n \subset \mathbb{C}^n$ are finitely generated algebra over $\mathbb{C}$

Algebra of invariants is polynomial ring $\mathbb{C}[e_1, \dots, e_n]$ (unusual to have no nontrivial relations)
tends to happen if G is a reflection group

$G = A_n$ alternating group

$$\Delta = \prod_{i<j} (x_i - x_j) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \cdots$$

A_n = subgroup of S_n fixing Δ index 2 if $n \geq 2$

Invariants of A_n: polynomials in $e_1, \dots, e_n, \Delta$

Δ^2 is symmetric $\to$ poly in $e_1, \dots, e_n$

$n=2$ $\quad \Delta^2 = e_1^2 - 4e_2$

messy for $n > 2$

Example of a syzygy

A_n: ring of invariants is finitely generated by $e_1, \dots, e_n, \Delta$ but <u>nontrivial relation</u> $\underbrace{\Delta^2 - p(e_1, \dots, e_n) = 0}_{\text{first order syzygy}}$

Let $G = \mathbb{Z}/3\mathbb{Z}$ acting on $\mathbb{C}^2$ $\quad \sigma^3 = 1$, $\sigma \in G$ $\quad \sigma(x,y) = (\omega x, \omega y)$, $\omega^3 = 1$, $\omega = e^{2\pi i/3}$

$x^a y^b$ invariant if $3 \mid a+b$

$x^3 \quad x^2y \quad xy^2 \quad y^3$

$z_0 \quad z_1 \quad z_2 \quad z_3 \rightsquigarrow$ generate algebra of invariants

$$\left.\begin{aligned} z_0 z_3 &= z_1 z_2 \\ z_0 z_2 &= z_1^2 \\ z_1 z_3 &= z_2^2 \end{aligned}\right\} \text{3 syzygies}$$

$$\left.\begin{aligned} z_1 z_3 - z_1 z_2 &= a_2 \\ z_1^2 - z_0 z_2 &= a_3 \\ z_2^2 - z_1 z_3 &= a_1 \end{aligned}\right\} \text{first order syzygies}$$

$z_1 a_1 + z_2 a_2 + z_3 a_3 = 0 \to$ second order

exact sequence: $\quad$ dim 3 free module

$$0 \longrightarrow R^1 \longrightarrow R^3 \longrightarrow k[z_0, z_1, z_2, z_3] \to \text{invariants}$$

R_3

$a_1 \mapsto z_1^2 - z_1 z_2$

$a_2 \mapsto \dots$

$a_3 \mapsto \dots$

$b \mapsto z_1 a_1 + z_2 a_2 + z_3 a_3$

$$\dots \to R^x \to R^n \to R^m \to k[z_0, z_1, \dots] \to \text{Invariant Ring}$$

R^x: second order syzygies; R^n: first order syzygies; R^m: R

Is R finitely generated as a k-algebra?
Is R^m finitely generated as an R-module?
Is R^n " " " " "

(*) Is this chain of module finite?

$k[x]$ fg. as algebra and module

Hilbert: yes, if G is reductive (special case: $|G| < \infty$) and k char 0

Lecture 4: Invariant Theory

Binary quantics
↓ two variables ↓ don't know what degree is

$$a_n x^n y^0 + a_{n-1} x^{n-1} y^1 + \dots + a_0 y^n$$

Idea: take basis of $\mathbb{C}^{n+1}$: $a_n, a_{n-1}, \dots, a_0$

Group $SL_2(\mathbb{C})$ acts on $\mathbb{C}^n$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}$$

$$a_n (ax+by)^n (cx+dy)^0 + a_{n-1} (ax+by)^{n-1} (cx+dy)^1 + \dots$$

$$= a_n a^n + n a_{n-1} c^{n-1} + \dots) x^n + (\text{something worse}) x^{n-1} y + \dots$$

→ action of $SL_2(\mathbb{C})$ on $\mathbb{C}^{n+1}$

Invariants are polynomials in $a_n, \dots, a_0$

Examples: Discriminant: constant $\times \prod (\alpha_i - \alpha_j)^2$ α_i, α_j roots of $a_n x^n + \dots + a_0 = 0$

$$a_2 x^2 + a_1 xy + a_0 y^2 \longrightarrow q^2 - 4 a_2 a_0 \quad (b^2 - 4ac)$$

Catalecticant: $\det \begin{vmatrix} a_0 & a_1/3 & a_2/6 \\ a_1/3 & a_2/6 & a_3/3 \\ a_2/6 & a_3/3 & a_4 \end{vmatrix}$

Paul Gordan: Invariants of binary quantics are f.g.
& difficult to compute

Ternary cubics

x^3 x^2y xy^2 y^3
x^2z xyz y^2z
xz^2 yz^2
z^3

$SL_3(\mathbb{C})$ action → invariants generated by 2 of degrees 4, 6 (really bruted)

"Solve 5 40 equations in 118 variables"

Seems like Invariant Theory sort of devolved into chaos by end of 19th century

Syzygies = relations between invariants
to even worse than invariants

(1) If you can show invariants are f.g. then syzygies are also f.g.

$I \to k[x_1, \dots, x_n] \to$ ring of invariants
(ideal of first order syzygies)

Any ideal of $k[x_1, \dots, x_n]$ is f.g. (as ideal)

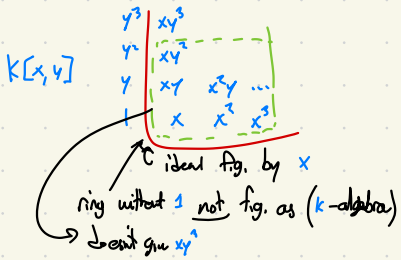
If all ideals are f.g., ring is called noetherian (Emmy Noether)

3 meanings of finite generation:

(1) f.g. as module or ideal
(2) f.g. as an algebra over a ring (ring → homomorphism)
(3) f.g. as a field

$k[x]$ f.g as algebra over k (x)
but not as module $1, x, x^2, x^3, \dots$

$k(x)$ = rational functions f.g. as field over k
but not algebra $\frac{1}{x-1}, \frac{1}{x-2}, \frac{1}{x-3}, \dots$



Extensions of Hilbert's thm

Hilbert showed invariant rings of G acting on $k[x_1, \dots, x_n]$ are often f.g. (k char 0)
↳ reductive

Is ring of invariants f.g. as an algebra for all groups?
Nagata → counterexample

Polynomial rings Noetherian
↳ are all ideals of any ring f.g.?
no! $k[x_1, \dots]$ (infinite variables)
○ ideal is not f.g.

$0 \to R^{n_k} \to \cdots \to R^{n_3} \to R^{n_2} \to R^{n_1} \to \underbrace{k[x_1,\dots,x_n] \to (\ ) \to 0}_{R^{n_0}}$] finite free resolution
Quotient (last way to write)

$R^{n_2} \to R^{n_1} \to R^{n_0} \to M \to 0$ free resolution
↳ modules over R

Does every f.g. module over Noetherian ring have finite free resolution?
True for integers! $0 \to \mathbb{Z}^x \to \mathbb{Z}^n \to M \to 0$] f.f.r. length 2
↑ free abelian group

Idea to fails: $R = k[x]/(x^2)$ basis $1, x$ $x^2 = 0$
$M = R/(x) \cong k$
$\cdots R \to R \to R \to k \to 0$
goes on forever! $1 \to 1$
$1 \to x$
$1 \to x$

Lecture 5: Noetherian Rings

TFAE:

(1) R is Noetherian

(2) All ideals of R are f.g.

(3) Every strictly increasing chain of ideals
$I_1 \subset I_2 \subset I_3 \subset \cdots$ is finite!

(4) Every nonempty set of ideals has a maximal element

Pf:

(1) $\Leftrightarrow$ (2) by def

(2) $\Rightarrow$ (3) Given a chain $I_1 \subset I_2 \subset \cdots$ form $I = \bigcup I_i$

I f.g. by $a_1, \ldots, a_k$

All a_i in I_n for some n

Then $I = I_n$ so chain stops at I_n

(3) $\Rightarrow$ (2) if $I \neq 0$ pick $a_1 \neq 0$ in I

if $I \neq (a_1)$ pick $a_2 \notin (a_1)$, $a_2 \in I$

if $I \neq (a_1, a_2)$ " a_3 " (a_1, a_2) $a_3 \in I$

$0 \subset (a_1) \subset (a_1, a_2) \subset \cdots$ finite by (2) so stops $\Rightarrow I$ f.g.

(3) $\Leftrightarrow$ (4) Nothing to do with rings.

General property for posets

(3) $\Rightarrow$ (4) for any poset: S is nonempty.

Pick $I_1 \in S$ if not max, pick I_2 with $I_1 \subset I_2$
I_2 " " " I_3 $I_1 \subset I_2 \subset I_3$
] implicitly using axiom of choice

etc. If no element maximal, we get infinite chain $\times$

$\Rightarrow$ maximal element

(4) $\Rightarrow$ (3) $I_1 \subset I_2 \subset \cdots$

Pick maximal element I_n by (4) $\Rightarrow$ chain finite: stops at I_n

Example: $k[x_1, x_2, \ldots]$ ∞ variables

(2) $(x_1, x_2, \ldots)$ not f.g. by def.

(3) $(x_1) \subset (x_1, x_2) \subset \cdots$ ∞ chain

(4) no maximal element

Decreasing / minimal: stronger condition (artinian)

$\mathbb{Z}$ $(2) \supset (4) \supset (8) \supset (16) \cdots$

∞ decreasing chain w/ no minimal element

Is it Noetherian?

$\mathbb{R}[x]$ polynomials ✓ from P.I.D. $\Rightarrow$ all ideals generated by 1 element

$\cap$

ring of analytic functions on $\mathbb{R}$ ✗ Sub $\mathbb{Z}$ w/ nonisolated pts. I = functions vanishing at all but finitely many pts. at $\mathbb{Z}$

$\cap$

Analytic on $[-1,1]$ closed ✓ finite num of zeroes on $[-1,1]$ f = polynomial $\times$ unit for with zeroes on $[-1,1]$

$\cap$

Analytic on $(-1,1)$ open ✗ $\mathbb{Z} = \{-\frac{1}{2}, -\frac{1}{3}, -\frac{1}{4}, \ldots\}$ same trick as above

$\cap$

Analytic at 0 ✓ $f = x^n \cdot$ unit only ideals (x^n) $n \geq 0$ and (0) discrete valuation ring

$\cap$

smooth near 0 ✗ f with ∞-order 0, $f \neq 0$ $f = e^{-1/x^2}$ $(x \neq 0)$, $f(0) = 0$ $(f) \subset (f^{1/2}) \subset (f^{1/3}) \subset \cdots$

$\cap$

maps to ring of formal power series ✓ $f = (x^n) \times$ unit $\rightarrow$ discrete valuation ring

All noetherian rings have well-behaved zeroes (finite orders, etc.)

Example: Is a subring of a Noetherian ring Noetherian?

Usually no. see above!

$R \subseteq \mathbb{Q}$ (field of quotients)

↑ Integral domain (no zero divisors)

Quotient rings: If R is Noetherian, so is any quotient R/I

ideals of R/I $\Leftrightarrow$ ideals of R containing I.

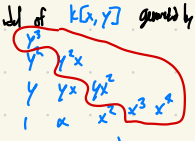
If R f.g. algebra over S, when S Noetherian then R is Noetherian $R = \frac{S[x_1, \ldots, x_n]}{I}$.

$\frac{k[x,y]}{(y^2 - x^3 + x)}$ Noetherian

$k[x]$ Every ideal generated by one element

Is every ideal of $k[x,y]$ generated by 2 elements?

A: No!



(y^3, y^2x, yx^2, x^4)

$I/(\text{degree } 3 \text{ polynomials})$ → V.S. requires at least 4 generators

Final example: Puiseaux series $k((x))$ (formal power series)

$a_0 + a_1 x + a_2 x^2 + \cdots$ infinite

we don't care if this converges!

think about them as lists $\{a_i\}$

$$k[[x]] \subseteq k[[x^{1/2}]] \subseteq \cdots \subseteq k[[x^{1/k!}]]$$

Is this Noetherian? No: $(x) \subset (x^{1/2}) \subset (x^{1/6}) \subset \cdots$

Lecture 6: Proof of Hilbert's thm

$k[x_1, \ldots, x_n]$ $\quad \mathbb{Z}[x_1, \ldots, x_n]$

All ideals are f.g.

$\Leftrightarrow$ All chains of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq$ eventually constant

more general:

R Noetherian $\Rightarrow R[x]$ Noetherian

k is Noetherian so $\uparrow \Rightarrow$ thm.

Proof: Suppose I is an ideal of $R[x]$

I_0 = ideal of leading coefficients of degree 0 elements ($a_0 \in I$) (constants)

I_1 = " " " " " 1 ($a_1 x + a_0 \in I$)

I_2 = " " " " " 2 ($a_2 x^2 + a_1 x + a_0 \in I$)

(1) I_k is ideal of R $\leftarrow$ so I_k f.g. (as ideal of R)

(2) $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots \leftarrow$ so for some n, $I_n = I_{n+1} = \cdots$

finite set of generators for I:

S_0 = finite set of polynomials of degree 0, a_0 whose leading terms generate I_0

S_1 = " " " " $a_1 x + a_0$ " " " " I_1

$\vdots$

S_n = " " " " $a_n x^n + \cdots + a_0$ Leading term a_n generates I_n

$S = \bigcup S_i$. Show S generates I.

If $f = a_m x^m + \cdots \in I$, we can find some element g of ideal (S) with leading coefficient

$m \leq n$: $a_m \in I_m$

$m > n$: $a_m x^n + \cdots$ multiply by x^{m-n}

$f - g \in (S)$ ← smaller degree than f, still in I repeat until $f=0 \Rightarrow I$ f.g.

Problem: not entirely constructive – for which n does chain stop?

Let $I \subseteq \mathbb{Z}$ is 1 a ideal? ✗ When do you know when to stop?
2? ✗ It could be (0) or
3? ✗ (1000000000)
4? ✗
5? ✗

$R[[x]]$ is Noetherian if R is Noetherian

$a_0 + a_1 x + a_2 x^2 + \cdots$

Slick proof:
Look at smallest term of power series.

I_0 = ideal of a_0's
I_1 = ideal of a_1's
⋮

$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ I_k ideal of R

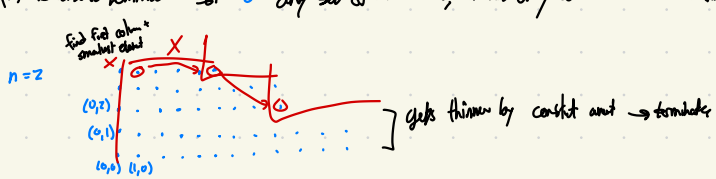
find n with $I_n = I_{n+1} = \cdots$

We seem to need an infinite sum to write f in terms of S.
need to add terms like $r_n s_n$, $r_{n+1} x s_n$, $r_{n+2} x^2 s_n$ ⋯
$(r_n + r_{n+1} x + r_{n+2} x^2 + \cdots) \notin R[x]$

So $R[[x]]$, $R[[x,y,z]]$ Noetherian ☺

Alternative Proof (Gordan):

(1) "Dickson's lemma" If S any set of monomials in $k[x_1, \ldots, x_n]$, it has only a finite number of minimal elements (ordered by divisibility) — partial order
exit conjecture: $x^3y^7 < x^4y^7 < x^5y^6$



(2) Now look at ideal $I \subseteq k[x_1, \ldots, x_n]$
order monomials w/ lex order → total order, well order

Define leading term of any poly as $x^{a^*} y^{b^*}$ s.t. maximal

Look at set of leading terms in I. This is a subset of monomials
It has finite # of minimal elements.
Pick a polynomial for each min elt
These then generate I. (If $f \in I$, pick one generator whose leading term $\leq$ leading term of f, use it to kill leading term of f → eventually goes to 0.) ▨
Woo Gröbner bases!

Lecture 7: finite generation of Algebra of invariants

Suppose G a finite group acts on finite dimensional vector space V over a field k with char 0.
Then algebra of invariants of G is f.g. (as a k-algebra)
↙ polynomials on k fixed by G.

$\dim V = n \rightarrow$ Algebra of polynomials $k[x_1, \dots, x_n]$
Grading: $\deg x_i = 1$
$\deg x_1^{n_1} x_2^{n_2} = n_1 + n_2 + \cdots$

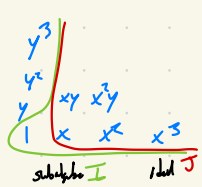
$R = \underset{\| }{R_0} \oplus \underset{\| }{R_1} \oplus \cdots$ $\quad R_i$ = things of degree i;
$k \quad (x_1, \dots, x_n)$

I = subalgebra of invariants
$I = I_0 \oplus I_1 \oplus I_2 \oplus \cdots$ ↙ no I_0 b/c $1 \in I_0$
J = ideal of R generated by $I_1, I_2, \dots$
$J = J_1 \oplus J_2 \oplus \cdots$

J = f.g. ideal by basis thm
generated by $a_1, \dots, a_k$ homogeneous

want to show $a_1, \dots, a_k$ generate algebra I.
(they generate the module (ideal) J of R)

Example:



× generates ideal J but does not generate algebra I

What extra property does I have?
It has a Reynolds operator $\rho \rightsquigarrow \rho(f) = \frac{1}{|G|}\sum_{g\in G} g(f)$

(k char 0 or at least char $k \nmid |G|$; G finite)

$\rho(1) = 1$
$\rho(fg) \neq \rho(f)\rho(g)$
$\rho(fg) = f\rho(g)$ if f fixed by G
$\rho(f) = f$ if f fixed by G

$$0 \to I \to R \to R/I \to 0$$
(I-modules)

ρ is a hom of I-modules from R to I
it splits the exact sequence
$R = I \oplus (\ker \rho)$ (as I-modules)

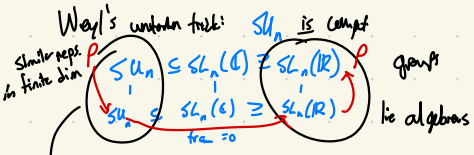
Proof by induction on degree that $a_1, a_2, \ldots$ generate I as k-algebra
pick $f \in I$ $\deg f > 0$
$f = a_1 c_1 + a_2 c_2 + \cdots$ $c_i \in R$
as $f \in$ ideal J

Apply ρ: $f = \rho(f) = \rho(a_1c_1) + \rho(a_2c_2) + \cdots$
(f fixed by G) $= a_1\rho(c_1) + a_2\rho(c_2) + \cdots$ (a_i fixed by G) ← is $k[a_1, \ldots, a_n]$
$\rho(c_i) \in I$
$\deg c_i < \deg f$ ($\deg a_i > 0$)
$\rho(c_i) \in k[a_1, \ldots]$ by induction ∎

Hilbert also proved for $SL_n(\mathbb{C})$: proof above works for compact groups: we can integrate over them!
(compact ⇒ finite volume)
$$\rho(f) = \frac{1}{|G|}\int_{g\in G} g(f)$$

But... $SL_n(\mathbb{C})$ not compact

Weyl's unitarian trick: SU_n is compact



groups

breaks for infinite dim b/c exponential map doesn't cover neighborhood of identity for infinite dim

$$\mathfrak{sl}_n(\mathbb{C}) \cong \mathfrak{sl}_n(\mathbb{R}) \otimes_{\mathbb{R}} \mathbb{C} \cong \mathfrak{su}_n(\mathbb{R}) \otimes_{\mathbb{R}} \mathbb{C}$$

Complex reps of $\mathfrak{su}_n$, $\mathfrak{sl}_n(\mathbb{R})$ same (complexification an isom)

Lecture 8: Noetherian Modules

module M over a ring R is Noetherian if all submodules are f.g. (R Noetherian as ring $\iff$ R noetherian as R-module)

$\Updownarrow$

any nonempty set of submodules has maximal element

$\Updownarrow$

every strictly increasing chain $M_1 \subset M_2 \subset \cdots$ of submodules is finite

Proof: analogous to Noetherian rings

$$0 \to A \to B \to C \to 0 \qquad A, B, C \text{ are } R\text{-modules}$$

B noeth $\iff$ A, C noetherian

$\Rightarrow$ easy

$\Leftarrow$

Take submodule M of B

generate M: (1) Take finite set of elements of M s.t. images of C generate image of M in C.
(2) Take finite set of elements of M generally $M \cap A$

If A, B noeth $\Rightarrow$ $A \oplus B$ Noetherian $\quad 0 \to A \to A \oplus B \to B \to 0$

> Any f.g. module M over a Noetherian ring is also Noetherian

$$0 \to R^n \to M \to 0$$

R^n: product of Noetherian modules

Application: syzygies f.g. (if invariants are)

$$\cdots R^m \to R^n \to R \to \text{invariants} \to 0$$

kernel = first order syzygies

R^n: Noetherian R-modules

R: $k[x_1, \ldots, x_n]$ Noetherian

All higher-order syzygies f.g. as R-modules

M f.g. over Noetherian ring

$\to R^{n_3} \to R^{n_2} \to R^{n_1} \to M \to 0$

n_1, n_2, n_3 finite

M has free resolution by f.g. free modules

Problem 1: chain might be infinite
Problem 2: Resolution might not be unique

$R = k[x_1, \dots, x_n]$

Chain finite, almost unique (could add $\to R \to R \to$ in somewhere)
$\rightsquigarrow$ minimal resolution unique

Noether: If G finite acts on v.s. V fin. dim/field k (any characteristic!)
then invariants of G are f.g.

Char $\neq 0 \Rightarrow$ no Reynolds operator!

$G = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \subseteq SL_2(k)$

$G \cong k^+$
acts on k^2

$k = \mathbb{F}_p$, G finite

want to find map that splits -- doesn't exist! action of G nontrivial

$0 \to k \to k^2 \to k \to 0$

G act trivially on

Proof (alternate argument):

Suppose $G \subset k[x_1, \dots, x_n]$ (k^n, x_i, R) each x_i is a root of polynomial

$(x - x_i)(x - g_1 x_i)(x - g_2 x_i) \cdots$

$= \prod_{g \in G} (x - g x_i) \in R[x]$

Coeffs are invariant under g
= elementary sym. functions in $g_1 x_1, g_2 x_2, \dots$

S = algebra generated by these coeffs.

$S \subseteq$ invariants $\subseteq R = k[x_1, \dots, x_n]$

f.g. algebra size $\leq n!|G|$

R is f.g. S-module

Each x_i is integral over S
↑ root of polynomial with leading coeff 1 and others in S

Generating set for $R = k[x_1, \dots, x_n]$ as S-module

$x_1^{n_1} x_2^{n_2} \cdots x_n^{n_n}$ $n_i < |G|$

$x_1^{|G|} =$ linear combination of $1, x_1, \dots, x_1^{|G|-1}$

$x_1^{|G|+1}$ " " " "

So have at most $|G|^n$ generators for R as an S-module.

$S \subseteq$ invariants $\subseteq R = k[x_1, \dots, x_n]$

① f.g. k-algebra ② f.g. S-module

Noetherian ring ④ f.g. S-module (submodule of Noetherian module) ③ Noetherian S-module

⑤ So invariants are f.g. k-algebra w/ generators:
(1) generators of S as k-algebra
(2) generators of invariants as S-module

Works in char 0... so why use Hilbert's at all?
A: Hilbert's works for some infinite groups

If $|G| = \infty$ in char $p > 0$ is ring of invariants a f.g. algebra?
much harder. Usually yes.

TFAE: G is algebraic group (i.e. $SL_n(k)$)

(1) If G acts on f.g. algebra over k, ring of invariants always f.g. algebra.

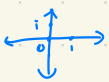
(2) G is reductive (no normal subgroups isomorphic to k^+) ← additive group of field not involved with G.

(3) If G acts on v.s. k^n with fixed vector $\neq 0$ then some poly fixed by G has $f(0) \neq f(v)$ → "nonlinear Reynolds operator"

Lecture 9: Euclidean Domains "How to draw a ring"

→ Point for each element
Point for each basis element
Point for each prime ideal

Examples: $\mathbb{R}$ 

$\mathbb{C}$ 

$\mathbb{Z}$ 

Gaussian integers $\mathbb{Z}[i] \subseteq \mathbb{C}$ 

Euclidean domain:

Integral domain R with division with remainder algorithm

Given $a, b \in R$ $b \neq 0$ then $a = qb + r$ ← remainder, ← quotient

$|r| < |b|$

$R \xrightarrow{1\text{-}1}$ well-ordered set such as $\{0, 1, 2, \ldots\}$

Euclidean domain → P.I.D. → unique factorization into primes

Euclid → P.I.D:

Pick $I \subseteq R$. If $I \neq (0)$ pick $a \in I$, $|a|$ minimal $(a \neq 0)$

check $I = (a)$ so I principal

$b \in I$, $b = aq + r$ $|r| < |a|$, $r \in I$ so $r = 0$

PID → UFD:

Key point: if p is irreducible ($p \neq 0$, unit, if $p = ab$, a or b is a unit)

then p is prime ($p | ab \Rightarrow p|a$ or $p|b$)

Proof: Suppose $p|ab$ if $p \nmid a$ look at $(p, a) = (x)$ $x | p$

so x is a unit and $(p, a) = (1)$

$\Rightarrow xp + ya = 1$

$xpb + yab = b$

$p | xpb + yab \Rightarrow p | b$

$\Rightarrow$ unique factorization into primes

key step: if $p_1 p_2 \cdots = q_1 q_2 \cdots$ p_i, q_i: irreducibles

then $p_1 \mid q_1 q_2 \cdots$

so $p_1 \mid$ some q_i

so $p_1 = q_i \times$ unit

remove, rinse, and repeat $\Rightarrow$ unique factorization up to units and ordering

So Euclidean domains are UFDs

$\mathbb{Z}[i]$ is Euclidean $\rightarrow$ If $a, b \in \mathbb{Z}[i]$, $b \neq 0$ then $a = qb + r$, $|r| < |b|$ $\quad |r|$ = complex absolute value

q in $\mathbb{Z}[i]$ (find) $\quad |a+ni| = \sqrt{n^2 + n^2}$ $\rightarrow$ well ordered

$\frac{a}{b} = q + \frac{r}{b}$

$\left|\frac{r}{b}\right| < 1 \Leftrightarrow |r| < |b|$

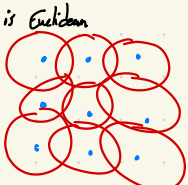
want to show any $\frac{a}{b}$ = something in $\mathbb{Z}[i]$ + something with $|\cdot| < 1$

$< r/b$

open unit disks with radius 1 cover $\mathbb{C}$ $\rightarrow$ we can always find something

$\Rightarrow$ so $\mathbb{Z}[i]$ is Euclidean

Exercise argument: $\mathbb{Z}[\sqrt{-2}]$

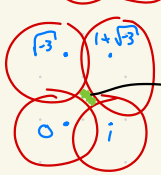


Open unit disks

Still cover plane!

So $\mathbb{Z}[\sqrt{-2}]$ also UFD

$\mathbb{Z}[\sqrt{-3}]$



point $\frac{1+\sqrt{-3}}{2}$

distance 1 from $0, 1, \sqrt{-3}, 1+\sqrt{-3}$

$\Rightarrow$ not necessarily Euclidean

In fact, not Euclidean, PID, or UFD $\quad 2 \times 2 = (1+\sqrt{-3})(1-\sqrt{-3})$

Example: $(2, 1+\sqrt{-3})$ not principal ideal

$\cdot = (1) = m + n\sqrt{-3}$

$\cdot = (2, 1+\sqrt{-3})$

triangle lattice

principal ideals form rectangular lattice $\quad (a) = a\mathbb{R}$

Replace $\mathbb{Z}[\sqrt{3}] \to \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ M+nW

ω $\omega^2+\omega+1=0$

unit disks cover plane → Euclidean Domain → PID

Euclidean Domains are rare even among UFDs

$R[x]$ UFD if R is

$k[x,y]$ is UFD, not PID → (x,y) not principal

Most PIDs are Euclidean Domains ($\mathbb{Z}$, $k[x]$, d.v.r; $\mathbb{Z}[i]$)

$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ PID but not Euclidean

If R Euclidean, let a be smallest element $a \neq 0$, $a \neq$ unit.
Every element of $R/(a)$ represented by 0 or unit. But $\mathbb{Z}\left[\frac{1+\sqrt{19}}{2}\right]$ has only 2 units: ± 1 → can't be Euclidean (somehow...)

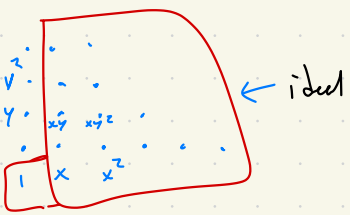
Picture method → good if underlying additive group can be embedded in a v.s.
Powerful when it works...but it doesn't usually...

Lecture 10: Weierstrass preparation thm

Draw a picture of each basic element

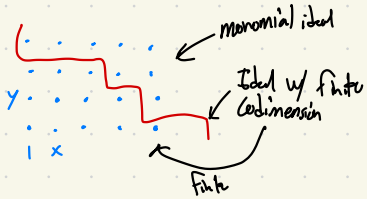
$k[x]$

$k[x,y]$

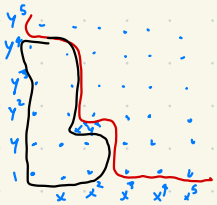


↑ ring not f.g. as algebra
not Noetherian

Ideals of finite codim



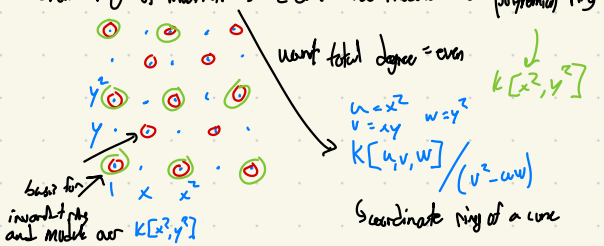
find $\dim R = k[x,y]/(x^3, x^2y^2, y^5)$



$\operatorname{codim} I = \dim k[x,y]/I = \dim R = 12$

$k[x,y]$ $\quad x \to -x \quad y \to -y$

Show: ring of invariants is 2-dim free module over polynomial ring



$k[[x,y]]$ is UFD

$k[[x]]$ UFD is trivial

↳ DVR, only ideals are (0), (x^n) $\Rightarrow$ PID

R UFD $\Rightarrow$ $R[x]$ UFD

$\Rightarrow R[x, y, \cdots]$ UFD

But R UFD $\not\Rightarrow R[[x]]$ UFD

Weierstrass Preparation Thm

Any power series in $k[[x,y]]$ $(\neq 0)$
can be written uniquely as $x^* \cdot$ unit $\cdot$ weierstrass poly.

$y^n + y^{n-1}(\ ) + y^{n-2}(\ ) \cdots + (\ )$

power series in x divisible by x

$(k[[x]])[y]$ // $(k[[y]])[x]$

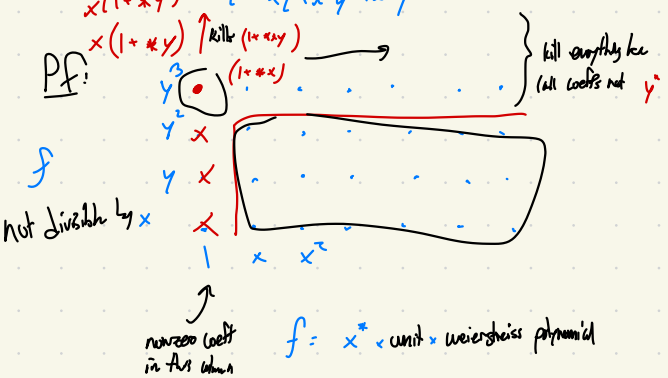
unit

$x(1+*y^2)$

$x(1+*y)$ kills $(1+*y)$

$1 + xy + x^2y^2 + x^3y^3 + \cdots$

Pf:



$f = x^* \cdot$ unit $\cdot$ weierstrass polynomial

Application: $k[[x,y]]$ is UFD.

It is Noetherian

Key point: if f irreducible, then it is prime
↳ if $f \mid gh$ then $f \mid g$ or $f \mid h$

Weierstrass assume f, g, h weierstrass polys

$f \mid gh \to fr = gh$ for some $r \in k[[x,y]]$

want to show r is poly in y

not weierstrass: $f = 1+x$ $r = 1 - x + x^2 - x^3 \cdots$, $g = h = 1$

$r = r_0 r_1$ r_0 = w. poly r_1 = unit

$(fr_0)r_1 = (gh)$

↑ w. polys ↑ $r_1 = 1$ by uniqueness of w. polys

So r is poly in y not x

so $f \mid gh$ in $(k[[x]])[y]$

so $f \mid g$ or $f \mid h$ bc ↑ is UFD

in $k[[x]][y]$

so $f \mid g$ or $f \mid h$ in $k[[x,y]]$

$\Rightarrow k[[x,y]]$ UFD

Warning: ring of convergent power series NOT UFD

f = convergent poly with infinite zeroes $z_1, \dots,$

$f(x) = (x - z_1) \cdots (x - z_n) \cdots$

Lecture 11: Spectrum of a ring

Draw a point for each prime ideal

Motivation:

X compact hausdorff space

R = ring of continuous functions on X

X is a good picture of R

↑ commutative C^* algebra

$|f| = \sup_{x \in X} |f(x)|$

Given R, reconstruct X:

points of $X \longleftrightarrow$ maximal closed ideals of R

$x \longleftrightarrow$ ideal of functions $f(x) = 0$

Stone-Weierstrass thm: all closed maximal ideals of R of this form

Topology on X: basis of open sets $\quad U(f) =$ "points where $f \neq 0$" $=$ points m with $f \in m$ (ideal as above)

Closed ideal $I \to Z(I)$ = set of max ideals containing I closed set
(not one-to-one) (common zeros of all $f \in I$)

Copy/extend for any commutable ring R

X = max ideals of R

Define topology as above

X called maximal spectrum of $R \quad \operatorname{Spec}_m(R)$

$R \to S \qquad m$ max ideal of S

Spec $\quad X \to Y \qquad f^{-1}(m)$ max ideal in R

Only works in C^*-algebras

$f: \mathbb{Z} \to \mathbb{Q}$

$m = 0$

$f^{-1}(m) = 0$ not max in $\mathbb{Z}$

Lets fix this problem $\quad R \to S \xrightarrow[\text{onto}]{} k \quad S/m$ = field

Image of $R \subseteq k$ so it is an integral domain, so it need not be a field

$R/f^{-1}(s) \subseteq k$

$f^{-1}(s)$ prime ideal $\iff R/p$ integral domain

$xy \in p \Rightarrow x \in p$ or $y \in p$

Subring of integral domain is integral domain

if $f: R \to S$ (1-1)

f^{-1}(prime) is prime

$\mathrm{Spec}(R)$: points correspond to prime ideals of R

topology → basis of open sets $U(f)$: $\{\mathfrak{p} \mid f \notin \mathfrak{p}\}$

closed sets: $Z(I) = \{\mathfrak{p} \mid I \subseteq \mathfrak{p}\}$

Check: do $Z(I)$ form a topology? $\bigcap Z(I_\alpha) = Z\left(\langle I_\alpha \rangle\right)$ (generated)

Closed under intersections: $Z(I) \cup Z(J) = Z(IJ)$ (generated by ij for $i \in I$, $j \in J$)

If $\mathfrak{p}$ prime, then $IJ \subseteq \mathfrak{p} \Leftrightarrow I \subseteq \mathfrak{p}$ or $J \subseteq \mathfrak{p}$

Examples

(0) not prime ideal: int domain definition $\Rightarrow 1 \neq 0$

(1) $R = 0$ (zero ring) $\mathrm{Spec}(R) = \emptyset$

(2) R = field $\mathrm{Spec}(R) = \{(0)\}$ is a point

(3) $R = \mathbb{C}[x]$

Prime ideals: maximal $(x-\alpha)$ $\alpha \in \mathbb{C}$

non max (0)

$\mathrm{Spec}(R) = \mathbb{C} \cup \infty$...ish

↳ generic point

$\mathrm{Spec}_m(R) = \mathbb{C}$

topology: closed sets $\mathbb{C}$, all finite sets

$I = (f) = \langle (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \rangle$

Topology not Hausdorff!

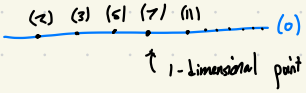
Add (0): (0) is not closed!

closure is whole space $\mathrm{Spec}(R)$

→ fuzzy generic point, everywhere dense

$\mathrm{Spec}(\mathbb{Z})$: maximal idals: $(2), (3), (5), (7), \ldots$
prime ideal: (0)

Closed sets: finite subsets of $(2), (3), (5), \ldots$
↑ not including (0), whole space



$\mathrm{Spec}(\mathbb{R}[x]) = \mathbb{R} \cup$ ~~generic pt~~ ← $\mathrm{Spec}(\mathbb{C}[x]) = \mathbb{C} \cup$ generic pt

max idls $(x-\alpha)$ $\alpha \in \mathbb{R}$
(0) not closed

max idls (x^2+bx+c) roots $x \pm iy$, $y \neq 0$
$b^2-4ac<0$

$\mathrm{Spec} \hookrightarrow$ generic pts (0)
$+ \{x+iy, x-iy\}$
$\hookrightarrow (0) \cup \mathbb{C}$ "folded in half"

in general
[$\mathrm{Spec}(k[x])$: pts ↔ orbits of $\mathrm{Gal}(\bar{k})$ on $\bar{k}$, together with (0)]

Lecture 12: Examples of Spec

Recall $\mathrm{Spec}\, R$ = topological space with points prime ideals of R

Why is it called the Spectrum of R?

Example: $R = \mathbb{C}[A]$ A = matrix in $M_n(\mathbb{R})$
↑ spectrum = eigenvalues → comes from quantum mechanics

If A has minimum polynomial $(x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\cdots$ spectrum $= \{\alpha_1, \alpha_2, \ldots\}$

$R \cong \mathbb{C}[x]/\text{min poly}$

↑ prim ideals: $(x-\alpha_i)$

Recall $\operatorname{Spec}\mathbb{Z}$ $\quad (2)\ (3)\ (5)\ \ldots\ (0)$

somewhat decomposed

$\operatorname{Spec}\mathbb{Z}\left[\frac{1}{2}\right]$ $\quad (3)\ (5)\ (7)\ \ldots\ (0)$ $\quad (2)$ killed

↑ if (2) is causing problems

$\operatorname{Spec}\mathbb{Z}_{(2)}$ $\quad (2)\ \ (0)$ $\quad (3), (5), \ldots$ killed

$= \left\{\frac{m}{n} \,\middle|\, n \text{ odd}\right\}$ ← focus on (2)

$\mathbb{Z}/2\mathbb{Z}$ $\quad \operatorname{Spec}\mathbb{Z}/2\mathbb{Z}$

$\operatorname{Spec}\mathbb{Z}[i]$ $\quad (1+i)\ (3)\ (2+i)\ (7)\ (11)\ (3+2i)\ (0)$

↓ $\quad (2-i)\quad (3-2i)$

$\operatorname{Spec}\mathbb{Z}$ $\quad (2)\ (3)\ (5)\ (0)$

$(7)\ (11)\ (13)$

1 mod 4 break into 2 primes

$(2) = (1+i)^2$

$(3) = (3)$

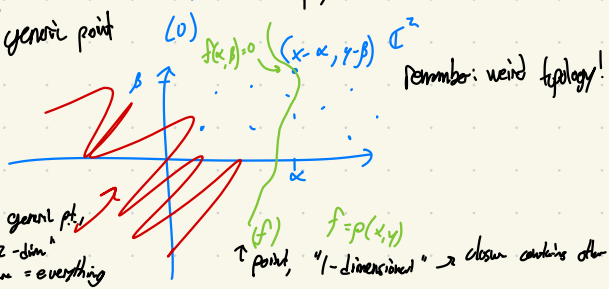
$(5) = (2+i)(2-i)$

$\operatorname{Spec}\mathbb{C}[x,y]$

maximal ideals: $(x-\alpha, y-\beta) \longleftrightarrow x, y \in \mathbb{C}^2$

prime ideals (f) f irred poly

generic point (0)

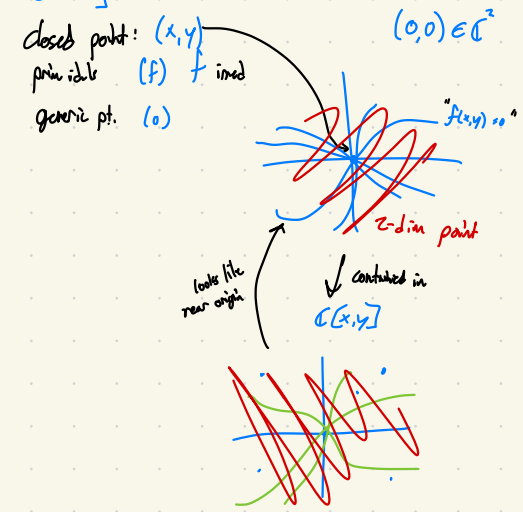


remember: weird topology!

(0) generic pt, "2-dim" closure = everything

↑ point, "1-dimensional" → closure contains other pts

$\mathbb{C}[[x,y]]$



Spec $\mathbb{Z}[x]$ → diff video in algebraic geometry

Spec of Hecke Ring → theory of modular forms

$$E_{12} = \frac{691}{65520} + \sum_n \sigma_{11}(n) q^n$$

$$= \frac{691}{65520} + q + 2049q^2 + \cdots$$

$$\Delta_{12} = q \prod_{n \geq 1} (1-q^n)^{24} = q - 24q^2 + \cdots$$

$$= \sum_n \tau(n) q^n$$

Hecke Algebra: spanned by Hecke operators T_n

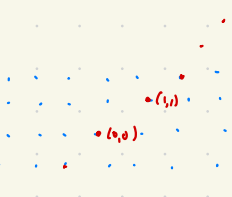
$$T_n(E_{12}) = \sigma_{11}(n) E_{12}$$

$$T_n(\Delta_n) = \tau(n) \Delta_n$$

Spec(Hecke Algebra)

↓

Subring of $\mathbb{Z} \times \mathbb{Z}$ generated by all $(\sigma_{11}(n), \tau(n))$



find other elements: are there any congruences $\sigma_{11}(n) \equiv \tau(n) \bmod N$

Ramanujan: $\sigma_{11}(n) \equiv \tau(n) \bmod 691$

$n=2 \quad 2049 \quad -24$

$\mathbb{Z} \times \mathbb{Z} \qquad (n,n) \qquad (n+691, n)$

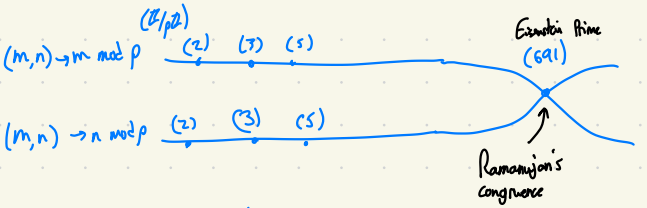
$R = \{(m,n) \mid m \equiv n \bmod 691\}$

$R \to \mathbb{Z} \times \mathbb{Z}$

$(m,n) \to m \quad n$

What is Spec R

$\operatorname{Spec} R \leftarrow \operatorname{Spec} \mathbb{Z} \cup \operatorname{Spec} \mathbb{Z}$



$691\,\Theta_\Lambda = 65520(E_{12} - \Delta)$

$\Theta_\Lambda = \sum_{\lambda \in \Lambda} q^{\lambda^2/2}$

Leech lattice

Lecture 13: topology of spectrum

$R \longrightarrow \operatorname{Spec} R$ points: prime ideals

↑ topological space

Basis opens: $U(f) = \{\mathfrak{P} \mid f \notin \mathfrak{P}\}$

"$f \neq 0$"

Closed sets $Z(I)$ (Ideal)

= primes containing I

Non-Hausdorff:

$\operatorname{Spec} \mathbb{Z}$: $(2)\ (3)\ \cdots\ (0)$

$\operatorname{Spec} R$ is quasicompact
= compact
= every open cover has a finite subcover

Suppose $\operatorname{Spec} R$ covered by open sets $U(f_i)$ (basis)
$\Rightarrow$ no prime (max) ideal contains all f_i
$\Rightarrow$ ideal generated by $\{f_i\}$ is R
$\Rightarrow$ $1 = \underbrace{\sum_i v_i f_i}_{\text{finite number}}$ ← algebra $\Rightarrow$ no infinite sums
$\Rightarrow$ $\operatorname{Spec} R$ covered by finite number of f_i.

Connectedness:
Is $\operatorname{Spec} R$ connected?
↑ nonempty, not union of two disjoint, nonempty open sets

R integral domain $\Rightarrow$ $\operatorname{Spec} R$ connected
= closure of (0) ↑prime b/c R integral domain

$\operatorname{Spec} R$ not connected:
$R = A \times B$ $\quad 1_A 1_B = 1$ any prime $\mathfrak{p}$ of R contains 1_A or 1_B so contains A or B
1_A 1_B

So $\operatorname{Spec} R = \operatorname{Spec} A \cup \operatorname{Spec} B$
$U(1_A)$ $U(1_B)$

Example: $\mathbb{Z}/120\mathbb{Z}$ CRT $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$
$\cong \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ m, n coprime

$\operatorname{Spec} \mathbb{Z}/120\mathbb{Z} =$ (2) (3) (5)

$\mathbb{Q}[G]$ G abelian group
↑basis $g \in G$
$gh = gh$
↑ring ↑group

G = klein 4-group

$1, a, b, c$ $\quad a^2 = b^2 = c^2 = 1$

$abc = 1$

Spec $\mathbb{Q}[G]$ $\quad e_0 = \frac{1+a+b+c}{4}$, $\quad e_1 = \frac{1-a+b-c}{4}$

$e_2 = \frac{1-a-b+c}{4}$ $\quad e_3 = \frac{1+a-b-c}{4}$

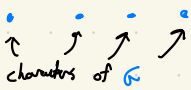
$e_i^2 = 1 \quad e_i e_j = 0 \quad i \neq j$

$e_0 + e_1 + e_2 + e_3 = 1$

$R = \mathbb{Q}[G] = e_0 R \oplus e_1 R \oplus e_2 R \oplus e_3 R$

$e_i R \cong \mathbb{Q}$

Spec $\mathbb{Q}[G]$



characters of G

$\mathrm{Hom}(G, \mathbb{C}^*)$

$\mathbb{C}[G]$ $\quad \chi : G \to \mathbb{C}^*$

$e = \frac{1}{|G|} \sum_{g \in G} \chi(g) g$

$\chi(a) = \chi(b) = -1 \quad \chi(c) = 1$

$|G| = 4$

$e = \frac{1-a-b+c}{4}$

$\frac{1-a-b+c}{4}$ $\quad a \to -1$, $b \to -1$, $c \to 1$

Irreducible

X irred if nonempty, not union of 2 proper closed sets

$\Leftrightarrow$ any 2 nonempty open sets intersect

Hausdorff + irreducible $\Rightarrow$ X is a point

Example: Spec $\mathbb{Z}$ is irreducible

Spec $\mathbb{Z} = \overline{(0)}$

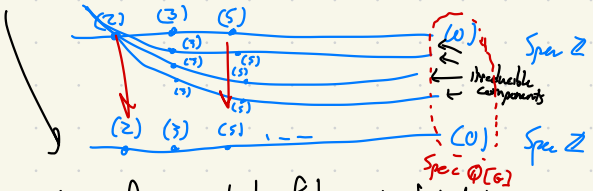
if x is a point, $\overline{x}$ is irreducible

$R = \mathbb{Z}[G]$ $\quad G$ = klein 4-group

Spec $\mathbb{Z}[G]$ $\quad$ characters of $\mathbb{Z}[G]$

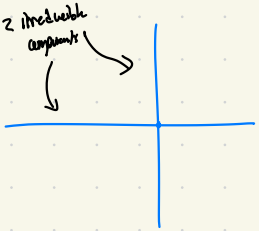
$\mathbb{Z} \to \mathbb{Z}[G] \rightrightarrows \mathbb{Z}$ $\quad a \to \pm 1$, $b \to \pm 1$

Spec $\mathbb{Z} \leftarrow$ Spec $\mathbb{Z}[G] \rightleftarrows$ Spec $\mathbb{Z}$



Common for spec to be finite union of irreducible components

Spec $\left(\mathbb{C}[x,y]/(xy)\right)$



It contains x or y

$\mathbb{C}[x]$ or $\mathbb{C}[y]$

$\mathbb{R}[x,y]/(y^2-x^3+x)$

polynomial curves on $y^2=x^3-x$

looks disconnected, but that's just in the Euclidean topology; however, it is connected and irreducible

Lecture 14: Irreducible subsets of Spec R

$x \in X$ $\quad \overline{x}$ irreducible

In Spec R, any closed irreducible subset is of the form $\overline{x}$, $x \in \text{Spec } R$

Pf: Let $Z(I)$ be irred. closed subset (I ideal)

$Z(I) = \overline{P}$ $\quad P = I$?

I need not be prime

$I = (4) \subseteq \mathbb{Z}$

$Z(I) = (2)$

Replace I by $\sqrt{I} = \{r \in R \mid r^n \in I \ n \geq 1\}$

↑ radical of I

Check under $\times$: if $r, s \in \sqrt{I}$

$r^m \in I \quad s^n \in I \quad m, n > 0$

$(r+s)^{m+n} = r^{m+n} + r^{m+n-1}s + \cdots + r^m s^n + \cdots + s^{m+n}$

divisible by $r^m \in I$ | divisible by $s^n \in I$

If $I \subseteq \mathfrak{p}$ $\quad \sqrt{I} \subseteq \mathfrak{p}$

$r^n \in \mathfrak{p} \Leftrightarrow r \in \mathfrak{p}$

So $Z(I) = Z(\sqrt{I})$

So we may assume $I = \sqrt{I}$

If $I = \sqrt{I}$ and $Z(I)$ irreducible, then I is prime

pick a, b with $ab \in I$ want to show $a \in I$, $b \in I$

Suppose not.

$(Ia)(Ib) \subseteq I \qquad (ab \in I)$

so $Z(Ia) \cup Z(Ib) = Z(I)$

↑ closed | ↑ closed | ↑ irreducible

$\Rightarrow Z(I) = Z(Ia)$ or $Z(Ib)$

WLOG $Z(Ia) = Z(I)$

but no power of a is in I since $a \notin I$, I prime

by Lemma (below), $\exists$ prime $\mathfrak{p}$ disjoint from $\{1, a, a^2, \ldots\}$

contains I ... contradicts $Z(Ia) = Z(I)$

$p \notin \quad p \in$

So I is prime. Easy to check $Z(I) = \overline{I}$

Lemma: Suppose S multiplicative subset of R disjoint from ideal I

$1 \in S$, $a, b \in S \Rightarrow ab \in S$

Then we can find a prime ideal $\mathfrak{p}$ $\quad \mathfrak{p} \cap S = \emptyset \quad p \supseteq I$

Pf: pick $\mathfrak{p}$ (maximal) among ideals disjoint from S containing I

↳ Zorn

we show $\mathfrak{p}$ is prime: suppose $ab \in \mathfrak{p}$

$\mathfrak{p} + (a)$, $\mathfrak{p} + (b)$ cannot both contain an element of S (otherwise so would $\mathfrak{p}$ by multiplicativity)

WLOG $\mathfrak{p} + (a) \cap S = \emptyset$

by maximality of $\mathfrak{p}$, $\mathfrak{p} = \mathfrak{p} + (a) \Rightarrow a \in \mathfrak{p}$ ↯

Application of lemma:

Spec of $C(X)$ is weird...
(continuous real functions on X; X compact Hausdorff space)

Max idls of $C(X)$ are just m_x $x \in X$
(functions vanishing at x)

If I is any idl s.t. for each $x \in X$, we can find $f_x \in I$ $f_x \neq 0$ then $I = R$

Cover X by sets where $f_x \neq 0$ (open sets $\Rightarrow$ finite cover)
(X compact)

finite # of f_x,

$y \in X \Rightarrow$ some $f_x(y) \neq 0$

$\sum f_x^2 > 0$ on X

So it a unit in I so $I = R$

(1) every prime of $C(X)$ is $\subseteq$ some unique max idel m_x $x \in X$

if $\mathfrak{p} \subseteq m_x \subseteq m_y$

$f(x) \neq 0$ $g(y) \neq 0$

$fg = 0$

$fg \in \mathfrak{p}$ so $\mathfrak{p}$ not prime

(2) If $\mathfrak{p}$ is closed, $\mathfrak{p} \subseteq m_x$ then

$\mathfrak{p} = m_x$ If $y \neq x$ $\mathfrak{p}$ contains element f $f(y) \neq 0$

(3) nonclosed prime ideals are weird

problem: do they exist?

Can't construct them, use lemma

pick point x (non-isolated)

I = idl of functions vanishing in nbhd of x

$S = \{1, f, f^2, \dots\}$ $f(x) \neq 0$ $f \notin I$

by Lemma, can find prim $\mathfrak{p}$ $\mathfrak{p} \cap S = \emptyset$ $\mathfrak{p} \supseteq I$

$\mathfrak{p} \subseteq m_x$

$\mathfrak{p} \neq m_x$

$f \in m_x$

$f \notin \mathfrak{p}$

So $\mathfrak{p}$ is non-maximal, non-closed prim ideal (apparently this depends on axiom of choice...)

Lecture 15: Noetherian Topological Spaces

R Noetherian ring $\to$ $\operatorname{Spec} R$ Noetherian top. space

for top. space X, tfae.

(1) Every nonempty set of closed sets has a minimal element
(2) Every nonempty set of open sets has a maximal element
} completeness of open/closed sets

(3) Every increasing sequence of open sets $U_1 \subseteq U_2 \subseteq U_3 \subseteq \cdots$ stabilizes

(4) Same for closed sets $\curvearrowright$ (decreasing)

(5) Every open set is quasicompact

R noetherian $\Rightarrow$ $\operatorname{Spec} R$ noetherian
(Closed sets correspond to (some) ideals)

X hausdorff + Noetherian $\Rightarrow$ X finite + discrete
(i.e. two props very incompatible!)

If $\operatorname{Spec} R$ Noetherian, is R noetherian?

$R = \underbrace{k[x_1, x_2, \dots]}_{(x_1^2, x_2^2, \dots)}$ ∞ variables

$\operatorname{Spec} R$ is a point only prim is $(x_1, x_2, \dots)$

R not Noetherian $\longrightarrow$ not f.g.

Noetherian induction: sps P property of closed sets $C \subseteq X$, where X noetherian
sps all proper closed subsets of C have $P \Rightarrow C$ has P
Then all closed sets have P.

Pf. if not, pick minimal closed set C without P
All proper subsets of C have P by minimality, so C has P by assumption ↯

Thm: In a Noetherian top. space, any closed set is the union of finite # of closed irreducibles

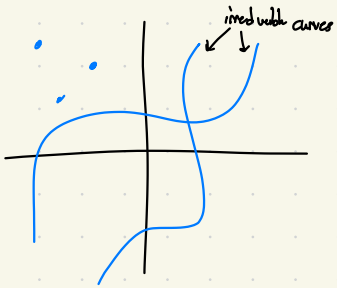
Pf: property P: C is union of finite # of irreducibles
Sps. every proper closed subset of C has prop P:

C → irreducible: union of 1 irreducible
→ not irreducible: $C = D \cup E$ D, E proper closed subsets
so D, E union of finite # of irreducibles by assumption
$\Rightarrow C$ is (by union)

Apply Noetherian induction ∎

R Noetherian ring $\Rightarrow$ all closed subsets of $\operatorname{Spec} R$ = union of finite # of irreducible = sets $\overline{x}$ (closure of points)

Examples: $R = \mathbb{C}[x,y]$ Algebraic set = set of common zeros of some polynomials
~ set of prime ideals containing some polynomials

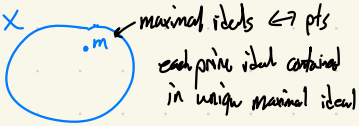


irreducible algebraic sets = varieties

Example: $\operatorname{Spec} C(X)$ X compact, Hausdorff
↑ continuous real functions

Closed sets of $\operatorname{Spec} R$ not usually union of finite irreducibles

hard-ish to figure out irreducibles of $\operatorname{Spec} C(X)$ b/c hard to figure out prim ideals of $C(X)$
not so important though



each irreducible subset contains at most 1 maximal ideal → copy of X → not decomposable into finite # of irreducibles

$C(X)$ non-noetherian, $\operatorname{Spec} C(X)$ non-noetherian ⇒ thm doesn't apply

Group S_3, group ring $\mathbb{Z}[S_3]$ → not commutative (womp womp)
Take center → spanned by conjugacy class $\{1\}$ $\{(12),(23),(31)\}$ $\{(123),(132)\}$

1 $a = (12)+(23)+(31)$ $b = (123)+(132)$

$R \cong \underset{1}{\mathbb{Z}} \oplus \underset{a}{\mathbb{Z}} \oplus \underset{b}{\mathbb{Z}}$ as Group

$a^2 = 3+3b$
$b^2 = 2+b$
$ab = 2a$

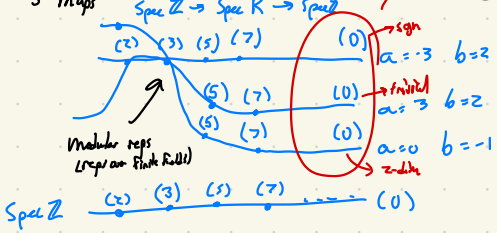
$\mathfrak{p}$ prim → $R/\mathfrak{p}$: $b^2-b-2=0$
$(b+1)(b-2)=0$
$b=-1$ or $b=2$

2 cases: $b=-1$ → $a^2=0$ → $a=0$
$a^2=3+3b$ $b=2$ → $a^2=9$ → $a=\pm 3$

This gives 3 homomorphisms $R \to \mathbb{Z}$
$b \mapsto -1$ $a \mapsto 0$
$b \mapsto 2$ $a \mapsto 3$
$b \mapsto 2$ $a \mapsto -3$

$S_3 \to k^n$ ⇝ class relations to $\operatorname{Spec} R$
$\mathbb{Z}(S_3) \to k$
↑ center ↑ representations

3 maps $\operatorname{Spec}\mathbb{Z} \to \operatorname{Spec} R \to \operatorname{Spec}\mathbb{Z}$



So $\operatorname{Spec} R$ has 3 irreducible components

Lecture 16: Localization

Ring R, subset S

Construct new ring: $R[S^{-1}]$

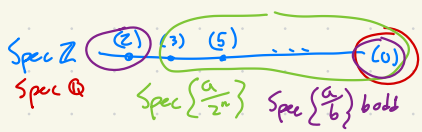
So all elements of S have inverses

Example: $R = \mathbb{Z}$ S = nonzero integers

$R[S^{-1}] = \mathbb{Q}$

$R = \mathbb{Z}$ $S = 2$ $R[S^{-1}] = \left\{\frac{a}{2^n}\right\}$

$R = \mathbb{Z}$ $S = \{3,5,7,\dots\}$ $R[S^{-1}] = \left\{\frac{a}{b}\right\}$ b odd



Localization: restriction to subset of spectrum (turns things into units)

$R = \mathbb{C}[x]$ S = all nonzero elements

$R[S^{-1}] = \mathbb{C}(x) = \left\{\frac{p(x)}{q(x)} \,\middle|\, q \neq 0\right\}$

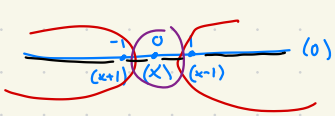
$R = \mathbb{C}[x]$ $S = \{x\}$

$R[S^{-1}]$: ring of all Laurent polynomials $= \left\{\sum_{-\infty}^{\infty} a_n x^n\right\}$

$= \left\{\frac{p(x)}{x^n}\right\}$

$R = \mathbb{C}[x]$ $S = \{x-\alpha \mid \alpha \neq 0\}$

$R[S^{-1}] = \left\{\frac{p(x)}{q(x)} \text{ defined at } 0\right\}$

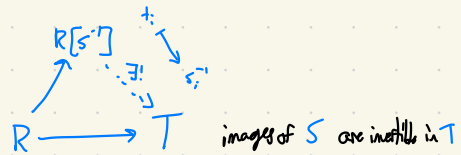


How do we construct $R[S^{-1}]$

$R[S^{-1}] = \frac{R[t_1, t_2, t_3, \ldots]}{(s_1 t_1 - 1, s_2 t_2 - 1, \ldots)}$ — one variable for each $s \in S$

t_i = inverse of s_i

how big is this?



images of S are invertible in T

$R \to R[S^{-1}]$

what is the kernel?

$rs = 0 \quad s \in S$
$\Rightarrow r = 0$ in $R[S^{-1}]$
$rs_1 s_2 = 0 \quad s_1, s_2 \in S$
$\Rightarrow r = 0$ in $R[S^{-1}]$
⋮

We assume S is a multiplicative subset

$1 \in S \quad s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$

Harmless: given S, take all finite products of $s_i \in S$ (and 1)
→ gives same $R[S^{-1}]$, makes little difference in practice
why? simplifies notation

So assume S is multiplicative with no zero divisors

Construct $R[S^{-1}]$

copy construction of $\mathbb{Q}$ from $\mathbb{Z}$

take all pairs $(r, s) \quad r \in R \quad s \in S$
r/s

recall $\frac{r_1}{s_1} = \frac{r_2}{s_2}$

Equivalence relation: $\frac{r_1}{s_1} \equiv \frac{r_2}{s_2} \iff r_1 s_2 = r_2 s_1$

Define $+, -, \times, 0, 1 \qquad 0 = \frac{0}{1}$

$\left(\frac{r_1}{s_1}\right) \times \left(\frac{r_2}{s_2}\right) = \frac{r_1 r_2}{s_1 s_2}$ → S multiplicative

$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$ → S multiplicative

$R \to R[S^{-1}]$
$r \mapsto \frac{r}{1}$

Check: (1) $\equiv$ is equivalence relation

(2) ops are well defined $\frac{r_1}{s_1} \equiv \frac{r_2}{s_2} \Rightarrow \frac{r_1}{s_1} + \frac{r_3}{s_3} = \frac{r_2}{s_2} + \frac{r_3}{s_3}$

(3) ring axioms

Most checks: easy

Subtle point: check $\equiv$ is transitive

$\frac{r_1}{s_1} \equiv \frac{r_2}{s_2}$ $\quad$ $\frac{r_2}{s_2} \equiv \frac{r_3}{s_3}$ shall imply $\frac{r_1}{s_1} \equiv \frac{r_3}{s_3}$

$r_1 s_2 = r_2 s_1$ $\quad$ $r_2 s_3 = r_3 s_2$ $\quad$ only if s_2 not zero divisor $\Rightarrow$ $r_1 s_3 = r_3 s_1$

$r_1 s_3 s_2 = r_2 s_1 s_3 = r_3 s_2 s_1 \rightarrow s_2(r_1 s_3 - r_3 s_1) = 0$

$R \longrightarrow R[S^{-1}]$ is injective $\leftarrow$ S no zero divisors

$r \mapsto \frac{r}{1}$ $\quad$ $\frac{r}{1} \equiv 0 \Leftrightarrow r = 0$

All elements of $R[S^{-1}]$ are of the form $\frac{r}{s}$

$\frac{r}{1} = 0 \Leftrightarrow r = 0$

Examples:

(1) R integral domain, S = nonzero elements $\rightarrow$ $R[S^{-1}]$ = field of quotients

(3) R any ring $\quad$ S = non zero-divisors $\rightarrow$ $R[S^{-1}]$ = total quotient ring

↑ multiplicative (↑ "biggest" quotient ring s.t. $R \subseteq R[S^{-1}]$

$R = \mathbb{Z} \times \mathbb{Z} \rightarrow R[S^{-1}] = \mathbb{Q} \times \mathbb{Q}$

S may have zero divisors

put I = (ideal) $r \in R$ with $rs = 0$ for some $s \in S$

$r_1 s_1 = 0$ $\quad$ $r_2 s_2 = 0$

$(r_1 + r_2) s_1 s_2 = 0$

$r_1 + r_2 \in I$ ↑ multiplicative

Image of S in R/I has no zero divisors

So can form $(R/I)[S^{-1}]$

$R[S^{-1}]$ → has universal properties!

Key point: the kernel of $R \rightarrow R[S^{-1}]$ is just $I = \{r \mid rs = 0 \text{ for some } s \in S\}$

Elements of $R[S^{-1}]$ all of form $rs^{-1} = 0 \Leftrightarrow rs_1 = 0$ for some $s_1 \in S$

$\frac{r_1}{s_1} = \frac{r_2}{s_1} \Leftrightarrow s(r_1 s_2 - r_2 s_1) = 0$ for some $s \in S$

↑ works directly if you don't want to quotient by I first

Examples: (1) $R = \mathbb{C}[x,y]/(xy)$ (y kills x) $\quad S = x$

$R[S^{-1}] \cong \mathbb{C}[x, x^{-1}]$

(2) $\mathfrak{p}$ prime ideal

S = complement of $\mathfrak{p}$

So can form $R[S^{-1}] = R_{\mathfrak{p}}$ localization of R at prime $\mathfrak{p}$

$\operatorname{Spec} R \sim \operatorname{Spec} R[S^{-1}]$

Lecture 17: $\operatorname{Spec} R[S^{-1}]$

$$f : R \longrightarrow R[S^{-1}]$$

ideals of R $\qquad$ ideals of $R[S^{-1}]$

$I \mapsto f(I)$ (not an ideal in general)

$I \mapsto$ ideal generated by $f(I)$ (extension I^e)

I is an ideal $\Rightarrow$ $f^{-1}(I)$

$J \longmapsto f^{-1}(J)$

contraction of J (ideal J^c)

If J is an ideal of $R[S^{-1}]$ then J = ideal generated by $f(f^{-1}(J))$

$$f(f^{-1}(J)) \subseteq J$$

Suppose $x \in J$ then $x = r/s$

so $r/1 = (1/s)\, r \in J$

so $r \in f^{-1}(J)$

so $r/1 \in f(f^{-1}(J))$

so $r/s \in$ ideal generated by

$J \mapsto f^{-1}(J)$

(injective map from ideals of $R[S^{-1}]$ to ideals of R)

Corollary: If R is Noetherian, so is $R[S^{-1}]$ ← localization is really nice

Noetherian $\Leftrightarrow$ ascending chain condition

($R[S^{-1}]$ not usually f.g. as R-algebra, so Hilbert's basis thm doesn't really help)

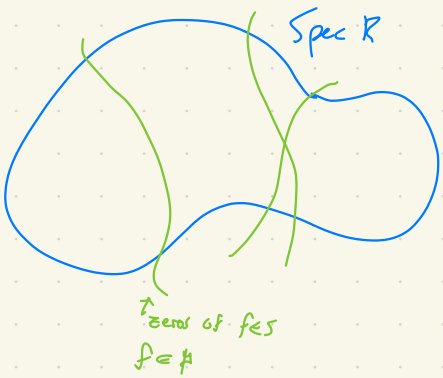
$\operatorname{Spec} R[S^{-1}]$ homeomorphic to subspace of $\operatorname{Spec} R$

it is subset (or, isomorphic to one, see above)

check topology: $\operatorname{Spec} R[S^{-1}]$ has basis of open sets $U(r/s)$ = prime not containing r/s

$= U(r/1)$

$\sim U(r)$ in $\operatorname{Spec} R$



pretend $s \in S$ are functions on $\operatorname{Spec} R$

$\operatorname{Spec} R[S^{-1}] = \operatorname{Spec} R$ - all zeros of elements of S

$\operatorname{Spec} R[S^{-1}] \cong$ subset of $\operatorname{Spec} R$

open subset of Spec R if S f.g.

subset of primes $\not\ni$ disjoint from S

Examples: $R_{\mathfrak{p}} = R[S^{-1}]$, S = complement of prime ideal $\mathfrak{p}$

"localization of R at prime $\mathfrak{p}$"

Examples $\mathbb{Z}_{(0)} = \mathbb{Q}$ $\mathbb{Z}_{(2)} = \{\frac{a}{b} \mid b \text{ odd}\}$

$\mathbb{C}[x]_{(0)} = \mathbb{C}(x)$ $\mathbb{C}[x]_{(x)}$ = rational functions defined at $0 \in \mathbb{C}$

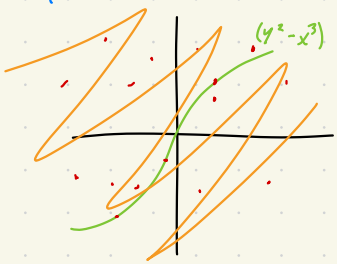
$R = \mathbb{C}[x,y]$ primes: (0)

(f), f irreducible polynomial i.e. $y^2 - x^3$

$(x-\alpha, y-\beta)$ $\alpha, \beta \in \mathbb{C}$

(f) finite set (0) closure contains everything

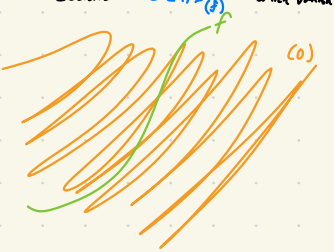
Spec $\mathbb{C}[x,y]$ $\quad (x-\alpha, x-\beta) \leftrightarrow (\alpha,\beta) \in \mathbb{C}^2$



Localize at (0) $\mathbb{C}[x,y]_{(0)}$

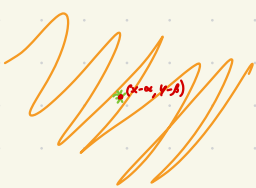
$\mathbb{C}[x,y]/(0)$

Localize $\mathbb{C}[x,y]_{(f)}$ ← invert all functions except those which vanish along f



$\mathbb{C}[x,y]/(f)$

Localize $\mathbb{C}[x,y]_{(x-\alpha, y-\beta)}$



$\mathbb{C}[x,y]/(x-\alpha, y-\beta)$

Quotient at prime: take all pts "inside" primes

Localize at prime: take all pts outside + nearby → "infinitely close"

Spec $R/\mathfrak{p}$: closure of $\mathfrak{p}$ contains all points

$\mathfrak{p}$ becomes minimal (zero) ideal

Spec R: points in closure of $\mathfrak{p}$ (prime containing $\mathfrak{p}$)

Spec $R_{\mathfrak{p}}$: points whose closure contains $\mathfrak{p}$ (primes contained in $\mathfrak{p}$)

$\mathfrak{p}$ becomes maximal ideal

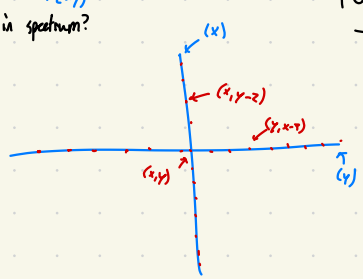
$\mathfrak{p}$ is <u>weird</u> closed pt

Example: localize $\mathbb{C}[x,y]/(xy)$ at (x,y)

How many points in spectrum?

Localize at (x,y) → $(0,0)$

Spec $\mathbb{C}[x,y]/(xy)$



3 pts in spectrum

Lecture 16: functions on $\operatorname{Spec} R$

$R = C(X)$ X compact Hausdorff

elements of R are functions on X

$X = \max \operatorname{Spec}(R)$

Can we do something similar for any R

R: functions on $\operatorname{Spec} R$

$\mathfrak{m}_x \subset C(X)$

↑ functions f, $f(x) = 0$ field $C(X)/\mathfrak{m}_x \cong \mathbb{R}$

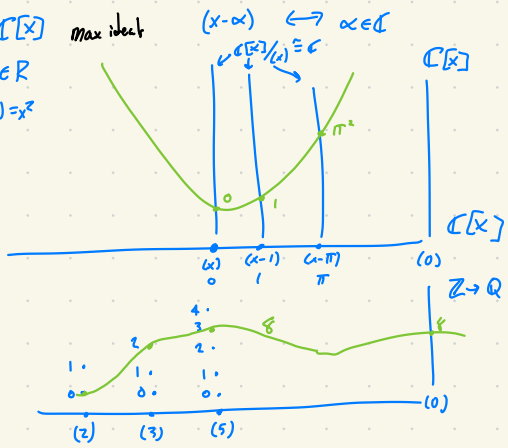
R = any ring $\mathfrak{p} \in \operatorname{Spec} R$ we get integral domain $R/\mathfrak{p}$

$f \in R$ as function $\operatorname{Spec} R \to \{R/\mathfrak{p}\}$

$R = \mathbb{C}[x]$ max ideals $(x-\alpha) \longleftrightarrow \alpha \in \mathbb{C}$

$f \in R$

$f(x) = x^2$



$R \longrightarrow$ (functions)

is this injective?

$f \to 0$ in all fields $(R/\mathfrak{p})$ → field of quotients

$f \to 0$ in $R/\mathfrak{p} \iff f \in \mathfrak{p}$

$f \to 0$ in all $R/\mathfrak{p} \iff f \in \bigcap_{\mathfrak{p}} \mathfrak{p}$

$a^2 = 0 \Rightarrow a \in$ all primes

$a^n = 0 \Rightarrow a \in$ all primes
$n \geq 1$

Nilradical of R $= \sqrt{0} = \{a \mid a^n = 0 \text{ for some } n\}$

$\subseteq \bigcap_{\mathfrak{p}} \mathfrak{p}$

↳ equals intersection of all primes

($S \cap I = \emptyset \Rightarrow$ find prim $\mathfrak{p}$ s.t. $\mathfrak{p} \supseteq I$ $\mathfrak{p} \cap S = \emptyset$)

$S = 1, a, a^2, \dots, a^n, \dots \quad I = (0)$

$S \cap I = \emptyset$ so $\exists\, \mathfrak{p} \supseteq I \quad \mathfrak{p} \cap S = \emptyset$

so $a \notin \mathfrak{p}$

$f \in R$ is a function from $\operatorname{Spec} R$ to local rings $R_{\mathfrak{p}}$ (instead of $R/\mathfrak{p}$)

Q: when does f have image 0 in $R_{\mathfrak{p}}$

A: when $fs = 0$ for some $s \notin \mathfrak{p}$

Suppose f has image 0 in all $R_{\mathfrak{p}}$ $\mathfrak{p} \in \operatorname{Spec} R$

f killed by some $s_{\mathfrak{p}} \notin \mathfrak{p}$ for any $\mathfrak{p}$

$\operatorname{Ann} f = \{x \mid fx = 0\}$

↑ ideal

$\operatorname{Ann} f \not\subseteq \mathfrak{p}$ for any $\mathfrak{p} \in \operatorname{Spec} R$

so $\operatorname{Ann} f = R$

so contains $1 \Rightarrow 1 \cdot f = 0 \Rightarrow f = 0$ yay injectivity!

$f \in R$: function with domain $\operatorname{Spec} R$ at any $\mathfrak{p} \in \operatorname{Spec} R$, takes values in $R_{\mathfrak{p}}$ $R_{\mathfrak{p}}/\mathfrak{p}$ ← integral domain

$C(X)$ suppose U open $\subseteq X$

$\mathcal{O}(U)$ = continuous functions on U

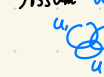
↑ sheaf time apparently

Properties: (1) $U \subseteq V$ $\mathcal{O}(V) \xrightarrow{\text{restriction}} \mathcal{O}(U)$

(2) presheaf: $U = U_1 \cup U_2 \cup \dots$

If $f \in \mathcal{O}(U)$ is 0 on every $\mathcal{O}(U_i)$ then $f = 0$

(3) Sheaf property: Assume $U = \bigcup_i U_i$ $f_i \in \mathcal{O}(U_i)$



f_i, f_j have same image on $\mathcal{O}(U_i \cap U_j)$

Then, can find $f \in \mathcal{O}(U)$ with restriction f_i on U_i

Problem: Given ring R, $\operatorname{Spec} R$

Want to define ring $\mathcal{O}(U)$, U open in $\operatorname{Spec} R$

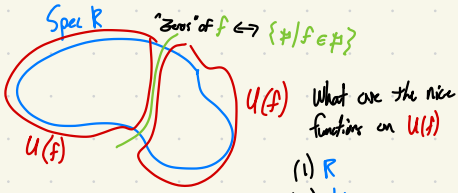
behaving "like this"

↑ as if $\mathcal{O}(U)$ is "nice" function on U

Just look at open sets $U(f) = \{\mathfrak{p} \mid f_i \notin \mathfrak{p}\}$

what about other open sets? ignore them!

So: what should $\mathcal{O}(U(f))$ be?



What are the nice functions on $U(f)$

(1) R

(2) $1/f$

Define $\mathcal{O}(U(f)) = R[f^{-1}]$

We have defined a "sheaf of rings" on $\operatorname{Spec} R$:

$U(f_i) \longrightarrow R[f_i^{-1}]$

Open sets of $\operatorname{Spec} R$ — Rings

want this to behave like Open sets of X ⟶ continuous functions on X

Lecture 19: Affine Schemes

Affine scheme of a ring

↑ pretending that R ring of functions on $\operatorname{Spec} R$

Open sets $U(f)$ $f \in R$

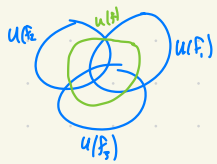
$\mathcal{O}(U(f)) = R[f^{-1}]$

↑ "functions on $U(f)$"

Restriction: $U(f_1 f_2) \subseteq U(f_1)$

$R[(f_1 f_2)^{-1}] \leftarrow R[f_1^{-1}]$ ✓

Proof: If $U(f)$ covered by $U(f_i)$



$g \in \mathcal{O}(U(f))$ is 0 in $\mathcal{O}(U(f_i))$ $\forall i$:
$\Rightarrow g = 0$ in $R[f^{-1}]$

Replace R by $R[f^{-1}]$ → can assume $f = 1$

$U(f_i)$ cover $\operatorname{Spec} R$ no prime ideal contains all f_i
$\Rightarrow$ ideal generated by f_i is R
$\Rightarrow \sum a_i f_i = 1$ for some a_i

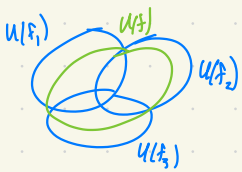
Suppose $g \in R$ $g = 0$ on all $\mathcal{O}(U(f_i))$
$g f_i^{n_i} = 0$ for some n_i
$\hookrightarrow g = 0$ in $R[f_i^{-1}]$

$(f_1, \dots, f_n) = R$ $\quad (\sum a_i f_i = 1)^N$
$(f_1^{n_1} \cdots f_n^{n_n}) = R$

so $\sum b_i f_i^{n_i} = 1$ for some b_i
$\sum b_i f_i^{n_i} g = g$
$\underbrace{\quad}_{0}$

$\Rightarrow g = 0$

Sheaf Condition: Suppose $U(f_i)$ cover $U(f)$



Given $r_i / f_i^{n_i}$ on $\mathcal{O}(U(f_i))$
Suppose same on $U(f_i) \cap U(f_j)$
Then can find some $r/f^n \in U(f)$
equal to $r_i / f_i^{n_i}$ on $U(f_i)$

1) Cheat: assume R integral domain for simplicity
2) Assume $f = 1$ by replacing R by $R[f^{-1}]$
3) As before $\sum a_i f_i = 1$ for some a_i ($U(f_i)$ cover $\operatorname{Spec} R$)
4) Can assume all $n_i = 1$ (replace f_i by $f_i^{n_i}$)

Goal: find $r \in R$ with $f_i r = r_i$ $\left(r = \frac{r_i}{f_i}\right)$

$\sum a_i f_i = 1 \Rightarrow \sum a_i f_i r = r$

$\| \quad \sum a_i r_i$

So we define $r = \sum a_i r_i$

now check $f_i r = r_i$:

$f_i r = \sum a_j r_j f_i = \sum a_j f_j r_i = r_i$

$r_j f_i = r_i f_j$ true because $\frac{r_j}{f_i} = \frac{r_i}{f_j}$ on $\mathcal{O}(f_i) \cap \mathcal{O}(f_j)$ + R integral domain

$r = \frac{r}{f_i}$ in $\mathcal{O}(u(f_i))$ $\Rightarrow$ behaves like fractions!

Spec R: $\mathcal{O}(u(f_i)) \leftrightarrow R[f^{-1}]$

Dictionary:

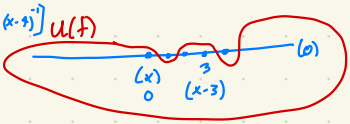
Algebra Ring R:	$\leftrightarrow$	Geometry Affine scheme Spec R:
prime ideal	$\leftrightarrow$	point
maximal ideal	$\leftrightarrow$	closed point
$f \in R$	$\leftrightarrow$	sort-of "function" $\mathfrak{p} \to R_{\mathfrak{p}}$
		"hypersurface of zeros" $\{\mathfrak{p} \mid f \notin \mathfrak{p}\}$
Ideal	$\leftrightarrow$ (not 1-to-1)	closed sets $Z(I)$
local ring $R_{\mathfrak{p}}$	$\leftrightarrow$	local ring of Spec R = "functions defined near $\mathfrak{p}$"
localization $R[f^{-1}]$	$\leftrightarrow$	open set $u(f)$ ← basis for topology
localization $R[S]$	$\leftrightarrow$	(ish) $\cap$ open sets
Idempotent $a^2 = a$	$\leftrightarrow$	closed & open sets u "$a = 0$" → clopen sets

Modules over R $\leftrightarrow$ Sheaves

Spec $\mathbb{C}[x]$

$f = (x-1)(x-3)$

$\mathcal{O}(u(f)) = \mathbb{C}[x]\left[\frac{1}{(x-1)}, \frac{1}{(x-3)}\right]$ ← allow poles at $1, 3$

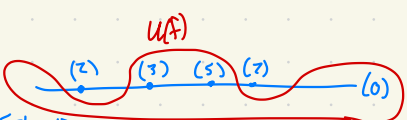


$\frac{x^2}{(x-1)(x-3)} \in \mathcal{O}(u(f))$

Spec $\mathbb{Z}$

$f = 14$

$\mathcal{O}(u(f)) = \mathbb{Z}[2^{-1}, 7^{-1}]$



$\frac{9}{28} \in \mathcal{O}(u(f))$

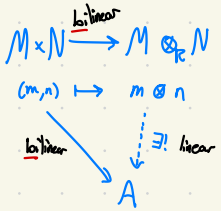
$= \frac{3^2}{2^2 \cdot 7}$

Lecture 20: Tensor Products

$M \otimes_R N$ gives a module over R

Module over R ↑ ring ↑ subtleties omitted

$M \otimes_R N$ is "universal" module for bilinear maps from $M \times N$

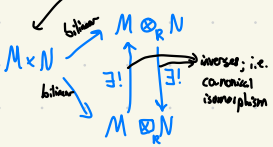


Bilinear maps $M \times N \to A$

$\|$

linear maps $M \otimes_R N \to A$

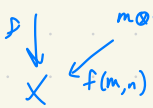
$M \otimes_R N$: unique? Exists?



Any two $\otimes$ are canonically isomorphic (essentially unique)

Existance: trivial

$M \times N \to M \otimes_R N$ = (free R-module generated by $m \otimes n$) / $(r(m \otimes n) - (rm) \otimes n, r(m \otimes n) - m \otimes rn,$ $(m_1 + m_2) \otimes n - m_1 \otimes n - m_2 \otimes n,$ $m \otimes (n_1 + n_2) - m \otimes n_1 - m \otimes n_2)$



make the map bilinear

useless in practice — quotient a huge thing by another huge thing with no clue how to work with it

Warning: for non-commutative rings, tensor product more subtle

$M \otimes_R N$ — M right R-module, N left R-module

↑ abelian group, not R-module

need M 2-sided, N left R-module

If M, N are R bi-modules, so is $M \otimes_R N$

Examples: $\otimes$ of modules over vector spaces, $\mathbb{Z}$

(1) $(M_1 \oplus M_2) \otimes N \cong (M_1 \otimes N) \oplus (M_2 \otimes N)$

bilinear maps $(M_1 \oplus M_2) \times N$
"same as" pairs Bilin map $M_1 \times N \to *$
$M_2 \times N \to *$

Same applies for $N = N_1 \oplus N_2$

(2) $R \otimes_R M \cong M$

Bilinear maps $R \times M \to X$
"same as" linear maps $M \to X$

for vector spaces: $k^m \otimes k^n \cong k^{mn}$

$\oplus$ mn copies of $k \otimes_k k \cong k$

Don't confuse $V \otimes W$, $V \times W$

$V \times W \xrightarrow{\text{not linear!}} V \otimes W$

basis $v_1, \dots, v_m, w_1, \dots, w_n$ (mn elements) basis $v_i \otimes w_j$ (mxn elements)

V basis $v_1, \dots, v_m$
W basis $w_1, \dots, w_n$

for f.g. abelian groups:
Any f.g. abelian group is $\oplus$ of copies of $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$

$\mathbb{Z} \otimes \mathbb{Z} = \mathbb{Z}$ $\quad \mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$ $\quad \mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/m\mathbb{Z}$

generated by $1 \otimes 1$

$m(1 \otimes 1)$
$= m1 \otimes 1 = 0$
$n(1 \otimes 1) = 0$
Similarly
$(m, n)(1 \otimes 1) = 0$
gcd

$\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z}$ is "at most" $\mathbb{Z}/(m,n)\mathbb{Z}$

there is a bilinear map $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \xrightarrow{\text{ordb}} \mathbb{Z}/(m,n)\mathbb{Z}$

$a \quad b \mapsto ab$

$\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/(m,n)\mathbb{Z}$

$\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} = 0$

if m, n coprime

$\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/3\mathbb{Z} = 0$

$\mathbb{Z}/24\mathbb{Z} \otimes \mathbb{Z}/20\mathbb{Z} = \mathbb{Z}/4\mathbb{Z}$

$R/I \otimes R/J \cong R/(I,J)$

(I, J: ideals; (I,J): ideal generated by I, J)

$R/I \otimes_R M \cong M/IM$

Tensor products and exactness

Suppose $0 \to A \to B \to C \to 0$ exact (R-modules)

Is $0 \to A \otimes M \to B \otimes M \to C \otimes M \to 0$ exact?

yes, if R is a field $\to B \cong A \oplus C$

no, if $R = \mathbb{Z}$

$0 \to \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$ ← universal counterexample to "everything"

$\otimes \mathbb{Z}/2\mathbb{Z}$

zero map ↓

$0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{\times 2} \mathbb{Z}/2\mathbb{Z} \xrightarrow{id} \mathbb{Z}/2\mathbb{Z} \to 0$

no longer exact!

not injective

BIG PROBLEM! → Homological algebra studies this problem

Lecture 21: Tensor Products and Exactness

Recall problem from last lecture:

right exact $\otimes \mathbb{Z}/2\mathbb{Z}$ ↷

$$0 \to \mathbb{Z} \xrightarrow{x^2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

$$\not{0} \to \mathbb{Z}\otimes\mathbb{Z}/2\mathbb{Z} \xrightarrow{x^2} \mathbb{Z}\otimes\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}\otimes\mathbb{Z}/2\mathbb{Z} \to 0$$

$\mathbb{Z}/2\mathbb{Z}$; x^2 not injective ; $\mathbb{Z}/2\mathbb{Z}$; $\mathbb{Z}/2\mathbb{Z}$

Homomorphisms $\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, *)$

left exact ↷

$$0 \to \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \to \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \to \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \to \not{0}$$

0 ; 0 (not onto) ; $\mathbb{Z}/2\mathbb{Z}$

$$\mathrm{Hom}(*, \mathbb{Z}/2\mathbb{Z}) \not{\leftarrow} \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \xleftarrow{x^2} \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \leftarrow \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \leftarrow 0$$

$\mathbb{Z}/2\mathbb{Z}$; not onto ; $\mathbb{Z}/2\mathbb{Z}$; $\mathbb{Z}/2\mathbb{Z}$

add this on after → $A \to B$, $B \xrightarrow{y} X$

$\mathrm{Hom}(A, X) \leftarrow \mathrm{Hom}(B, X)$

Suppose $0 \to A \to B \to C$ exact

then so is $0 \to \mathrm{Hom}(M, A) \to \mathrm{Hom}(M, B) \to \mathrm{Hom}(M, C)$

Let $f \in \mathrm{Hom}(M, B)$ s.t. image in $\mathrm{Hom}(M, C)$ is 0

Image of f is 0 in C

So image of $f \in \mathrm{Im}(A) \subseteq B$

So f "really" map from M to A

So $f \in$ image of $\mathrm{Hom}(M, A)$

Suppose $A \to B \to C \to 0$ exact

$\mathrm{Hom}(A, M) \leftarrow \mathrm{Hom}(B, M) \leftarrow \mathrm{Hom}(C, M) \leftarrow 0$

$f \in \mathrm{Hom}(B, M)$ suppose image is $0 \in \mathrm{Hom}(A, M)$

$\Rightarrow f$ vanishes on $\mathrm{Im}A \subseteq B$

$\Rightarrow f$ really hom from $B/\mathrm{Im}A = C$

$\Rightarrow f$ "really" in $\mathrm{Hom}(C, M)$

Suppose $A \to B \to C \to 0$ exact

$M \otimes A \to M \otimes B \to M \otimes C \to 0$

recall $\mathrm{Hom}(A,X) \leftarrow \mathrm{Hom}(B,X) \leftarrow \mathrm{Hom}(C,X) \leftarrow 0$ exact

then $\mathrm{Hom}(M, \mathrm{Hom}(A,X)) \leftarrow \mathrm{Hom}(M, \mathrm{Hom}(B,X)) \leftarrow \mathrm{Hom}(M, \mathrm{Hom}(C,X)) \leftarrow 0$ exact

$\mathrm{Hom}(M \otimes A, X) \leftarrow \mathrm{Hom}(M \otimes B, X) \leftarrow \mathrm{Hom}(M \otimes C, X) \leftarrow 0$

spaces of bilinear maps $M \times A \to X$

so induces tensor canonical isomorphism

Adjointness: $\otimes A$ left adjoint to functor $\mathrm{Hom}(A, *)$

Observe homs from $M \otimes C$ to $*$ same as homs from $M \otimes B$ to $*$ vanishing on $\mathrm{Im}\, M \otimes A$

so $M \otimes C$ really quotient $M \otimes B$ by $\mathrm{Im}\, M \otimes A$

so $M \otimes A \to M \otimes B \to M \otimes C \to 0$ exact

Calculate $\otimes \left[\otimes_R \mathrm{Hom}_R \right]$

$A \otimes M$

$R^m \to R^n \to A \to 0$

$\otimes M$ $\quad R^m \otimes M \to R^n \otimes M \to A \otimes M \to 0$

$M^m \to M^n \to A \otimes M \to 0$

$A \otimes M \cong M^n / M^m$

$\otimes$ commute with direct limits (special case of left-adjointness)

$A_1 \to A_2 \to A_3 \to \cdots$ $\qquad \varinjlim A_i = \dfrac{\text{union of all } A_i}{a_i \sim a_j \text{ if } a_i \text{ is mapped to } a_j \text{ under a map}}$

Bilinear maps $\left(\varinjlim A_i\right) \times M$ to X

same as $\varinjlim$ (Bilinear maps $A_i \times M \to X$)

convert to $\otimes$ $\left(\varinjlim A_i\right) \otimes M$

$= \left(\varinjlim A_i \otimes M\right)$

$\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ $\quad \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \xrightarrow{\times 3} \mathbb{Z} \xrightarrow{\times 4} \mathbb{Z} \to \cdots$

$\otimes \mathbb{Q} \quad \mathbb{Q} \xrightarrow{\times 2} \mathbb{Q} \xrightarrow{\times 3} \mathbb{Q} \xrightarrow{\times 4} \mathbb{Q}$

$\varinjlim \mathbb{Q} = \mathbb{Q}$

So $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}$

Nasty trap:

$\mathbb{Q} \otimes \mathbb{Z}/2\mathbb{Z}$

$\mathbb{Q} = \varinjlim \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \xrightarrow{\times 3} \mathbb{Z} \xrightarrow{\times 4} \cdots$ (injective; not injective (always))

$\otimes \mathbb{Z}/2\mathbb{Z}$ $\quad \mathbb{Q} \otimes \mathbb{Z}/2\mathbb{Z} = \varinjlim \mathbb{Z}/2\mathbb{Z} \xrightarrow{\times 0} \mathbb{Z}/2\mathbb{Z} \xrightarrow{\times 1} \mathbb{Z}/2\mathbb{Z} \xrightarrow{\times 0} \cdots$

$= \mathbb{Z}/2\mathbb{Z}$

$= 0$ (by the relation we quotiented out by)

Lecture 22: Flatness, Tensor Products, Localization

Define M is called flat if $M \otimes *$ preserves exactness

i.e. if $0 \to A \to B \to C \to 0$ exact, then

$0 \to M \otimes A \to M \otimes B \to M \otimes C \to 0$ also exact

always exact

Example: over $\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ not flat? (not exact)

over R, R is exact, $R \otimes_R A \cong A$

M flat $\Rightarrow$ $M_{\mathfrak{p}}$ vary "nicely"

↳ family of modules over local rings

Main result: $R[s^{-1}]$ is a flat R-module

↑ localization is always nice

Define: $M[s^{-1}]$. Recall: Defined $R[s^{-1}]$

elements r/s $\quad \frac{r}{s} = 0 \iff rs_1 = 0$ some $s_1 \in S$

Define $M[S^{-1}]$ in the same way. Essentially copy everything

elements of the form m/s $\quad m/s = 0 \iff ms_1 = 0$ for some $s_1 \in S$

$m/s_1 = m_2/s_2 \iff (ms_2 - ms_1)s = 0$ for some $s \in S$

Key point: $M \to M[S^{-1}]$ preserves exactness

$$0 \to A \to B \to C \to 0 \quad \text{exact}$$
$$\Rightarrow \quad 0 \to A[S^{-1}] \to B[S^{-1}] \to C[S^{-1}] \to 0 \quad \text{exact}$$

Suppose $bs^{-1} \in B[S^{-1}]$ has image 0 in $C[S^{-1}]$

b has image $c \in C$

$bs^{-1} \to cs^{-1} = 0$

so $cs_1 = 0$ for some $s_1 \in S$

so bs_1 in image of A, say, of $a \in A$

$bs^{-1} = bs_1 s_1^{-1} s^{-1} = a(s_1 s)^{-1} \in$ image of $A[S^{-1}]$

$M_{\mathfrak{p}}$ prime $\mathfrak{p}$

$= M[S^{-1}]$, S = complement of $\mathfrak{p}$

"stalk" of M at $\mathfrak{p}$

M "sheaf" of "modules" over "sheaf of rings"

$U(f) \to R[f^{-1}]$

$U(f) \to M[f^{-1}]$ ← "quasi-coherent sheaf"

stalk

$\mathfrak{p} \to R_{\mathfrak{p}} \qquad \mathfrak{p} \to M_{\mathfrak{p}}$

↑ family of them parametrized by points in $\operatorname{Spec} R$

$R[S^{-1}]$ is flat

$A \to A \otimes_R R[S^{-1}]$ preserves exactness?

$A \to A[S^{-1}]$ preserves exactness

Show: $A[S^{-1}] = A \otimes_R R[S^{-1}]$

$a s^{-1} \longmapsto a \otimes s^{-1}$

$(ar)s^{-1} \longleftarrow a \otimes r s^{-1}$

So $R[S^{-1}]$ is flat (as an R-module)

R/I not usually flat (as an R-module)

$\mathbb{Z}/2\mathbb{Z}$

$0 \to A \to B \to C \to 0$ R-modules

$\not{0} \to A/IA \to B/IB \to C/IC \to 0$

$A \otimes_R R/I$

localizing much easier + nicer than quotient

Suppose R integral domain (for proof simplicity)

$0 \to R \xrightarrow{\times a} R \to R/aR \to 0$ exact ($a \neq 0$)

$\otimes M$

M flat! $0 \to M \xrightarrow{\times a} M$ exact

$\Rightarrow$ mult by nonzero a is injective on M!

So flat modules are torsion-free

$ma = 0$ for $a, m \neq 0$

$R \ni a$, $m \in M$

for $\mathbb{Z}$, torsion-free modules are flat Torsion-free $\iff$ flat

↑ true for all PID

flatness $\iff$ localization

(1) Vanishing is local: $M = 0 \iff M_{\mathfrak{p}} = 0$ for all primes $\mathfrak{p}$ (or all max ideals)

Suppose $M_{\mathfrak{m}} = 0$ for all maximal ideals

Pick $x \in M$ $x = 0$ in $M_{\mathfrak{m}}$ $\Rightarrow$ x killed by something not in $\mathfrak{m}$.

$\mathrm{Ann}(x) \not\subseteq \mathfrak{m}$

So $\mathrm{Ann}(x)$ not in any max ideal

so $\mathrm{Ann}(x) = R$

so $x = 0$

(2) Exactness is local $\quad 0 \to A \to B \to C \to 0$ exact

$\iff 0 \to A_{\mathfrak{p}} \to B_{\mathfrak{p}} \to C_{\mathfrak{p}} \to 0$ exact for all prime $\mathfrak{p}$ (or max ideals)

($\Rightarrow$) localization preserves exactness

($\Leftarrow$) $\left(\ker(B \to C)/\mathrm{Im}(A \to B)\right)_{\mathfrak{m}}$ vanishes iff vanishes for all $\mathfrak{m}$

$= \ker(B \to C)_{\mathfrak{m}} / \mathrm{Im}(A \to B)_{\mathfrak{m}}$ as $R_{\mathfrak{m}}$ is flat

(3) flatness is local $\quad M$ is flat $\iff M_{\mathfrak{p}}$ flat for all primes $\mathfrak{p}$ (or maximal)

($\Leftarrow$) Suppose $0 \to A \to B \to C \to 0$ exact

want to show this $\otimes M$ is exact

$0 \to (A \otimes M)_{\mathfrak{m}} \to (B \otimes M)_{\mathfrak{m}} \to (C \otimes M)_{\mathfrak{m}} \to 0$

$\| \qquad\qquad \| \qquad\qquad \| \qquad\qquad \|$

$A_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} M_{\mathfrak{m}} \to \quad " \quad \to \quad " \quad \to 0$

Lecture 23: flat extensions

Rings $R \to S$ (S is an R-algebra, extension of R)

R-modules $\leftrightarrow$ S-modules

$M \longrightarrow S \otimes_R M$

$\mathrm{Hom}_R(M,N) \longrightarrow \mathrm{Hom}_S(S \otimes_R M, S \otimes_R N)$ (homomorphism? Usually, not.)

$S \otimes_R \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_S(S \otimes_R M, S \otimes_R N)$ (still not isomorphism)

$R = \mathbb{Z}$ $\quad S = \mathbb{Z}/2\mathbb{Z}$

$M = \mathbb{Z}/2\mathbb{Z}$ $\quad S \otimes_R M = \mathbb{Z}/2\mathbb{Z}$ $\quad S \otimes_R N = \mathbb{Z}/2\mathbb{Z}$

$N = \mathbb{Z}$

$S \otimes_R \mathrm{Hom}_R(M,N) = 0 \quad \mathrm{Hom}_S(S \otimes_R M, S \otimes_R N) = \mathbb{Z}/2\mathbb{Z}$

$\neq$

The map is isomorphism if S is a fld R-module and M is finitely presented

($\otimes S$ preserves exactness)

finitely presented: $R^m \to R^n \xrightarrow{\text{onto}} M \to 0$

m, n finite

R Noetherian: finitely generated $\Rightarrow$ finitely presented

want for $S \otimes_R \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_S(S\otimes_R M, S\otimes_R N)$ is isomorphism

(1) Trivial if $M = R$

(2) Obvious if $M = R^n$ (n finite)

$m_1, m_2 \to M_1 \oplus M_2$

(3) $R^m \to R^n \to M \to 0$ (m, n finite)

$\mathrm{Hom}(*, N)$

$$0 \to \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(R^n, N) \to \mathrm{Hom}_R(R^m, N)$$

$\otimes S$

flat

$$0 \to 0 \to S\otimes_R \mathrm{Hom}_R(M,N) \to S\otimes_R \mathrm{Hom}_R(R^n, M) \to S\otimes_R \mathrm{Hom}_R(R^m, N)$$

$$\| \quad \| \quad \downarrow ? \quad \| \quad \| $$

$$0 \to 0 \to \mathrm{Hom}_S(S\otimes_R M, S\otimes_R N) \to \mathrm{Hom}_S(S\otimes_R R^n, S\otimes_R N) \to \mathrm{Hom}_S(S\otimes_R R^m, S\otimes_R N)$$

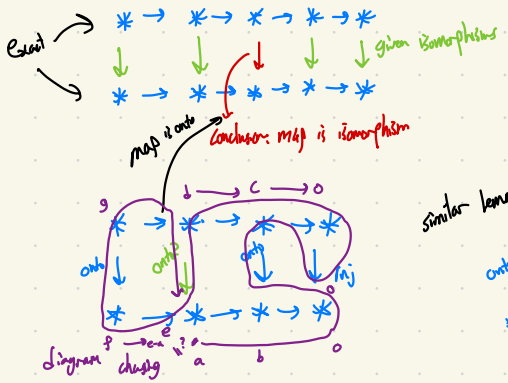
$\mathrm{Hom}(*, S\otimes_R N)$

$S\otimes$

$$S\otimes_R R^m \to S\otimes_R R^n \to S\otimes_R N \to 0$$

$$R^m \to R^n \to N \to 0$$

follows from 5-lemma:



$$\begin{array}{ccccccc} 0 & \to & 0 & \to & \mathbb{Z} & \to & \mathbb{Z} \quad \text{exact} \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 0 & \to & \mathbb{Z} & \to & \mathbb{Z} & \to & 0 \quad \text{exact} \end{array}$$

(arrows: onto, onto, not onto, onto)

Example: what if M is not finitely presented

$R = \mathbb{Q}$ $S = \mathbb{Q}[x]$ S flat R-module

$M = \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \cdots$ ∞-dim vector space

$N = \mathbb{Q}$

$$\mathbb{Q}[x] \otimes \mathrm{Hom}_{\mathbb{Q}}(M, N) \overset{?}{=} \mathrm{Hom}_{\mathbb{Q}[x]}\left(\mathbb{Q}[x]^{\oplus\infty} \otimes M,\ \mathbb{Q}[x] \otimes N\right)$$

$$\mathbb{Q}[x] \otimes \prod_{\infty} \mathbb{Q} \overset{?}{=} \prod_{\infty} (\mathbb{Q}[x] \otimes \mathbb{Q})$$

Does taking a tensor product commute with taking infinite products? No!

$\bigoplus_i x^i \otimes \prod_{\infty} \mathbb{Q}$ $\quad (a, x^i, a_2 x^i, \ldots)$

$(f_1(x), f_2(x), f_3(x), \ldots)$ $\quad f_i(x) \in \mathbb{Q}[x]$

$(f_1(x), f_2(x), \ldots)$ all f_i have degree $\leq I$ — bounded degree

unbounded degree

similar but nonequal

Lecture 29: Artinian modules

Recall: Noetherian:

(1) ascending chain condition for submodules $\quad M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$ finite

(2) every nonempty set of submodules has max. element

(3) every submodule is f.g.

Artinian:

(1) descending chain condition

property of points $\Updownarrow$ $\quad M_1 \supseteq M_2 \supseteq M_3 \supseteq \cdots$ stabilizes

(2) every nonempty set of submodules has minimal element

(3) ???

Examples

(1) Modules that are Artinian & Noetherian

0, $\mathbb{Z}/n\mathbb{Z}$ (over $\mathbb{Z}$), any module with finite number of elements, any finite dim v.s. over field

(2) Noetherian, not Artinian:

$\mathbb{Z}$ (over $\mathbb{Z}$) $\quad \mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset 8\mathbb{Z} \supset \cdots$

$\mathbb{Z}_{(2)} = \{\frac{a}{b} \mid b \text{ odd}\}$

(3) Neither Noetherian or Artinian

$\mathbb{Q}$ (over $\mathbb{Z}$) $\quad \cdots \supset \frac{1}{4}\mathbb{Z} \supset \frac{1}{2}\mathbb{Z} \supset \mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset \cdots$

(4) Artinian but not Noetherian (a bit weird...)

$\mathbb{Z}[\frac{1}{2}]/\mathbb{Z} \cong \mathbb{Z}/1\mathbb{Z} \subseteq \mathbb{Z}/2\mathbb{Z} \subseteq \mathbb{Z}/8\mathbb{Z} \subseteq \cdots$ union M

$a/2^n$

only proper submodules

Injective envelope $\mathbb{Z}/n\mathbb{Z}$

Dual to $\mathbb{Z}_{(2)}$

Rings: R Noetherian ring $\Leftrightarrow$ Noetherian R-module

R Artinian ring $\Leftrightarrow$ Artinian R-module

rest to "big"

Examples: $\mathbb{Z}$ Noetherian, not Artinian

$\mathbb{Z}[x_1, x_2, x_3, \ldots]$ ∞ variables $\rightarrow$ not Noetherian or Artinian

Artinian & Noetherian: $\mathbb{Z}/n\mathbb{Z}$, P.I.D/nonzero Ideal, $k[x]/(f(x))$

Noncommutative examples: $M_n(k)$, group rings of finite groups $k[G]$

any k-algebra that is a finite dim. v.s. over k.

$k[x,y]/$(ideal of finite codimension)

All Artinian rings are Noetherian

A module $M \neq 0$ is simple if only submodules are 0 and M

$\mathbb{Z}/p\mathbb{Z}$ $\quad$ k

Simple modules over R are $R/\mathfrak{m}$ for $\mathfrak{m}$ maximal ideal

M is called finite length if we can find

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n \subseteq M$$

M_i/M_{i-1} is simple $\qquad$ n = length of M

analogous to finite $\dim$ of v.s.

Example: (1) finite $\dim$ v.s.

(2) $\mathbb{Z}/p^n\mathbb{Z}$ $\quad$ $0 \subseteq \mathbb{Z}/p\mathbb{Z} \subseteq \mathbb{Z}/p^2\mathbb{Z} \subseteq \cdots \subseteq \mathbb{Z}/p^i\mathbb{Z}$

M finite length $\iff$ M Noetherian + Artinian

($\Rightarrow$) Simple $\Rightarrow$ Noetherian, Artinian

If $0 \to A \to B \to C \to 0$ exact, then

A, C Noetherian $\Rightarrow B$ Noetherian

A, C Artinian $\Rightarrow B$ Artinian

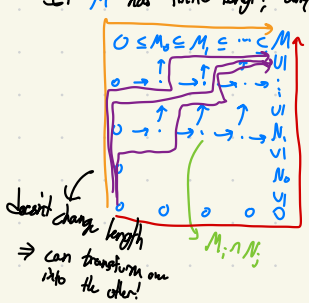
[A, C finite length $\Rightarrow B$ finite length]

($\Leftarrow$) $0 \subseteq M_1$ Minimal nonzero (Artinian $\Rightarrow$ minimum exists)

$0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = M$

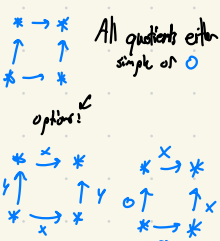
M_2 minimal $> M_1$ ↘ stops b/c Noetherian ∎

If M has finite length, any two maximal chains have same length



Could change length

⇒ can transform one into the other!



for any 2 chains with simple quotients, the number of times any given simple quotient is the same.

(1) Length of finite length module is well-defined
(2) Length is additive on exact sequences

$0 \to A \to B \to C \to 0$

$\text{length}(A) + \text{length}(C) = \text{length}(B)$

↓

dimension of vector space

similar to Jordan-Hölder

Lecture 25: Artinian Rings

Thm T.F.A.E. (for a ring)

(1) R is Noetherian and 0 is Π max
(2) R is Noetherian and all primes are maximal (R is 0-dimensional)
(3) R has finite length (as an R-module)
(4) R is Artinian

Pf: (1 ⇒ 2). $0 = m_1 m_2 \cdots m_n \subseteq \mathfrak{p}$

$\mathfrak{p}$ prime

So $\mathfrak{p}$ contains some m_i

$\Rightarrow \mathfrak{p} = m_i$

$\Rightarrow$ all prime ideals are maximal

(2 ⇒ 3) Suppose R not finite length

Choose I maximal so R/I not finite length

Show I prim: $S = R/I$, show S integral domain ($ab=0 \Rightarrow a=0$ or $b=0$)

S/a, S/b finite length if $a, b \neq 0$

S not finite length

$S/b \xrightarrow{\text{onto}} aS$ (finite length)

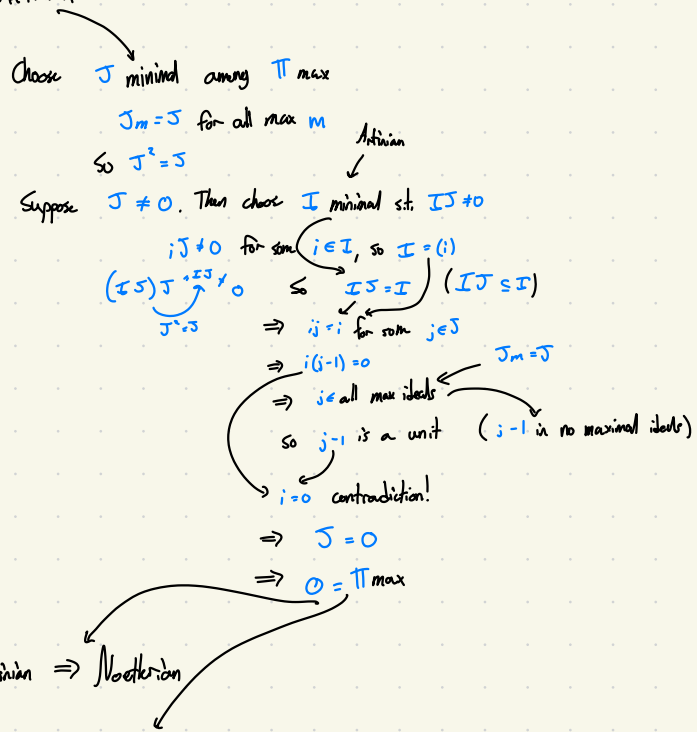
$S/b \cong S/\text{ann}(a)$ (finite length)

$0 \to aS \to S \to S/aS \to 0$

$\Rightarrow S$ finite length ×

(3 ⇒ 4) Did last time

(4 ⇒ 1) Artinian ⇒ $0 = \prod \text{max}$



Artinian ⇒ Noetherian

$0 = m_1 m_2 \cdots m_n$

$R \supseteq m_1 \supseteq m_1 m_2 \supseteq \cdots \supseteq m_1 \cdots m_n = 0$

each factor $m_1 \cdots m_i / m_1 \cdots m_{i+1}$ is v.s. over field R/m_{i+1}

R Artinian ⇒ all fields have finite dimension

Each factor has finite length so R has finite length so R is Noetherian ☑

$R = k[x,y]/(x^2, xy, y^2)$ → basis $(1, x, y)$

$m = (x,y)$ $\quad R \supseteq m \supseteq m^2 = 0$

R/m $\quad m/m^2$

dim 1 $\quad$ dim 2 over R/m $\quad (x,y)$

Corollary: any Artinian ring is a product of Artinian local rings (chinese remainder thm)

$0 = m_1^{k_1} \cdots m_n^{k_n}$ $\quad m_1, \ldots, m_n$ max

$R = R/m_1^{k_1} \times R/m_2^{k_2} \times \cdots$

↑ ↑ ↑

artinian local rings with one prime ideal

Discrete, finite

$\operatorname{Spec} R =$ m_1 m_2 m_3 m_4 m_5 m_6

Careful: converse not true (unless R is Noetherian)

$\left[R = k[x_1, x_2, \ldots]/(x_1^2, x_2^2, \ldots) \quad \operatorname{Spec} = \cdot \text{ but not Artinian}\right]$

↑ m

Lecture 26: Examples of Artinian rings

Artin $\Rightarrow$ product of local rings

$\mathbb{Z}/60\mathbb{Z} = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

Examples of Artin rings. ↙ Artin local ring, unique max ideal $R/m = k$

Length 0: 0

Length 1: k

Length 2: $k[x]/(f(x)) = k[x]/(x^2 + ax + b)$ ← deg 2

$k[x]/(x^2) \qquad k[x]/((x-\alpha)(x-\beta)) = k \times k$

irred quadr

$k[x]/(f(x)) = K \supset k$

$\mathbb{Q}[i] = \mathbb{Q}[x]/(x^2+1)$

$\cup|$

$\mathbb{Q}$

$\mathbb{Z}/p^2\mathbb{Z}$ length 2, $k = \mathbb{Z}/p\mathbb{Z}$

Length 3: $k \times k \times k \qquad k[x]/(x^2) \times k \qquad K$

$k[x,y]/(x^2, xy, y^2)$ Basis $(1, x, y)$

Length 4: $R \supseteq m \supseteq m^2 \supseteq m^3 = 0$

↑ dim 3 ↑ dim 1

$m/m^2 \xrightarrow{\times x+y^2} m^2/m^3 \cong k$

dim 2 dim 1

Quadratic form

Length $\geq 5, 6$: Complicated, really.

nilpotent

$R \supseteq m$ $m^n = 0$ for some n

→ Artin rings

→ Nilpotent Lie algebras

→ finite p-groups → # of order 2^{10} is 49487365422

What is dim of space of Artin rings over k with dimension n, m generators

$$k[x_1, x_2, \ldots, x_m] / I$$ ← codim n

Take n distinct pts in $\mathbb{A}^m = k^m$

I = all polys vanishing on n pts

→ mn-dim space of Artin rings

$m=1$: trivial. $I = (x^n + a_{n-1}x^{n-1} + \cdots + a_0)$

$m=2$: true.

$m=3$: fails! More ideals of codim n than would expect

$k[x_1, x_2, x_3]$ $m=3$

$M = (x_1, x_2, x_3)$

$M^i \supseteq I \supseteq M^{i+1}$ $(i > 0)$

Any subspace I like this is ideal

codim $= O(i^3) \sim n$ $m=3$

$\dim M^i / M^{i+1} = O(i^2)$

$\dim$ (subspaces of M^i / M^{i+1}) $= O(i^4)$

↑ Grassmannian

codim I $= O(i^3)$

$mn = O(i^3) < O(i^4)$

$\mathbb{R}[\sqrt{-1}]$

$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} = \prod$ Artin local rings

$= \mathbb{C} \times \mathbb{C}$

↑ idempotents

$\frac{1\otimes 1 + i\otimes i}{2}$ $\frac{1\otimes 1 - i\otimes i}{2}$

$\mathbb{Q}[\sqrt{2}] \otimes_{\mathbb{Q}} \mathbb{Q}[\sqrt{3}] \to$ field $\mathbb{Q}[\sqrt{2},\sqrt{3}]$

$k \otimes_k L$ k or L separable finite extension

L separable:

$L = k[x]/(f(x))$ f no multiple roots in $\bar{L}$

$k \otimes_k L = k[x]/(f(x))$ ← f may split in k

$f(x) = f_1(x) f_2(x) \cdots$

↑ ↗ ↑

coprime

$= k[x_1]/(f_1(x)) \times k[x_2]/(f_2(x)) \times \cdots =$ product of fields

Not separable: $K = k[\sqrt[p]{a}]$ k has char $p > 0$

$L = k[\sqrt[p]{a}]$ a not a p^{th} power

$L = k[x]/(x^p - a)$ $x^p - a$ irreducible

$K \otimes_k L = k[x]/(x^p - a)$

$K = k[b]$, $b^p = a$

$(x-b)^p$ ← artin local ring not (yet) a field (s)

$= k[x]/(x-b)^p$ ↑ nilpotent element ↖ large # of multiple factors

$k(x) \otimes_k k(y)$ not artinian!

Lecture 27: Associated Primes

Module M, set of associated primes $Ass(M)$

M finite length

$0 = M_0 \subset \underbrace{M_1 \subset M_2}_{M_i/M_{i-1} \text{ simple: } R/\text{max}} \subset \cdots \subset M_n = M$

Can we find analogs for f.g. modules?

over arbitrary rings, not really.

So assume R Noetherian

$R = \mathbb{Z}$

M = f.g. abelian group $= \mathbb{Z}^n \oplus \bigoplus_{p \text{ prime}} \left(\bigoplus_{n_i} \mathbb{Z}/p^{n_i}\mathbb{Z} \right)$

$\mathbb{Z}/p\mathbb{Z}$ $\quad$ $\mathbb{Z}_{(p)}$

$\mathbb{Z}_{(0)} \to$ prime $\quad$ $\downarrow$ prime

Can we break M into modules of form $R/\mathfrak{p}$, $\mathfrak{p}$ prime ideal?

$0 = M_0 \subset M_1 \subset \dots \subset M_n = M$

$M_{i+1}/M_i \cong R/\mathfrak{p}_i$ prime $\mathfrak{p}_i$

Yes! Assume $M \neq 0$. Show M has submodule $\cong R/\mathfrak{p}$ for $\mathfrak{p}$ prime

Pick ideal $\mathfrak{p} \subseteq R$ maximal among ideals such that $R/\mathfrak{p} \subseteq M$

$\mathfrak{p} = \mathrm{Ann}(a)$ $a \in M$

We show $\mathfrak{p}$ is prime. If not, can find $x, y \notin \mathfrak{p}$ s.t. $xy \in \mathfrak{p}$

look at image $\bar{x}$ of x in M $\quad$ $R/\mathfrak{p} \subseteq M$ $\quad$ $x \mapsto \bar{x}$

$\mathrm{Ann}(\bar{x})$ ideal of R

contains $\mathfrak{p}$, y ($\hookrightarrow xy \in \mathfrak{p}$) so is strictly bigger than $\mathfrak{p}$ and not R ($\hookrightarrow y \notin \mathfrak{p}$, $x \notin \mathfrak{p}$, $\bar{x} \neq 0$)

contradicts choice of $\mathfrak{p}$ so $\mathfrak{p}$ prime

$M \neq 0$ $\quad$ $0 \subset \overbrace{M_1}^{\cong R/\mathfrak{p}_1} \subset M_2 \subset M_3 \subset M_4 \subset \dots = M$ $\quad$ stops b/c M Noetherian

$M_1 \subseteq M$ $\quad$ M/M_1

$M_1 \cong R/\mathfrak{p}_1$ contains $R/\mathfrak{p}_2$

$\mathfrak{p}_1$ prime $\quad$ M_2 = inverse image of $R/\mathfrak{p}_2$

How often does $R/\mathfrak{p}$ occur in M - multiplicity of $R/\mathfrak{p}$ in M

M finite length: mult = # of times $R/\mathfrak{p}$ occurs in any maximal chain

Additive: $0 \to A \to B \to C \to 0$

$\mathrm{Mult}(R/\mathfrak{p}, A) + \mathrm{Mult}(R/\mathfrak{p}, C) = \mathrm{Mult}(R/\mathfrak{p}, B)$

$M = \mathbb{Z} + \mathbb{Z}/2\mathbb{Z}$

$\mathrm{Mult}(\mathbb{Z}/(0), M) = 1$

$\mathrm{Mult}(\mathbb{Z}/2\mathbb{Z}, M) = 1$?

Universal counter example: $0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$

$\mathrm{Mult}\ \mathbb{Z}/2\mathbb{Z}$ $\quad$ 0 $\quad$ 0 $\quad$ 1

$\mathrm{Mult}(\mathbb{Z}/(0), M)$ is well defined

$= \dim_{\mathbb{Q}}(M \otimes \mathbb{Q})$

$M = \mathbb{Z}^n \oplus$ finite

$M \otimes \mathbb{Q} = \mathbb{Q}^n \oplus 0$ $\dim = n$

$\dim_{\mathbb{Z}/2\mathbb{Z}}(M \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z})$ ↑ not additive

$\otimes \mathbb{Z}/2\mathbb{Z}$ does not preserve exactness

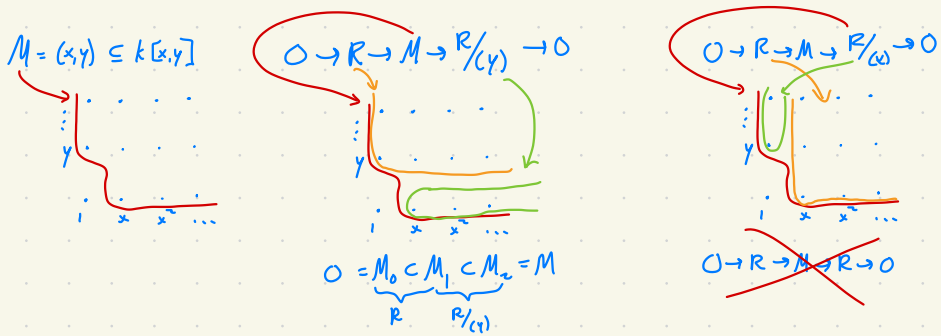
Mult of $\mathbb{Z}/(p)$ in M:

Is additive for $(p)=(0)$

Not additive for (or multiplicity) $(p) \neq 0$

Is additive for any p for finite groups

[Mult $R/\mathfrak{p}$ is additive for modules s.t. $Ass(M)$ has no elements strictly smaller than $R/\mathfrak{p}$]



Def $Ass(M)$ = set of prime that are annihilators of elements of M.

= ideals $\mathfrak{p}$ prime s.t. $R/\mathfrak{p} \cong$ submodule of M

R Noetherian, M f.g. $M \neq 0 \Rightarrow Ass(M) \neq 0$

Informally, $Ass(M) = \mathfrak{p}$ s.t. $R/\mathfrak{p}$ "definitely" occurs in M

$Ass(\mathbb{Z}) = \{(0)\}$

$Ass(\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}) = \{(0), (2)\}$

$Ass((x,y)) = \{(0)\}$

$0 \to A \to B \to C \to 0$

$Ass(B)$ $Ass(A)$ $Ass(C)$

Is $Ass(B) = Ass(A) \cup Ass(C)$

$0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$

Ass: (0) (0) (2)

$Ass(A) \subseteq Ass(C)$ obvious

$Ass(B) \subseteq Ass(A) \cup Ass(C)$

Suppose $R/\mathfrak{p} \cong$ submodule X of B

$X \cap A = \{0\}$ ↳ $X \cong$ submodule of $\mathfrak{p} \in Ass(C)$

$X \cap A \neq \{0\}$ ↳ Pick $a \neq 0$ in X, $a \in A$

$Ann(a) = \mathfrak{p} \rightarrow \mathfrak{p} \in Ass(A)$

$Ann(x)$, $x \neq 0$, $x \in R/\mathfrak{p}$ is $\mathfrak{p}$ (↑ integral domain)

M f.g. over R Noetherian

Consequences:

(1) $Ass(M)$ is finite

$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$

$M_{i+1}/M_i = R/\mathfrak{p}_i$ (↑ only associated prime is $\mathfrak{p}_i$)

$Ass(M) \subseteq \{\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_n\}$ (not necessarily equal; ↙ finite)

(2) $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$

M_{i+1}/M_i of form $R/\mathfrak{p}_i$ $\mathfrak{p}_i$ prime

Any element $\mathfrak{p} \in Ass(M)$ occurs in this chain

Lecture 28: Geometry of associated primes

M is f.g. over Noetherian ring R

$Ass(M) =$ primes $\mathfrak{p}$ s.t. $R/\mathfrak{p} \subseteq M$ (↑ finite)

$0 = M_0 \subseteq M_1 \subseteq \underbrace{M_2 \subseteq \cdots \subseteq M_n}_{M_{i+1}/M_i = R/\mathfrak{p}_i \ \mathfrak{p}_i \text{ prime}} = M$

$M = (x,y) \subseteq R = k[x,y]$

$Ass(M) = (0)$

M is torsion free over integral domain $R \rightarrow Ass(M) = (0)$

$R = \mathbb{Z}[\sqrt{-5}]$

$M = (2, 1+\sqrt{-5})$

Spec R = set of primes

∪

Ass (M)

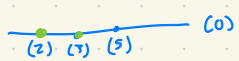
Support of M $\quad$ Supp (M) = set of primes $\mathfrak{p}$ with $M_{\mathfrak{p}} \neq 0$ ($M_{\mathfrak{p}}$: module over $R_{\mathfrak{p}}$)

= set of primes containing $\mathrm{Ann}(M) \subseteq R$

Ass (M) "detects" this

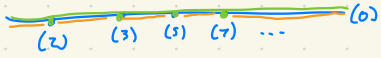
$R = \mathbb{Z}$ $\quad M = \mathbb{Z}/12\mathbb{Z}$

Spec R



Ass (M) = Supp (M) = $\{(2), (3)\}$

$M = \mathbb{Z}$



Supp (M) = Spec $(\mathbb{Z})$

Ass (M) = (0)

$M = \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

Supp (M) = Spec $\mathbb{Z}$

Ass (M) = $\{(0), (2)\}$

more info than minimal ↑ embedded ↑

for f.g. modules over Noetherian rings,

Supp $(M) = \overline{\mathrm{Ass}(M)}$

(1) $\mathfrak{p} \in \mathrm{Ass}(M) \Rightarrow \mathfrak{p} = \mathrm{Ann}(a)$ $\quad a \in M$

$\Rightarrow \mathfrak{p} \supseteq \mathrm{Ann}(M) \Rightarrow \mathfrak{p} \in \mathrm{Supp}(M)$

(2) $\mathfrak{p} \in \mathrm{Supp}(M) \Rightarrow M_{\mathfrak{p}} \neq 0$

Look at $\mathrm{Ass}(M_{\mathfrak{p}}) \neq 0$

Pick $q \in \mathrm{Ass}(M_{\mathfrak{p}})$ $\quad q \in \mathrm{Spec}(R_{\mathfrak{p}})$

$f: R \to R_{\mathfrak{p}}$

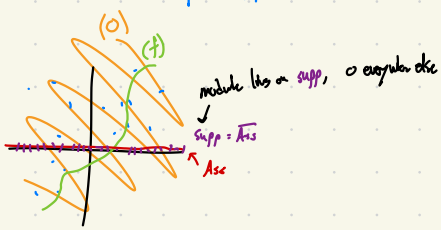
f^{-1}: Spec $R \leftarrow$ Spec $R_{\mathfrak{p}}$ $\quad f^{-1}(q) \in \mathrm{Ass}(M)$

contained in $\mathfrak{p}$

So $\mathfrak{p} \in \overline{f^{-1}(q)}$

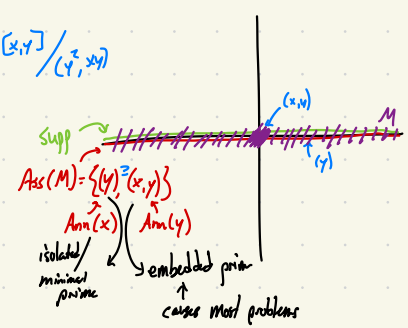
$R = k[x,y]$

Spec R



$M = k[x,y]/(y)$

$M = k[x,y]/(y^2, xy)$



$M = k[x,y]/(y)$

Ass (M) = (y)

Coprimary decomposition of M → Break up M into modules, each associated to one element of $Ass(M)$

Over $\mathbb{Z}$, A = f.g. abelian group

$A = A_0 \oplus A_2 \oplus A_3 \oplus \cdots$ (unique)

$A_0 \cong \mathbb{Z}^n$ (not unique)

A_2: 2-group, A_3: 3-group

$A = \mathbb{Z} \oplus \mathbb{Z}/_{2\mathbb{Z}}$

$Ass(\mathbb{Z}^n)$: (0) (n)

Ass: (2)

Ass: (3)

(1,0)

(1,1) non uniqueness caused by embedded primes

↖ if non-empty ↗

Can we write $M = \bigoplus_i M_i$ M_i has exactly one associated prime?

Nope :(

$M = R/(y^2, xy) \longrightarrow R/(y) \oplus R/(x,y^2)$

$1, x, x^2, x^3, \ldots$ $1, y$

y

M submodule of $\bigoplus M_i$

coprimary decomposition ↑ coprimary modules

Sum over $Ass(M)$

Lasker-Noether thm: If I an ideal of R (Noetherian)

Then I is $\bigcap$ (finite) of primary ideals

(former) world chess champion ↑ (Lasker) ↑ proved then while champ

J s.t. if $xy \in J$ then $x \in J$ or $y^n \in J$ for some n

R/J: every zero divisor is nilpotent (would be zero in a prime ideal)

In $\mathbb{Z}$, primes: $(0), (p)$

primary ideals: $(0), (p^n)$

Lecture 29: Lasker-Noether Theorem

M f.g. module over Noetherian ring R

coprimary $\iff$ M has ≤ 1 associated prime

$M \leq \bigoplus_{p \in Ass(M)} M_p$ ← coprimary

What is a ~~primary~~ module? doesn't exist

(1) If $I \subseteq R$ then I is a finite $\bigcap$ of primary ideals J

$xy \in J \Rightarrow x \in J$ or $y^n \in J$ for some $n \in \mathbb{N}$

(2) $N \subseteq M$ R-modules

Then N is finite $\bigcap$ of primary submodules

X is called primary submodule of M if

Lasker's def (but for modules not ideals) $\begin{cases} rm \in X \Rightarrow m \in X \text{ or } r^n M \subseteq X \text{ for some } n > 0 \\ r \in R \\ m \in M \end{cases}$

This is a property of quotient $M/X = Y$

$\begin{cases} \text{If } ry = 0 \text{ for some } y \neq 0 \text{ then } r^n y \text{ for some } n > 0 \\ \text{(or zero divisor)} \end{cases}$

$\Rightarrow$ Y is coprimary

(3) $M \subseteq \prod_{\mathfrak{p} \in Ass(M)} M_{\mathfrak{p}}$ (coprimary)

(2) $\Rightarrow$ (3): $N = 0$ primary submodule

$0 = \bigcap J_{\mathfrak{p}}$

$M \to \prod (M/J_{\mathfrak{p}})$ injective

↳ primary submodule & coprimary module

Coprimary:

(1) At most 1 associated prime

(2) $rm = 0 \Rightarrow m = 0$ or $r^n M = 0$ $(n > 0)$

(2) $\Rightarrow$ (1) Suppose $n \neq 0$ $m \in M$ prob $\mathfrak{p} = Ann(m)$

(2) $\Rightarrow$ $\boxed{P \subseteq \sqrt{Ann(M)}}$

If $\mathfrak{p}$ prime $Ann(M) \subseteq Ann(m) \subseteq \mathfrak{p}$

so $\boxed{\sqrt{Ann(M)} \subseteq \mathfrak{p}}$

So if $\mathfrak{p} \in Ass(M)$, $\mathfrak{p} = \sqrt{Ann(M)}$

So there is at most one associated prime.

otherwise take $R' = R/\mathrm{Ann}(M)$

(1) $\Rightarrow$ (2) (Assume $\mathrm{Ann}(M)=0$)

Pick $\mathfrak{p}$ an (only) associated prime of M

Contains $\mathrm{Ann}(m)$, $m \neq 0$

So just need to show $\mathfrak{p}$ is nilpotent $\Leftarrow$ (2)

Suppose $a \in \mathfrak{p}$ is not nilpotent

Then $M[a^{-1}]$ is nonzero

$x \in m$ is 0 in $M[a^{-1}]$ then $xa^n = 0$ for some n

$M[a^{-1}] = 0 \Rightarrow a^n \in \mathrm{Ann}(M) = 0$ for some n so a nilpotent

$M[a^{-1}] \neq 0 \Rightarrow \mathrm{Ass}(M[a^{-1}]) \neq \emptyset$ (primes of $R[a^{-1}]$)

pick $T \in \mathrm{Ass}(M[a^{-1}])$ (primes of $R[a^{-1}]$)

Q = inverse image of T in R

$$\begin{array}{ccc} R & \to & R[a^{-1}] \\ \cup & & \cup \\ Q & \to & T \end{array} \quad \text{(primes)}$$

Q = union $\mathrm{Ann}(m) \subseteq \mathrm{Ann}(ma) \subseteq \mathrm{Ann}(ma^2) \subseteq \dots$

$= \mathrm{Ann}(ma^n)$ for some n

so $Q \in \mathrm{Ass}(M)$ but $a \in \mathfrak{p}$, $a \notin Q$

so $\mathfrak{p} \neq Q$ so M has at least 2 associated primes $\times$

Proof of Lasker–Noether thm

$M \subseteq \bigcap M_{\mathfrak{p}}$ (coprimary)

Proof: If not true, pick maximal submodule N s.t. M/N not contained in (finite) product of coprimary ideals

May assume $N = 0$

(1) M not coprimary

So it has 2 submodules

$M_1 \cong R/\mathfrak{p}_1$ $\quad$ $M_2 \cong R/\mathfrak{p}_2$ $\quad$ $\mathfrak{p}_1 \neq \mathfrak{p}_2$

$\mathrm{ann}(x) = \mathfrak{p}_1$ $(x \neq 0)$ $\quad$ $\mathrm{ann}(x) = \mathfrak{p}_2$ $(x \neq 0)$

$M_1 \cap M_2 = 0$

$M_1 \cap M_2 \to M \xrightarrow{\text{inj}} M/M_1 \oplus M/M_2 \subseteq$ finite product of coprimaries — ✗ ☒

$M = R/I \subseteq \prod (R/I_\mathfrak{p})$ ← coprimary, ↳ primary

$\Rightarrow I = \bigcap I_\mathfrak{p}$

Lecture 30: Symbolic Powers

Lasker-Noether: $I \subseteq R$ Noetherian

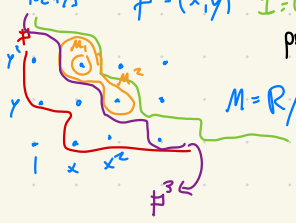
$I = \bigcap$ primary ideals

Primary Ideals? (0), $(p^n) = (p)^n$

Are prime ideals the same as powers of primes? No!

Primary ideals need not be $(p)^n$

$R = k[x,y]$ $\mathfrak{p} = (x,y)$ $I = (y^3, x^2y^2, x^3y, x^6)$ primary



$M = R/I$ $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_{10} = M$

only associated prime of M is $R/\mathfrak{p}$ so R/I is coprimary so I is primary

Warning: do not confuse

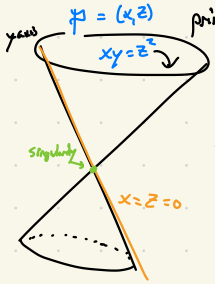
(1) $\mathfrak{p} = (x,y)$ as coprimary module w/ Ass prime (0)

(2) $\mathfrak{p} = (x,y)$ as prime ideal, coprimary module $R/\mathfrak{p}$ w/ ass prime $\mathfrak{p}$

(3) A power $\mathfrak{p}^n$ that is not primary

$R = k[x,y,z]/(xy - z^2)$

$\mathfrak{p} = (x,z)$ prime: $R/\mathfrak{p} \cong k[y]$ integral domain



$\mathfrak{p}^2$ not primary!

$R/\mathfrak{p}^2 : k[x,y,z]/(x^2, xz, z^2, xy)$

y is zero divisor $yx = 0$

y not nilpotent $1, y, y^2, \ldots$ linearly ind.

So $\mathfrak{p}^2$ not primary

primary decomposition: $\mathfrak{p}^2 = (x, z^2) \cap (x, y, z)^2$ ← embedded prime

primary for $\mathfrak{p}$: (x,z) — primary for (x,y,z)

$R/(x,z^2) \cong k[y,z]/(z^2)$ — $\mathrm{Ass}(\mathfrak{p}^2)$

Suppose $\mathfrak{m}$ maximal in R

Any ideal I with $\mathfrak{m} \supseteq I \supseteq \mathfrak{m}^n$ $(n \geq 1)$

is primary R/I has maximal $\mathfrak{m}/I$ → nilpotent $\mathfrak{m}^n \in I$

so $\left(\frac{\mathfrak{m}}{I}\right)^n = 0 \in R/I$

So all zero-divisors are nilpotent

So I is primary

Special case: $\mathfrak{m}^n$ primary iff $\mathfrak{m}$ is maximal

Symbolic Powers

$\mathfrak{p} \subseteq R$ prime $f: R \to R_{\mathfrak{p}}$

$\mathfrak{p}R_{\mathfrak{p}}$ is maximal

$f^{-1}(\mathfrak{p}^n R_{\mathfrak{p}})$ $(\mathfrak{p}R_{\mathfrak{p}})^n = \mathfrak{p}^n R_{\mathfrak{p}}$ is primary

primary → inverse of primary ideal is primary

elements s.t. $xy \in \mathfrak{p}^n$ — turn it into something primary

for some $y \notin \mathfrak{p}$

called nth symbolic power $\mathfrak{p}^{(n)}$

$R = k[x,y,z]/(xy - z^2)$ $\mathfrak{p} = (x,z)$ $\mathfrak{p}^2 = (x^2, xz, z^2)$

$\mathfrak{p}^{(2)} = (x, z^2)$

$\mathfrak{p}^{(2)} \supseteq \mathfrak{p}^2$

$\ni x \notin$

$xy \in \mathfrak{p}^2$ $y \in \mathfrak{p}$

$= z^2$

$(x,z) \subseteq (x,y,z)$

$(x,z)^{(1)} = (x,z^2)$ $\not\supseteq (x,y,z)^{(2)} = (x,y,z)^2$

x vanishes to order 2 along y-axis but is not generated by products of 2 elements vanishing to order 1

$\mathfrak{p}^{(n)}$ = "functions vanishing to order n along $\mathfrak{p} = 0$"

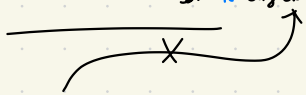
Lecture 31: Nullstellensatz

Nullstellensatz
zero position theorem

Weak Nullstellensatz: (1) What are the maximal ideals of $k[x,y,\dots]$

obvious ones: $(x-a, y-b, \dots) \leftrightarrow (a,b,\dots) \in k^n$

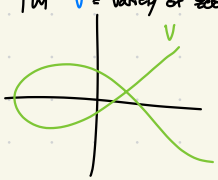
If k algebraically closed, this gives all maximal ideals.



$k = \mathbb{R}$ $\quad \mathbb{R}[x] \supseteq (x^2+1)$ is max ideal

Strong Nullstellensatz: (2) Suppose I is an ideal of $k[x,y,\dots]$

Put V = variety of zeros



What is ideal J of elements vanishing on V?

$I \subseteq J$

$k[x] \supseteq I = (x^3)$

$V = \{0\}$ $\quad J = (x) \neq I$

$x^3 \in I$ but $x \notin I$

If $f^n \in I$, then f vanishes on V so $f \in J$

So $\sqrt{I} \subseteq J$

Strong Nullstellensatz: $\sqrt{I} = J$ for k algebraically closed

J/I = nilradical of R/I

= nilpotent elements

J can be really hard to find

Example: Space of nilpotent matrices

$$X = \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{n1} & \cdots & x_{nn} \end{pmatrix}$$

X nilpotent $\Leftrightarrow X^n = 0$

$I \subseteq k[x_{11}, \ldots, x_{nn}]$ generated by coeffs. of x^n

Zero set of I = nilpotent matrices

Other functions vanishing on V:

$$x_{11} + x_{22} + \cdots + x_{nn}$$

X nilpotent $\Rightarrow$ all eigenvalues 0

$\Rightarrow$ $0 = \text{trace} = \sum$ eigenvalues

Characteristic poly: $\det(\lambda I - x)$

$= \lambda^n$ for x nilpotent

So all coeffs of $\det(\lambda I - x)$ of λ^i $i < n$ also vanish on V.

$$X = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$x^2 = \begin{bmatrix} a^2+bc & (a+d)b \\ (a+d)c & d^2+bc \end{bmatrix}$$

$I = (a^2+bc, (a+d)b, (a+d)c, d^2+bc)$

$\sqrt{I}$? Not obvious.

$a+d \in \sqrt{I}$

$(a+d)^k \in I$ for some k. What is k?

$k = 2$?

$(a+d)^2 \notin I$

$(a+d)^3 \in I$ I contains $(a+d) \times \{b, c, a-d, a^2, d^2\}$

$(a+d)^2$ is ideal generated by $a^2+2bc+d^2, (a-d)^2$

$(a+d)(a^2+bc) - (a+d)bc$

$\det \quad ad - bc = (a+d)d - (bc+d)$

trace, in I

radical $\sqrt{I} = (a+d, ad-bc)$

$k[a,b,c,d]/(a+d, ad-bc)$

$= k[a,b,c]/(a^2+bc)$ No zero divisors ✓

($\Rightarrow$ no nilpotent elements)

Example: $X = \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{n1} & \cdots & x_{nn} \end{pmatrix}$ $\quad Y = \begin{pmatrix} y_{11} & \cdots \\ \vdots & \ddots \end{pmatrix}$

I = ideal of $k[x_{11}, \ldots, y_{nn}]$ generated by coeffs of $XY - YX$

V = pairs of commuting matrices

$\sqrt{I} \stackrel{?}{=} I$ we actually don't know...

Proof (weak): (working over $\mathbb{C}$)

m = max ideal of $\mathbb{C}[x_1, \ldots, x_n]$

$\mathbb{C}[x_1, \ldots, x_n]/m$ is f.g. extension of $\mathbb{C}$ and a field

$\mathbb{C}$ so $x_i = a_i$ in $\mathbb{C}$ as $\mathbb{C}$-algebra; countable dim as $\mathbb{C}$-vectorspace $\Rightarrow$ algebraic

$x_i - a_i \in m$

$m = (x_1 - a_1, \ldots)$

So is $\mathbb{C}$ as $\mathbb{C}$ is algebraically closed

If a is transcendental over $\mathbb{C}$

$\frac{1}{a - \alpha}$ for $\alpha \in \mathbb{C}$ (uncountable)

would be uncountable # of lin. ind. elements

(in $n+1$ vars) (in n vars)

Proof (Weak $\Rightarrow$ Strong): I = ideal in $k[x_1, \ldots, x_n]$

V = zero set

f vanishes on V want to show $f^m \in I$ for some m

$f x_0 = 1$ look at $(I, 1 - x_0 f)$ in $k[x_0, \ldots, x_n]$

↑ no common roots so not in any max ideal by weak Nullstellensatz so it is $k[x_1, \ldots, x_n]$

Rabinowitsch trick

So $1 = a_1 b_1 + \cdots + a_s b_s + a(1 - x_0 f)$

$a_1 b_1 + \cdots + a_s b_s$ in I; $a(1 - x_0 f)$ in $k[x_0, \ldots, x_n]$

Put $f = \frac{1}{x_0}$ in $k(x_0, \ldots, x_n)$

$1 = a_1 b_1 + \cdots + a_s b_s$ $\quad a_i \in k[x_1, \ldots, x_n, \frac{1}{f}]$

$a_i = c_i / f^m$

$f^m = c_1 b_1 + \cdots + c_s b_s$

$\in I$ ∎

Lecture 32: Zariski's Lemma

Nullstellensatz

weak: max ideals of $k[x_1,\dots,x_n]$ are $(x_1-a_1,\dots,x_n-a_n)$

strong: $I \subseteq k[x_1,\dots,x_n]$ $\quad V = \{\text{zeros of } I\}$

$f=0$ on $V \iff f^k \in I$

Key point: Zariski's Lemma:

Suppose field K is f.g. as algebra over k

then it is f.g. as a module

Proved last lec. for $k=\mathbb{C}$

Proof idea: picked $K = k(x_1,\dots,x_m)$

Generators of algebra K of form $\frac{f_i(x_1,\dots,x_m)}{g_i(x_1,\dots,x_m)}$

all poles are factors of g_i

Proof K generated by $\underbrace{x_1,\dots,x_m}_{\text{algebraically ind.}}, \underbrace{x_{m+1},\dots,x_n}_{\text{algebraic over } k[x_1,\dots,x_m]}$

$m=0$: done.

So assume $m>0$. Ring $k[x_1,\dots,x_m]$ has infinite # of irreducibles (up to units)

k infinite: $x_1-\alpha$ $\alpha\in k$

k finite: copy Euclid's proof for $\mathbb{Z}$

Each $x_{m+1},\dots,x_n$ is a root of nonzero polynomial, coeffs in $k[x_1,\dots,x_m]$

Leading coeffs $b_{m+1},\dots,b_n$ ← "poles" of $x_{m+1},\dots,x_n$

$x_{m+1},\dots,x_n$ are integral over $k\left[x_1,\dots,x_m,\frac{1}{b_{m+1}},\dots,\frac{1}{b_m}\right]$ ← localization

So k is finite (as module) over this

Pick irreducible poly $f\in k[x_1,\dots,x_n]$ ← new pole

not dividing $b_{m+1},\dots,b_n$

$k[x_1,\dots,x_m,f^{-1}] \subseteq K$ ← finite $k[x_1,\dots,x_m]$ module

↑ finite over $k[x_1,\dots,x_m]$

$1 \subset \langle 1,f^{-1}\rangle \subset \langle 1,f^{-1},f^{-2}\rangle \subset \cdots$

$f^{-m} = a_0 + a_1 f^{-1} + \cdots + f^{1-n} \implies m=0$

$f^{-1} = a_0 f^{n-1} + \cdots + a_{n-1}$

Weak Nullstellensatz

$k[x_1,\dots,x_n]/\text{max ideal}$ ← f.g. as module/k (by Zariski:)
(k alg. closed)

So it is k as k alg closed ⇒ no intermediate extensions

So $x_i = \text{some } a_i \pmod{\text{max ideal } m}$

$a_i \in k$

$m \supseteq (x_1 - a_1, x_2 - a_2, \dots)$ ∎

If $f: A \to B$ hom of f.g. algebras/k
then f^{-1}(maximal ideal) is maximal

[(Counter)example: $f: k[x] \to k(x)$
$f^{-1}(0) = 0$]

$f: A \to B$

$k \subseteq A/f^{-1}(m) \to B/m$ f.g. k-module by Zariski

↑ contained in finite extension of field k so is a field.

So $f^{-1}(m)$ is maximal

Weak Nullstellensatz ⇒ Strong Nullstellensatz

$I \subseteq k[x_1,\dots,x_n]$ $f=0$ on V (zero set of I in k^n)

Look at localization $k[x_1,\dots,x_n,f^{-1}]$

set of max ideals ⊆ max ideals of $k[x_1,\dots,x_n]$

$f \notin m$ ($(x_1-a_1,\dots,x_n-a_n)$)

~ "$f \neq 0$"

So $I[f^{-1}]$ not in any max ideal of $k[x_1,\dots,x_n,f^{-1}]$

So is whole ring

So $1 \in I[f^{-1}] = \left\{ i/f^k \right\}$ $k \geq 1$ $i \in I$ ∎

Lecture 33: Integral elements

S is R-algebra. $s \in S$ integral over R

if $s^n + r_{n-1}s^{n-1} + \dots + r_0 = 0$ $r_i \in R$

$R = \mathbb{Z}$ $\quad S = \mathbb{Q}$

$s = \frac{a}{b}$ $\quad \left(\frac{a}{b}\right)^n + r_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + r_0 = 0 \quad r_i \in \mathbb{Z}$

$a, b \in \mathbb{Z}$

$(a,b) = 1$ $\quad a^n + \left(r_{n-1}a^{n-1}b + \cdots + r_0 b^n\right) = 0$

If $p \mid b$ some prime, then $p \mid a$ so b unit, meaning $\frac{a}{b} \in \mathbb{Z}$ $\quad (\mathbb{Z} \to$ ufd, $\mathbb{Q} \to$ field of quotients$)$

Properties: S integral $\Rightarrow R[S]$ finite (as R-module)

Generated as a module by

$1, s, s^2, \ldots, s^{n-1}$

$(s^n = r_{n-1}s^{n-1} + \cdots + r_0)$

If S finite over R (as module)

then all elements of S are integral

R Noetherian:

$\langle 1 \rangle, \langle 1, s \rangle, \langle 1, s, s^2 \rangle, \ldots, \langle 1, s, \ldots, s^{n-1} \rangle = \langle 1, s, \ldots, s^n \rangle$

$\Rightarrow \quad s^n$

$\Rightarrow \quad s^n = r_0 + r_1 s + \cdots + r_{n-1}s^{n-1}$

Cayley-Hamilton thm:

Any endomorphism φ of f.g. R-module M is integral

Proof: Suppose M generated by $m_1, \ldots, m_n$ ← not a basis!

φ given by some $n \times n$ matrix ← not unique!

so $\left(\begin{pmatrix} \varphi & & & \\ & \varphi & & \\ & & \ddots & \\ & & & \varphi \end{pmatrix} - A\right)\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0$

matrix with entries in $R[\varphi]$

Matrix $\times$ Adjoint $=$ det $\times \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$

So $\det\left(\begin{pmatrix} \varphi & & & \\ & \varphi & & \\ & & \ddots & \\ & & & \varphi \end{pmatrix} - A\right)$

acts as 0 on $\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$

so as 0 on M

det is polynomial in φ, coeffs in R

Leading coeff 1 (φ^n)

So φ root of $\det\left(\begin{pmatrix}\varphi & & \\ & \varphi & \\ & & \varphi\end{pmatrix} - A\right)$

So φ integral.

IP S finite over R

all elements of S are integral

$M = S$ if $s \in S$, φ = endomorphism, multiplication by s

$s: S \to S$

So s is integral over R

So S finite over $R \iff S$ generated (as algebra) by finite # of integral elements

($\Rightarrow$) done. All elements of S are integral

($\Leftarrow$) Given 2 finite subalgebras of S, S_1, S_2

then S_1, S_2 generate finite subalgebra

f.g. as module

$S_1 = (a_1, \dots, a_m)$ $S_2 = (b_1, \dots, b_n)$

$S_1, S_2 \leq \langle \{a_i b_j\} \rangle$

Integral nice with $+, \times$

Example:

$R = \mathbb{Z}$ $S = \mathbb{C}$

integral elements of $\mathbb{C}$ over $\mathbb{Z}$

= algebraic integers

form a ring

$\sqrt{2} + \sqrt[3]{2} + \sqrt[5]{2}$

find a poly in $\mathbb{Z}[x]$ with this as a root

No thanks. It has degree 30. But exists b/c integral elements

Normalization: if S is integral closure (all elements integral over R) of R in field of quotients

S is called normalization of R

Example: normalization of $\mathbb{Z}[\sqrt{5}]$

field of quotients: $\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5}\}$

$\subseteq$ Normalization contains $\{m + n\sqrt{5},\ n, m \in \mathbb{Z}\}$

$m + \sqrt{5}n \in S$

$\Rightarrow m - \sqrt{5}n \in S$

$\Rightarrow 2m \in S$ so in $\mathbb{Z}$

$m = \frac{1}{2}$? $\quad \frac{1+\sqrt{5}}{2} = \varphi \qquad \varphi^2 = \varphi + 1$

So normalization of $\mathbb{Z}[\sqrt{5}]$ is $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$

Same for $\mathbb{Z}[\sqrt{d}]$ $\quad d \equiv 1 \pmod 4$

$\frac{1+\sqrt{d}}{2} \qquad x^2 \pm x - \frac{d-1}{4}$

Exercise: find normalization of $\mathbb{Z}[\sqrt{d}]$ for d (squarefree) integer

Integral closure of integral closure = integral closure

$x^3 + \alpha x + \sqrt[5]{2} = 0$

$\alpha^3 + \alpha + 1 = 0$

$\Rightarrow$ x is algebraic integer

$s_1, \dots, s_n$ integral over R

$s^n + s_{n-1}s^{n-1} + \dots + s_0 s^0 = 0$

$\Rightarrow s$ integral over R

$$R \subseteq \underbrace{R[s_0, \dots, s_{n-1}]}_{\text{finite}} \subseteq \underbrace{R[s_0, \dots, s_{n-1}, s]}_{\text{finite}}$$

finite

Integral domain R called normal if it is integrally closed in the field of quotients

Example: If R UFD, then R is normal

$\mathbb{Z}[\sqrt{5}]$ not normal

$\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$

Lecture 34: Geometry of Normalization

$R \subseteq S$ $\quad S$ finite over R (as R-module)

$s \in S$ integral over $R[s]$ finite

R normal in quotient field $R \subseteq k$ if integral elements already in R

$f: \operatorname{Spec} S \to \operatorname{Spec} R$

$f^{-1}(\text{point})$ is finite set

↳ quasi-finiteness ↳

$R[x] \subseteq R[x, x^{-1}]$

Spec — (no connection) —

$R \subseteq S$ finite $\Rightarrow$ quasifinite

$\operatorname{Spec} S \longrightarrow \operatorname{Spec} R$

pick $\mathfrak{p} \in \operatorname{Spec} R$

want to show $f^{-1}(\mathfrak{p})$ is a finite set

(1) Quotient by $\mathfrak{p}$

So can assume $\mathfrak{p} = 0$ (so R integral domain)

(2) Localize at $\mathfrak{p} = (0)$ in R

$\Leftrightarrow$ Replace R by field of quotients

(3) Now, R is a field. S is finite dim. v.s. over R so is Artinian so has only finite # of primes. So $f^{-1}(\mathfrak{p})$ finite (and discrete)

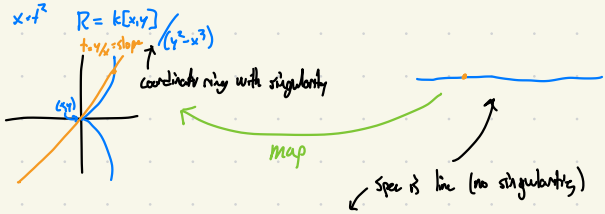
} preserves $f^{-1}(\mathfrak{p})$

Normalization:

Sort of mild resolution of singularities

Example: $R = k[t^2, t^3]$ $\quad 1, t^2, t^3, t^4, \dots$

$y = t^3$ $\quad x = t^2$ $\quad R = k[x,y]/(y^2 - x^3)$



Normalize R: field of quotients $k(t)$

t integral over R

$R \subseteq k[t]$

↑ integral closure of R

Suppose R is u.f.d (so integrally closed)

Look at $R[\sqrt{r}] \cong R[t]/(t^2-r)$

↑ quadratic extension

What is normalization?

When is $p\sqrt{r}+q$ integral over R

$p\sqrt{r}-q$ also integral

So $2q$ integral, so in R

Example $\mathbb{Z}[\sqrt{-3}]$ $\frac{\sqrt{-3}}{2}+\frac{1}{2}$ in integral closure

Assume $\frac{1}{2} \in k$ so $q \in R$

So $(p\sqrt{r})^2$ integral over R

$= p^2 r \in k$ (field of quotients)

so $p^2 r \in R$

Example: $y^2 = x^3+ax^2+bx+c$

$R = k[x,y]/(y^2 - x^3 - ax^2 - bx - c)$

Integral closure?

$r = x^3+ax^2+bx+c$

$= (x-\alpha)^2(x-\beta)$

$p = \frac{1}{(x-\alpha)}$

$= (x-\alpha)(x-\beta)(x-\gamma)$

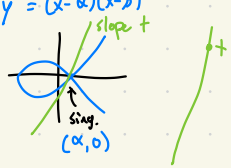
α, β, γ diff

Integral closure $= R$

$\rightarrow R$ normal

$\frac{y}{x-\alpha} \in$ integral closure

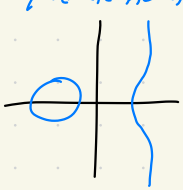
$y^2 = (x-\alpha)^2(x-\beta)$



$R = k[x,y]/(y^2 - \cdots)$ $\left[\frac{y}{x-\alpha}\right]$

$= k[t]$ $t = \frac{y}{x-\alpha}$

$y^2 = (x-\alpha)(x-\beta)(x-\gamma)$



$z^2 = x^2+y^2$

$R = k[x,y,z]/(z^2 - x^2 - y^2)$

want to show R normal

R quadratic extension of $k[x,y]$ $k(x,y)\left[\sqrt{x^3+y^2}\right]$

x^3+y^2 not divisible by square (char $k \neq 2$)

So $k[x,y]\left[\sqrt{x^3+y^2}\right]$ is normal

Serre: R normal $\iff$ all singularities of Spec R have codim ≥ 2
and if $R_{\mathfrak{p}}$ has dim ≥ 2 it has depth ≥ 2

Resolution of sings of surface:
(1) Normalize: all sings are points
(2) Blow up all points
algebraic geometry

Lecture 35: Nakayama's lecture

Examples (motivation):

(1) R is local ring of analytic functions near $0 \in \mathbb{C}$ max ideal $\mathfrak{m}$ = functions vanishing at 0

$\bigcap \mathfrak{m}^n = 0$ $\mathfrak{m}^n$ = functions vanishing to order n

(2) R is local ring of smooth functions near $0 \in \mathbb{R}$ $\mathfrak{m}$ = max ideal

$\bigcap \mathfrak{m}^n \neq 0$ $\begin{cases} e^{-1/x^2} & (x \neq 0) \\ 0 & x = 0 \end{cases}$

(3) $R = \bigcup_{n \geq 1}$ formal power series $x^{\frac{1}{n}}$

$\mathfrak{m}$ = things w/ constant term 0

$\bigcap \mathfrak{m}^n \neq 0$ $\mathfrak{m} = \mathfrak{m}^2$

$\bigcap \mathfrak{m}^n = \mathfrak{m}$

$R \to \hat{R}$ ← completion ← is this map injective? Kernel = $\bigcap \mathfrak{m}^n$

$R/\mathfrak{m} \leftarrow R/\mathfrak{m}^2 \leftarrow R/\mathfrak{m}^3 \leftarrow \cdots$

$k[x]$ $k \leftarrow k[x]/(x^2) \leftarrow k[x]/(x^3)$

$\mathfrak{m} = (x)$ $k[[x]]$

Aim $\bigcap \mathfrak{m}^n = 0$ if $\mathfrak{m}$ max, R Noetherian local ring

Nakayama's Lemma: If M f.g. module over a local ring R with max ideal $\mathfrak{m}$ then $\mathfrak{m}M = M \Rightarrow M = 0$

Proof: Suppose M generated by $a_1 \dots a_n$ n minimal

If $n \geq 1$ put $a_1 = \sum_{\substack{m_i \in \mathfrak{m} \\ a_i \in M}} m_i a_i$ $(M = \mathfrak{m}M)$

$(1 - m_1) a_1 = \sum_{i>1} m_i a_i$

$(1-m_1)$ unit (local ring) so a_1 = combination of $a_2, \dots, a_n$ (not minimal!) $\rightarrow\leftarrow$

also works for $\mathfrak{m}$ = Jacobson radical of R $= \bigcap$ all max ideals

Corollary: If M f.g. over local ring R and $m_1, \dots, m_n$ generate $M/\mathfrak{m}M$ then they generate M

Proof: Put $N = M/\langle m_1, \dots, m_n \rangle$ so N f.g and $N = \mathfrak{m}N$

so $N = 0 \Rightarrow M = \langle m_1, \dots, m_n \rangle$

If it is not true that M has properly $m_1, \dots, m_n$ generate $M/\mathfrak{m}M$ then $m_1, \dots, m_n$ generate M

$R = \mathbb{Z}_{(2)}$ $M = \mathbb{Q}$ $\mathfrak{m} = (2)$

$M/\mathfrak{m}M = 0$ ← not f.g

Application: suppose $R \subseteq S$ rings, S integral over R.

Then $\operatorname{Spec} S \to \operatorname{Spec} R$ is onto.

Proof: pick $\mathfrak{p} \in \operatorname{Spec} R$

(1) Localize at $\mathfrak{p}$: invert all elements of $\left(\frac{R}{S}\right)$ not in $\mathfrak{p}$.

Then $\mathfrak{p}$ maximal

(2) Check $\mathfrak{p}S \neq S$. If true, $1 = \sum_{\substack{p_i \in \mathfrak{p} \\ s_i \in S}} p_i s_i$

M = subalgebra/R generated by s_i.

Then $1 \in \mathfrak{p}M$ so $\mathfrak{p}M = M$

M f.g. as R-module b/c S integral over R] Nakayama $\Rightarrow M = 0$ ↯

So $\mathfrak{p}S \neq S$. pick maximal Q of S containing image of $\mathfrak{p}$

Then $Q \cap R = \mathfrak{p}$ $\mathfrak{p} \in \operatorname{Spec} R$ image of $Q \in \operatorname{Spec} S \Rightarrow$ map is onto!

Lecture 36: Artin-Rees Lemma

$\bigcap m^n = 0$

filtrations of modules:

Decreasing filtration:

$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$

Typical example: $M_n = I^n M$ ← ideal of R

↑ I-adic filtration

$M = R = \mathbb{Z}$ $I = (p)$ p prime

$M_n = p^n \mathbb{Z}$ ← p-adic filtration

filtration → topology

$\{M_n\}$ = base of nbhds of 0 in M

$x + M_n$ $x \in M$

Suppose $M \subseteq N$

↑ I-adic topology ↑ I-adic topology

$I^n N$

same topology? → $I^n M \overset{?}{=} M \cap I^n N$

No ∴

$R = \mathbb{Z}$ $M = \mathbb{Z}$ $N = \mathbb{Q}$ $I = (2)$

2-adic topology on $\mathbb{Z}$ = Hausdorff ≠ 2-adic topology on $\mathbb{Q}$ = indiscrete: open sets $\emptyset, \mathbb{Q}$

$R = \mathbb{Z}$ $N = \mathbb{Z}$ $M = 4\mathbb{Z}$ $I = (2)$

$N \supseteq IN \supseteq I^2N \supseteq \cdots$

$\mathbb{Z} \supseteq 2\mathbb{Z} \supseteq 4\mathbb{Z} \supseteq \cdots$

$M \cap I^nN$ $\quad 4\mathbb{Z} \supseteq 8\mathbb{Z} \supseteq 4\mathbb{Z} \supseteq 8\mathbb{Z} \supseteq 16\mathbb{Z} \supseteq \cdots$

I^nM $\quad 4\mathbb{Z} \supseteq 8\mathbb{Z} \supseteq 16\mathbb{Z} = 32\mathbb{Z} \supseteq \cdots$

↖ different filtrations, same topology (filtration one just shifted)

A filtration $\{M_n\}$ of M is called stable if

$IM_n \subseteq M_{n+1}$ and equality holds for $n \geq N$ some N

Example: $M_n = I^nM$ is stable.

Any two stable filtrations give same topology

$M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$ $\quad I^kM \subseteq M_k$

$M \supseteq IM \supseteq I^2M \supseteq \cdots$

If $n \geq N$ $\quad M_{n+1} = IM_n$

$M_{n+k} = I^kM_n \subseteq I^kM$

notion of 'shifted' filtration from above

Artin-Rees Lemma

Suppose $M \subseteq N$ two f.g. modules over a Noetherian ring R with ideal I. Then:

(Strong) any stable filtration on N restricts to a stable filtration on M.

⇓

(Weak) I-adic topology on N restricts to I-adic topology on M

Key step: A filtration $N_0 \subseteq N_1 \subseteq \cdots$ with $IN_n \subseteq N_{n+1}$ is stable iff $N_0 \oplus N_1 \oplus N_2 \oplus \cdots$ is f.g. over $R \oplus I \oplus I^2 \oplus \cdots$ (graded)

deg 0 1 2 3

$N_n \oplus IN_{n+1} \oplus I^2N_{n+2} \oplus \cdots$

↑ take fin. set of generators here (stable → f.g.)

Artin-Rees proof: Suppose $N_0 \supseteq N_1 \supseteq \cdots$ is stable

$\Rightarrow N_0 \oplus N_1 \oplus N_2 \oplus \cdots$ ← blowup algebra

is f.g. over $R \oplus I \oplus I^2 \oplus \cdots$ ← Noetherian (f.g. algebra over R)

$M_n = N \cap N$

$\Rightarrow M_0 \oplus M_1 \oplus M_2 \oplus \cdots$ f.g. module

$\Rightarrow M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$ is stable

Application: suppose R is Noetherian local ring with max ideal $\mathfrak{m}$.

Then $\boxed{\bigcap \mathfrak{m}^n = 0}$

Proof: $J = \bigcap \mathfrak{m}^n$ $\quad \mathfrak{m}^n \cap J = J$ for all n

So $\mathfrak{m}$-adic topology on R restricted to J is indiscrete

J is f.g. module (R-noetherian)

So Artin-Rees $\Rightarrow$ $\mathfrak{m}$-adic topology on J is indiscrete

$\Rightarrow \mathfrak{m} J = J$

$\Rightarrow J = 0$ by Nakayama

$\bigcap \mathfrak{m}^n = 0$

Lecture 37: Blowup algebras

Blowup algebras

filtration: $R_0 \quad R_1 \quad R_2 \quad R_3 \cdots$

$R_i R_j \subseteq R_{i+j}$

Decreasing: $R \supseteq R_1 \supseteq R_2 \supseteq \cdots$

Example: $R_n = I^n$

Increasing: $R_0 \subseteq R_1 \subseteq R_2 \subseteq \cdots$

Example: R_i spanned by products of at most i elements taken from set $\{a_1, \ldots, a_k\}$

Blowup Algebra:

$R_0 \supseteq R_1 \supseteq \cdots$ $\quad R_n = I^n$ (usually)

Blowup Algebra: $R_0 \oplus R_1 \oplus R_2 \oplus \cdots$

used in pf. of Artin-Rees: deg 0, 1, 2 → Graded

$W \subseteq V$ varieties. Blowup of V along W

Roughly: Suppose W, V smooth. Replace each pt. of W by projection of normal bundle

Graded Algebra:

$R_0 \supseteq R_1 \supseteq R_2 \supseteq \cdots \to R_0/R_1 \oplus R_1/R_2 \oplus R_2/R_3 \oplus \cdots$

R local ring I = max ideal $\mathfrak{m}$

$R/\mathfrak{m} \to k \oplus \mathfrak{m}/\mathfrak{m}^2 \oplus \mathfrak{m}^2/\mathfrak{m}^3$

$k[x,y] \to k[x,y]_{(x,y)} \to k[x,y]$

$\mathbb{Z}_{(2)}$ $\quad I = (2)$

Graded ring: $(\mathbb{Z}/2\mathbb{Z}) \oplus \left(2\mathbb{Z}/2^2\mathbb{Z}\right) \oplus \cdots = \left(\mathbb{Z}/2\mathbb{Z}\right)[x]$

Completion:

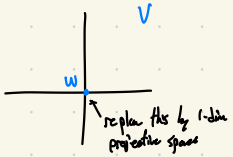
$R/I \leftarrow R/I^2 \leftarrow R/I^3 \leftarrow \cdots$

$\hat{R} = (a \leftarrow_1 b \leftarrow_1 c \cdots$

$R = k[x]$ $\quad I = (x)$

$R \leftarrow R[x]/(x^2) \leftarrow R[x]/(x^3)$

$k[[x]]$



R = coordinate ring of V

I = s.t. R/I coordinate ring of W

$\tilde{R} = R \oplus I \oplus I^2 \oplus \cdots$ graded ring

Blowup of V along W = $\mathrm{Proj}(\tilde{R})$

Extended Rees algebra:

$R \oplus R \oplus R \oplus R \oplus [\oplus I^{-2} \oplus I^{-3} \oplus \cdots$

deg $-3 \quad -2 \quad -1 \quad 0 \quad 1 \quad 2 \quad 3$

$\downarrow$

$k[t] \to$ E.R.A.

↳ Graded algebra of R is

deformation of R

$R_0 \subseteq R_1 \subseteq R_2$

(1) Blowup Algebra $R_0 \oplus R_1 \oplus R_2 \oplus \cdots$ ($t \leftrightarrow 1 \in R_1$)

Example: $R = k[x,y]$

R_n = Spanned by monomials of degree $\le n$

$\to k[x,y,t]$

(2) Graded Algebra $R_0 \subseteq R_1 \subseteq R_2 \subseteq \cdots$

$R_0 \oplus R_1/R_0 \oplus R_2/R_1 \oplus \cdots$

Turn noncommutative rings into commutative ones

Example: R = ring of differential operators over k (char 0)

Generated as k-algebra by $x_1, \ldots, x_n, \frac{d}{dx_1}, \ldots, \frac{d}{dx_n}$

$\frac{d}{dx_1} = D_1$, $\frac{d}{dx_n} = D_n$

$D_i x_j = x_j D_i$ if $i \neq j$

$D_i x_i = x_i D_i + 1$ ← Leibniz rule

$\frac{d}{dx_i}(x_i g) = x_i \frac{d}{dx_i}(g) + g$

R_i = Space spanned by products of at most i generators of $x_1, \ldots, x_n, D_1, \ldots, D_n$

If $a \in R_i$, $b \in R_j$ $\quad ab \in R_{i+j}$, $\quad ab - ba \in R_{i+j-1}$

$ba \in R_{i+j}$ ↑ proved by induction

$R_0 \oplus R_1/R_0 \oplus R_2/R_1 \oplus \cdots$ is commutative!

$\Downarrow$

polynomial algebra on $\overline{x_1}, \ldots, \overline{x_n}, \overline{D_1}, \ldots, \overline{D_n}$ (images)

Application: ring of diff operators has no zero divisors

$a, b \in$ ring of diff ops

highest part $\bar{a}, \bar{b} \in$ graded ring

if $a, b \neq 0$ then $\bar{a}, \bar{b} \neq 0$

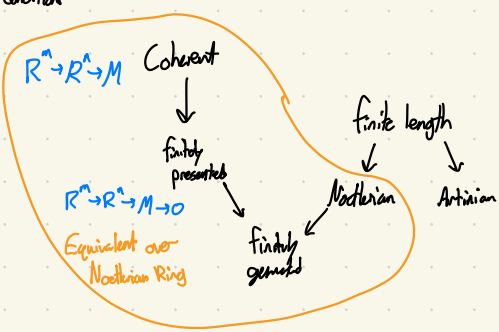
$\Leftarrow$ $\bar{a}\bar{b} \neq 0$ $\quad k[x_1, \dots, x_n]$ no zero divisors

Top degree part of ab = (top degree part of a) $\times$ (" " " b)

$\Rightarrow \neq 0$

Lecture 38: Survey of Module properties

finiteness conditions:



Module cheat sheet

Same over local rings or P.I.D.

free : $M = \overbrace{R \oplus R \oplus R}^{n \text{ times}}$

stably free : $M \oplus R^n$ free (n finite)

Locally free (Zariski) $\quad M[f_i^{-1}]$ free $\quad (f_1, \dots, f_n) = R$

f.g. ↑

Projective

Same for → finitely presented modules nice

f.p. ↑

$A \to B \to 0$

Stalks locally free $\quad M_p$ free, $p \in \operatorname{Spec} M$

f.g. ↑

nice + common

common

flat

$0 \to A \to B \Rightarrow 0 \to M \otimes A \to M \otimes B$

key prop.

most technical
least intuitive

torsion-free

$am = 0 \Rightarrow m = 0$
(a regular)

Lecture 39: Stably free modules

(over R)

M stably free if $M \oplus R^n$ is free (M finite)

Example: Stably free but not free:
Tangent space of sphere S^2

R = continuous functions on S^2

M = continuous vector fields

module under pointwise mult.

Check: M stably free $\quad M \otimes R \cong R^3$ (canonic isomorphism)

tangent bundle of S^2 ↑ normal bundle

Algebraically: $R = \mathbb{R}[x,y,z]/(x^2+y^2+z^2-1)$
= polynomials on S^2

$M = (a,b,c) \quad a,b,c \in R$
with $ax+by+cz=0$
$\subseteq R^3$

$R^3 = M \oplus R$

$d = ax+by+cz$

$(a,b,c) \mapsto (a-xd, b-yd, c-zd, d)$
$M \qquad R$

M not free: hairy ball theorem

Any continuous vector field on S^2 vanishes at some point.
So tangent bundle not free bundle.
So M not free module over R

$S^{n-1} \subseteq \mathbb{R}^n$

As before, M module over R

$M \oplus R \cong R^n$

When is M free?

$n = 1, 2, 4, 8$

S^0, S^1, S^3, S^7

groups — nonassociative multiplication with inverses

$\mathbb{R} \subset \mathbb{H}$ — $\mathbb{O}$ octonions

Tangent space is free

J.F. Adams: No other n work — Hard proof using k-theory

↳ hard case $n = 2^m$

Serre's Conjecture: Quillen, Suslin

Any fg projective module over $k[x_1, \dots, x_n]$ free?

Easy to show it is stably free.

finite free resolution:

$$0 \to F_n \to \cdots \to F_2 \to F_1 \to F_0 \to P_0 \to 0$$

$$0 \to P_{n-1} \oplus P_n \to \cdots \to P_0 \oplus P_1 \to P_1 \oplus P_0 \to P_0 \to 0$$

$$P_0 \oplus (P_1 \oplus P_2) \oplus (P_3 \oplus P_4) \oplus \cdots \cong (P_0 \oplus P_1) \oplus (P_2 \oplus P_3) \oplus \cdots$$

free, free, free

So P_0 stably free

Serre's Conjecture $\Leftrightarrow$ Every stably free module over $k[x_1, \dots, x_n]$ is free

$M \oplus R \cong R^m \Rightarrow M \cong R^{m-1}$?

$(f_1, \dots, f_m)$ $f_i \in R$

$f_1, \dots, f_m$ generate unit ideal in R

$\cong R^m \Leftrightarrow (f_1, \dots, f_m)$ can be extended to an invertible matrix in $M_m(R)$

Stably free modules of rank 0.

$M \oplus R^n \cong R^n$ for some n

$M \oplus R^1 \cong R^1$ rank = difference

$M \oplus N \cong R$ M, N ideals

Then $MN = 0$ (direct sum)

Then M, N not free if M or $N \neq 0$

So if $M \oplus R \cong R$, then $M = 0$

If $M \oplus R^n \cong R^n$

take nth exterior powers Λ^n

$\Lambda^n(A \oplus B)$

$= \Lambda^n A \oplus \Lambda^{n-1}(A) \otimes \Lambda^1(B) \oplus \cdots$

$\cdots \oplus M \otimes R^n \oplus R \cong R \Rightarrow M \otimes R^n \cong 0 \Rightarrow M = 0$

Stably free rank 1:

$M \oplus R^n \cong R^{n+1}$

take $n+1$ exterior powers

$\Lambda^2 M \otimes \cdots \oplus (M \otimes R \cong R) \Rightarrow M \cong R$

Add R^n to both sides

$* \oplus M \otimes R^n \cong R^{n+1}$

$*$: vanish; $M \otimes R^n \cong R^{n+1}$: equal by assumption

Lecture 40: The Eilenberg-Mazur swindle

$1 = 0$

$1 - 1 + 1 - 1 + 1 \cdots$

$= (1-1) + (1-1) + (1-1) \cdots = 0$

$= 1 \quad (-1+1) \quad (-1+1) \quad (-1+1) \cdots = 1$

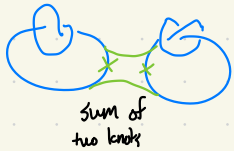
Problem: ∞ sums not well defined

If $A + B = 0$ ∞ sums well-defined and behave well, then $A = B = 0$

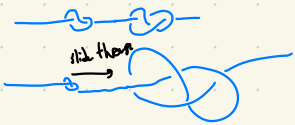
$A + (B + A) + (B + \cdots) = (A + B) + (A + B) + \cdots$

$A = 0 \qquad 0$

Knots:



Sum is commutative:



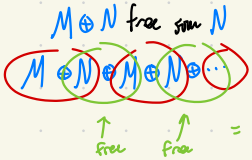
∞ sums defined: (for continuous knots)
(not smooth)

Problem: M stably free $\Leftrightarrow$ $M \oplus R^n$ free for n finite what if infinite?

$M \oplus R^n$ free (n anything)
$\Leftrightarrow$ M projective

(1) $M + (\text{free}) = (\text{free}) \Rightarrow M$ projective
(2) M projective $\Rightarrow M + (\text{free}) = (\text{free})$

$M \oplus N$ free sum N



Stably free of infinite rank are free

$M \oplus R^n = R^\infty$

$R^\infty \to M \oplus R^n$

$R^\infty \oplus R^m \to M \oplus R^n$ m,n finite

$R^m = X \oplus R^n$

$M = R^\infty \oplus X$ (stably free)

$X \oplus R^n \oplus X \oplus R^n \oplus X \oplus R^n \oplus \cdots \oplus R^\infty$ → free module

$= X \oplus (R^n \oplus X)^\infty \oplus R^\infty = X \oplus R^\infty = M$

Lecture 41: Locally free modules

~ Vector bundles

Vector bundle: $V \to X$

fibers vector spaces

Locally: $R^n \times U_i \to U_i$ U_i open $\subseteq X$

Typical example:

$TX \to X$ (↑ tangent space)

R continuous functions on X

M sections of V

Analog for rings:

R: $\operatorname{Spec} R$ $(\sim X)$

Spec covered by open sets

$U_i = \operatorname{Spec} R[f_i^{-1}]$

$(f_1, \ldots, f_n) = R$

M locally free

$M[f_i^{-1}]$ free over $R[f_i^{-1}]$

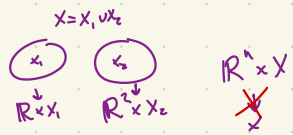
Stably free $\Rightarrow$ locally free

(not f.g. $\Rightarrow$ free

f.g. $\Rightarrow$ f.g. projective $\Rightarrow$ locally free

locally free $\Rightarrow$ stably free? No!

Boring reason:



Spec R disconnected

$R = \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Spec: • •

M ○ 1-dim

"$\mathbb{Z}/3\mathbb{Z}$"

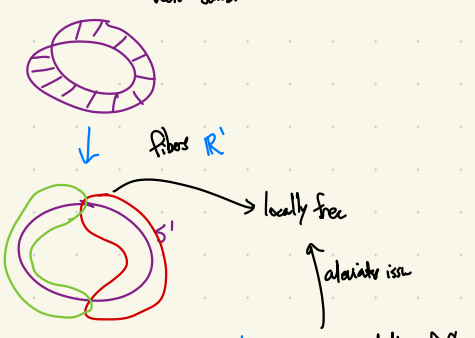
locally (but not stably) free

Interesting reason:

M may be twisted

Example: Moebius band

= vector bundle



Not stably free: go around S^1: reverse orientation of fiber

$M \oplus M \cong \mathbb{R}^2 \times S^1$

Example: $M = (2, 1+\sqrt{-5})$

$R = \mathbb{Z}[\sqrt{-5}]$

↑ not UFD. $6 = 2 \times 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

M non-principal, so not free as module (not generally true but true for this ring)

M locally free:

(1) Cover $\operatorname{Spec} R$ by open sets

$$\operatorname{Spec} R[\tfrac{1}{2}] \cup \operatorname{Spec} R[\tfrac{1}{3}] = \operatorname{Spec} R$$

(2) $M[\frac{1}{2}]$ free over $R[\frac{1}{2}]$ obvious $2 \in M$

$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \| \; M[\frac{1}{2}]$

$M[\frac{1}{3}]$ free over $R[\frac{1}{3}]$

↑ is generated by $1+\sqrt{-5}$ $\quad 2 = \dfrac{(1+\sqrt{-5})(1-\sqrt{-5})}{3}$

free $\quad\quad\quad\quad$ unit ↗ 3

$$M \oplus M \cong R \oplus R$$

$a = \quad 2 \oplus 1+\sqrt{-5} \in M \oplus M$

$b = \quad (1-\sqrt{-5}) \oplus 2 \in M \oplus M$

$3a - (1-\sqrt{-5})b = 0 \oplus (1+\sqrt{-5})$

$(1-\sqrt{-5})a - 2b = 0 \oplus 2$

$\quad\quad 0 \oplus M \quad\quad M$

$\Rightarrow a, b$ generate $M \oplus M$

$R \oplus R \xrightarrow{\sim} M \oplus M$

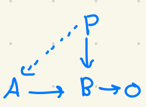
$1 \oplus 0 \mapsto a$

$0 \oplus 1 \mapsto b$

Lecture 42: Projective Modules

Projective Modules vs. Locally free Modules

$\quad\quad\quad\quad\quad\quad\quad\quad \leftrightarrow$ vector bundles



R covered by open $\operatorname{Spec} R[f_i^{-1}]$

$M[f_i^{-1}]$ free over $R[f_i^{-1}]$

$(f_1, \dots, f_n) = R$

Basic properties:

(1) free modules are projective

(2) If $P = X \oplus Y$ projective, X, Y also projective

(3) Any $\oplus$ of projective modules is projective

Projective $\Leftrightarrow$ locally free (vector bundle)

Yes (com. alg.) (diff. geo.) No (alg. geometer) (complex analytic geo.)

Why is there a difference?

$$H^1(\mathrm{Hom}(A,B)) \to \underbrace{\mathrm{Ext}^1(A,B)}_{\text{Vanishes for all } B \Leftrightarrow A \text{ projective}} \to H^0\Big(\underbrace{\mathrm{Ext}^1(A,B)}_{\text{vanishes if } A \text{ locally free (or locally projective)}}\Big)$$

IF this vanishes, locally free $\Rightarrow$ projective

$H^1(M) = 0$?

Yes (commutative rings, smooth manifolds) "partition of unity"

Ring theory case: locally free $\Rightarrow$ projective

Does projective $\Rightarrow$ locally free?

Yes, for f.g. modules

no in general

f.g. projective module M

$\Rightarrow$ finitely presented

$\Rightarrow$ stalks are free

$\hookrightarrow M_{\mathfrak{p}}$ over $R_{\mathfrak{p}}$ ($\mathfrak{p}$ prime)

f.p. module + stalks free

$\Rightarrow$ locally free

A projective module that is not locally free:

R = functions from ∞ set X to $\mathbb{Z}/2\mathbb{Z}$

(complete Boolean algebra)

$= (\mathbb{Z}/2\mathbb{Z})^{\infty}$? doesn't matter if countable or not

$M = I$ = function of finite support

$I : (1,0,1,0,1,0,0,0,0,0,0)$

I is projective

$I = \bigoplus I_x$

I_x order 2 functions w/ support $x \in X$

I_x projective: $R = I_x \oplus$ (functions w/ support disjoint from x)

$\bigoplus$ projective is projective $\Rightarrow$ I projective

Show I not locally free:

$I[f^{-1}]$ over $R[f^{-1}]$ $\quad f \in R$

↑ product of copies of $\mathbb{Z}/2\mathbb{Z}$

f finite support: $I[f^{-1}] \cong R[f^{-1}]$ free

f infinite support: $I[f^{-1}]$ not free

So cover $\operatorname{Spec} R$ by finite number of $\operatorname{Spec} R[f_i^{-1}]$ f_i has finite support

But if $f_1 \dots f_n$ have finite support, $(f_1, \dots, f_n) \neq R$

for vector bundles over smooth manifold

$\bigoplus$ finite dim vector bundles is vector bundle

↑ possibly infinite

Analog for rings is <u>false</u>

$\bigoplus$ locally free modules (finite rank) need <u>not</u> be free

not locally free

Example $I \subseteq R$

$\bigoplus I_x$ ← locally free

Lecture 43: Stalkwise locally free modules

Locally free

↓

projective

↓

stalkwise locally free

} Same for f.p. modules

Example: $R = \mathbb{Z}$

$M = \left\{ \frac{a}{b} \mid b \text{ squarefree} \right\}$

$\mathfrak{p} \in \operatorname{Spec} \mathbb{Z}$

$M_{\mathfrak{p}} \cong \mathbb{Z}_{\mathfrak{p}}$

All stalks of M are 1-dim free

M not projective

M invertible $\Leftrightarrow$ locally free of rank 1 (↑ can't replace w/ stalkwise)

M not f.g.

R = functions X to $\mathbb{Z}/2\mathbb{Z}$

I = functions of finite support

I: projective not locally free

$M = R/I$: stalkwise locally free, not projective

f.g. (generated by 1 element)

not f.p. (requires I also f.g.)

Stalks free: $R_{\mathfrak{p}} \cong \mathbb{Z}/2\mathbb{Z}$

R boolean: $x^2 = x$ for all x

boolean + local $\Rightarrow \mathbb{Z}/2\mathbb{Z}$

$\Rightarrow$ all modules over R have all stalks free

Not projective: $0 \to I \to R \to M \to 0$

$R = I \oplus M$ (↑ proj $\Rightarrow$ split)

f.g. ↑ ↑ not f.g.

finitely presented + stalkwise locally free $\Rightarrow$ projective

$0 \to K \to F \to A \to 0$ — A flat, F free, I ideal

(1) $K \cap FI = KI$

$0 \to K \otimes I \to F \otimes I \to A \otimes I \to 0$

$0 \to K \cap FI \to FI \to II \to 0$

(2) If $u \in K$, find $f : F \to K$ fixing u

$u = \sum r_i f_i$ (f_i basis of F) $\quad I = (r_1, r_2, \ldots)$

$u \in K \cap FI = KI$

$u = \sum k_i r_i$ (some k_i) $\quad f(f_i) := r_i$

(3) If $u_1, \dots, u_n \in K$, can find $F \to K$ fixing u_i

follows from (2) by induction

(4) If K is f.g., A is projective

$\Leftarrow$ $0 \to K \to F \to A \to 0$ splits $\to A$ projective

Lecture 44: Flat Modules

$0 \to A \to B$ exact

$\Rightarrow$ $0 \to M \otimes A \to M \otimes B$ $\Leftrightarrow M$ flat

M flat $\Leftrightarrow$ $M_{\mathfrak{p}}$ flat over $R_{\mathfrak{p}}$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$

Stalkwise locally free modules

$\Rightarrow$ flat (stalks free $\Rightarrow$ flat)

free $\to$ stably free $\to$ locally free $\to$ projective

flat $\leftarrow$ stalkwise free

↑ most useful + easy to check

More examples: any localization $R_{\mathfrak{p}}$ is flat

for schemes modules $\to$ sheaves

projective sheaves = rare

flat sheaves = common

Not flat: $\mathbb{Z}/2\mathbb{Z}$ (over $R = \mathbb{Z}$)

$0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$ (flat, not flat) quotients of flat modules not flat

$0 \to (x,y) \to k[x,y] \to k \to 0$ (not flat, flat)

$0 \to A \to B \to C \to 0$ exact

B, C flat $\Rightarrow A$ flat

A, C flat $\Rightarrow B$ flat

A, B flat not always C flat

Thm Suppose M finitely presented module over local ring R (f.g. enough, proof more complicated (and we care mostly about Noetherian rings))

TFAE: (1) M free

(2) M projective

(3) M flat

(4) $0 \to A \to B \to M \to 0$ exact $\Rightarrow$ $0 \to A/\mathfrak{m} \to B/\mathfrak{m}$ exact $\}$ $\mathrm{Tor}_1(M, R/\mathfrak{m}) = 0$

Proof (4) ⇒ (1)

Choose $f: R^n \to M$ isomorphism

$$(R/\mathfrak{m})^n \to (M/\mathfrak{m}M)^n$$

We want to show this is an isomorphism

Check f onto

$R^n \to M \to N \to 0$

(1) N f.g. b/c M is
(2) $N = \mathfrak{m}N$

} Nakayama: $N=0$
So f is onto

$0 \to K \to R^n \to M \to 0$

↑ f.g. (kernel (b/c M is f.p.))

$\otimes$ with $R/\mathfrak{m}$

$$0 \to K/\mathfrak{m}K \to (R/\mathfrak{m})^n \xrightarrow{\sim} M/\mathfrak{m}M \to 0 \quad \text{exact} \quad (\text{b/c of (4): } \operatorname{Tor}_1(R/\mathfrak{m}, M) = 0)$$

So $K/\mathfrak{m}K = 0$
K is f.g.

} Nakayama: $K=0$

So $R^n \cong M \Rightarrow M$ is free ☑

Corollary: If M f.p. module over any ring R,

TFAE:
(0) M locally free
(1) M projective
(2) M stalkwise free
(3) M flat

} analogs of vector bundles

(3) ⇒ (2): (stalkwise) flat ⇒ stalkwise free
(2) ⇒ (1): Earlier
(1) ⇒ (0): Trust

Lecture 45: Torsion-free modules

free → stably free → locally free → projective → stalkwise free → (flat) → torsion-free → coprimary + integral domain

Integral domain: M torsion free if $xm=0 \Rightarrow x=0$ or $m=0$ $\quad x\in R, m\in M$

General ring: if $xm=0 \Rightarrow m=0$ or x is zero divisor (don't really care) $\quad x\in R, m\in M$

flat $\Rightarrow$ torsion free: x not zero divisor $\Rightarrow$ $0\to R \xrightarrow{\cdot x} R \to R/xR \to 0$ exact

M flat: $0\to M \xrightarrow{\cdot x} M$ exact

so x not zero divisor on $M \Rightarrow M$ torsion free.

Torsion free but not flat:

(over P.I.D., torsion free $\Leftrightarrow$ flat)

M flat $\Leftrightarrow M\otimes I \subseteq M$ for all ideals I (for any R)

$I=(x,y)\subseteq k[x,y]=R$

I torsion free but not flat.

$\mathrm{Tor}_1(I,k)\neq 0$ (will define later)

OR: $0\to I \to k[x,y]$

$\otimes I$ $\qquad I\otimes I \to I$ not exact

Example w/ R local: $R=k[[x,y]]$ $\quad I=(x,y)$

Torsion-free $\Rightarrow$ coprimary (over integral domains)

only one associated prime

(0) $\quad$ $\mathrm{Ann}(m)$ $m\in M$

Coprimary $\not\Rightarrow$ torsion-free

$M=\mathbb{Z}/2\mathbb{Z}$ $\quad R=\mathbb{Z}$

(2) associated prime

Homological Algebra 1: Tor for Abelian groups

$\mathrm{Tor}(A,B)$

Čech: Manifold M has homology groups $H_i(M,\mathbb{Z})$

Problem: Express $H_i(M,G)$ $\quad H_i(M,G)$

in terms of $H_i(M,\mathbb{Z})$

What is this?

$0\to H_i(M,\mathbb{Z})\otimes G \to H_i(M,G) \to \mathrm{Tor}(H_{i-1}(M,\mathbb{Z}),G) \to 0$

(splits non-canonically)

$0 \to A \to B \to C \to 0$ exact, abelian groups

$\otimes M$ $A \otimes M \to B \otimes M \to C \otimes M \to 0$ exact

↑ not injective $\left(0 \to \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0\right)$

$\mathbb{Z}/2\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$

↑ not injective

$0 \to \mathrm{Tor}(A,M) \to \mathrm{Tor}(B,M) \to \mathrm{Tor}(C,M) \to A \otimes M \to B \otimes M \to C \otimes M \to 0$ exact!

↑ injective over $\mathbb{Z}$; $\mathrm{Tor}(C,M)$ fixes injectivity

Def $\mathrm{Tor}(A,B)$:

Choose free resolution of A

$0 \to \mathbb{Z}^m \to \mathbb{Z}^n \to A \to 0$

$\otimes B$ $\circlearrowright \to \mathrm{Tor}(A,B) \to B^m \to B^n \to A \to 0$

↑ not injective in general

(1) Where does def. come from?

(2) Seems to depend on resolution of A?

(3) Why is it called Tor?

(4) How do we compute?

(1) Algebraic topology:

Manifold M

triangulable if

Chain complex:

$\xrightarrow{d} C_2 \xrightarrow{d} C_1 \xrightarrow{d} C_0$

C_i basis of i-dim simplices

$H_i(M)$ = homology of complex

$= (\ker C_i \to C_{i-1}) / \mathrm{Im}(C_{i+1} \to C_i)$

$H_i(M,G)$: $\to C_2 \otimes G \to C_1 \otimes G \to C_0 \otimes G \to \dots$

→ homology of this ↗

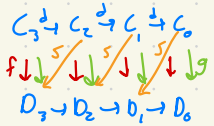
So tor ~ homology

(2) M can have 2 diff. triangulations

do we get the same homology groups?

Easier: $M \underset{g}{\overset{f}{\rightrightarrows}} N$

do these induce same map from homologies of M to N



f, g induce same map on homology iff they are homotopic

$sd - ds = f - g$

(3) Why called "Tor"?

$\mathrm{Tor}(A,B)$ for f.g. abelian groups depends only on torsion subgroups of A and B ← elements of finite order

(4) Compute $\mathrm{Tor}(A,B)$ A, B f.g. abelian groups

relation to tensor products → $\mathrm{Tor}(A \oplus B, C) \cong \mathrm{Tor}(A,C) \oplus \mathrm{Tor}(B,C)$

$\mathrm{Tor}(A, B \oplus C) \cong \mathrm{Tor}(A,B) \oplus \mathrm{Tor}(A,C)$

So just need to compute $\mathrm{Tor}(A,B)$ for A, B cyclic

$\mathrm{Tor}(\mathbb{Z}, G)$: $0 \to 0 \to \mathbb{Z} \to \mathbb{Z} \to 0$ ($\mathbb{Z}$: 0, $\mathbb{Z}$: n)

$\otimes G$ $\quad 0 \otimes G \to \mathbb{Z} \otimes G$

$0 \to \mathrm{Tor}(\mathbb{Z}, G) \to 0 \to G$ ← kernel

$\mathrm{Tor}(\mathbb{Z}, G) = 0$

$\mathrm{Tor}(\mathbb{Z}/n\mathbb{Z}, G)$ $\quad 0 \to \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$

$\otimes G$ $\quad \mathbb{Z} \otimes G \xrightarrow{\cdot n} \mathbb{Z} \otimes G \to (\mathbb{Z}/n\mathbb{Z}) \otimes G \to 0$

$0 \to \mathrm{Tor}(\mathbb{Z}/n\mathbb{Z}, G) \to G \xrightarrow{\cdot n} G$

$\mathrm{Tor}(\mathbb{Z}/n\mathbb{Z}, G) \cong$ elements of order n in G

$\mathrm{Tor}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/(m,n)\mathbb{Z}$ ← gcd

$\mathrm{Tor}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = 0$

$\mathrm{Tor}(A,B)$ depends only on torsion of A, B

Note: $\mathrm{Tor}(A,B) \cong \mathrm{Tor}(B,A)$ ← natural isomorphism

↑ true in general, but not obvious

for A, B finite, $\mathrm{Tor}(A,B) \cong A \otimes B$

BAD! Not a natural isomorphism → depends on choice of generator of A, B

Homological Algebra 2: Properties of Tor

$\mathrm{Tor}(A,B)$ A, B Abelian

(1) Check well-defined $0 \to \mathbb{Z}^m \to \mathbb{Z}^n \to A \to 0$

$0 \to \mathrm{Tor}(A,B) \to B^m \to B^n$

(2) $\mathrm{Tor}(A,B)$ is a functor in A, B

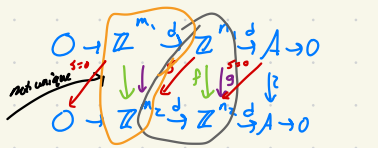
$B \to C$ $\quad \mathrm{Tor}(A,B) \to \mathrm{Tor}(A,C)$

(3) $\mathrm{Tor}(A,B) \cong \mathrm{Tor}(B,A)$

(4) Long exact sequence $0 \to A \to B \to C \to 0$

$0 \to \mathrm{Tor}(A,M) \to \mathrm{Tor}(B,M) \to \mathrm{Tor}(C,M) \to A \otimes M \to B \otimes M \to C \otimes M \to 0$

Well defined:



$\otimes B$ $\quad 0 \to \mathrm{Tor}(A,B) \to B^{m_1} \to B^{n_1} \to A$

$\exists \downarrow \quad \downarrow \quad \downarrow$

$0 \to \mathrm{Tor}'(A,B) \to B^{m_2} \to B^{n_2} \to A$

f, g homotopic

$\to \; ds = f - g \quad d(f-g) = 0$ $\qquad f - g = sd + ds$

$\to \; f - g = sd \quad d(f-g) = (f-g)d = dsd$

$0 \to \mathrm{Tor}(A,B) \to B^{m_1} \to B^{n_1}$

in ker d $\quad f\downarrow = \downarrow g \quad f \downarrow \downarrow g \quad f \downarrow \downarrow g$

$0 \to \mathrm{Tor}'(A,B) \to B^{m_2} \to B^{n_2}$

$f - g = sd$

f, g same on kernel of d

We get well-defined map $\mathrm{Tor}(A,B) \leftrightarrows \mathrm{Tor}'(A,B)$

Composition is identity

$\Rightarrow \mathrm{Tor}(A,B) \cong \mathrm{Tor}'(A,B)$

↑ canonical isomorphism

Tor is a functor in A, B $\qquad 0 \to \mathbb{Z}^m \to \mathbb{Z}^n \to A \to 0$

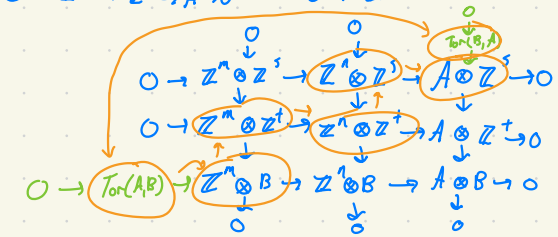
$\mathrm{Tor}(A,B) \to B^m \to B^n$

$B \to C$ $\qquad \exists \downarrow \quad \downarrow \quad \downarrow$

$\mathrm{Tor}(A,B) \to \mathrm{Tor}(A,C)$ $\qquad \mathrm{Tor}(A,C) \to C^m \to C^n$

$\mathrm{Tor}(A,B) \cong \mathrm{Tor}(B,A)$

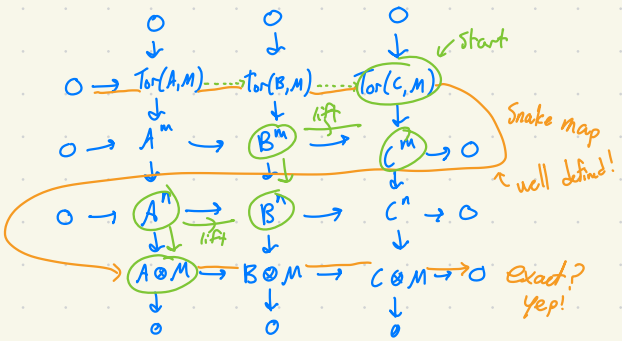
$0 \to \mathbb{Z}^m \to \mathbb{Z}^n \to A \to 0$ $\quad$ $0 \to \mathbb{Z}^s \to \mathbb{Z}^t \to B \to 0$



So we get a ~~Iso~~ isomorphism $\mathrm{Tor}(A,B) \rightleftarrows \mathrm{Tor}(B,A)$

Long exact sequence: $0 \to A \to B \to C \to 0$

$\otimes M$: $0 \to \mathbb{Z}^m \to \mathbb{Z}^n \to M \to 0$



find $\mathrm{Tor}(\mathbb{Q}/\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$

$\mathrm{Tor}(\mathbb{Q}, A) = 0$

$\mathbb{Q}$ is flat → preserve ~~tensor~~ products

$0 \to \mathbb{Z}^m \to \mathbb{Z}^n \to A \to 0$

$0 \hookrightarrow \mathbb{Q}^m \to \mathbb{Q}^n \to A \to 0$ (Tor)

$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$

$\otimes A$ $\quad \mathrm{Tor}(A,\mathbb{Q}) \to \mathrm{Tor}(A,\mathbb{Q}/\mathbb{Z}) \to \mathbb{Z} \otimes A \to \mathbb{Q} \otimes A$

$\| \qquad\qquad \| \qquad\qquad\qquad\qquad \| \qquad\qquad \|$

$0 \to \mathrm{Tor}(A,\mathbb{Q}/\mathbb{Z}) \to A \to \mathbb{Q} \otimes A$

$\mathrm{Tor}(A,\mathbb{Q}/\mathbb{Z}) = \ker(A \to \mathbb{Q} \otimes A) =$ torsion of A

$A = \mathbb{Q}/\mathbb{Z} \to$ torsion is $\cong \mathbb{Q}/\mathbb{Z}$

Homological Algebra 3: Tor over rings

$\mathrm{Tor}_i^R(A,B)$ $\quad R$ ring, A, B R-modules

Def:

(1) $\to R^{n_3} \to R^{n_2} \to R^{n_1} \to R^{n_0} \to A \to 0$ exact

(2) $\otimes B$ $\quad \to B^{n_3} \to B^{n_2} \to B^{n_1} \to B^{n_0} \to 0$

(3) H_i $\quad \ker(B^{n_i} \to B^{n_{i-1}}) \Big/ \mathrm{Im}(B^{n_{i+1}} \to B^{n_i}) = \mathrm{Tor}_i^R(A,B)$

Questions: (1) well-defined?
(2) functor?
(3) symmetric?
(4) Long exact sequence $\quad 0 \to A \to B \to C \to 0$

$\cdots \mathrm{Tor}_0(C,M) \to \mathrm{Tor}_1(A,M) \mathrm{Tor}_1(B,M) \to \mathrm{Tor}_1(C,M) \to A \otimes M \to B \otimes M \to C \otimes M \to 0$

Examples:

1) Serre's definition of intersection multiplicities

$$\text{length}\left(\sum_i (-1)^i \mathrm{Tor}_i^R(R/I, R/J)\right)$$

R = local ring
I, J ideals

2) Homology of a group G

$H_i(G,M) = \mathrm{Tor}_i^{\mathbb{Z}[G]}(\mathbb{Z}, M)$

3) Homology of lie algebra A

$H_i(A,M) = \mathrm{Tor}_i^{U(G)}(R, M)$ ($U(G)$: universal enveloping algebra of A)

4) Hochschild:

$HH(A,M) = \mathrm{Tor}_i^{A \otimes A^\circ}(A, M)$

Calculations:

(1) $R = k[x]/(x^2)$ $\quad$ Basis $1, x$

$M = k = R/(x)$ $\quad \mathrm{Tor}_i^R(k,k)$

$\cdots \to R \xrightarrow{1 \mapsto x} R \xrightarrow{1 \mapsto 1} R \to k \to 0$

$\otimes k$

$k \xrightarrow{0} k \xrightarrow{0} k \xrightarrow{0} k$

H_i $\quad k \quad k \quad k \quad k$

$\mathrm{Tor}_0 \quad \mathrm{Tor}_1 \quad \mathrm{Tor}_2 \quad \mathrm{Tor}_3(k,k)$

shows no finite resolution!

$\mathrm{Tor}_i(k,k) = k$ for all $i \geq 0$

(2) $R = k[x,y]$

$k_{00} = R/(x,y)$ $\quad k_{ab} = R/(x-a, y-b)$

Resolution of k_{00}

$$0 \to R \to R \oplus R \to R \to k \to 0$$

$\otimes k_{00}$ $\quad 1 \mapsto (y,-x)$ $(1,0) \mapsto x$ $(0,1) \mapsto y$

$$0 \to k \xrightarrow{0} k^2 \xrightarrow{0} k \to 0$$

H_* : $\quad k \quad k^2 \quad k$

$\quad \uparrow \quad \uparrow \quad \uparrow$

$\quad \mathrm{Tor}_2 \quad \mathrm{Tor}_1 \quad \mathrm{Tor}_0$

$$0 \to R \to R^2 \to R \to k \to 0$$

$1 \mapsto (y,-x)$

$(1,0) \mapsto x$

$(0,1) \mapsto y$

$\otimes k_{01}$ $\quad k \to k^2 \to k$ $\quad$ Exact

$1 \mapsto (1,0)$

$(1,0) \mapsto 0$

$(0,1) \mapsto 1$

H_* : $\quad 0 \quad 0 \quad 0$

$\mathrm{Tor}_i(k_{00}, k_{01}) = 0$ for all i

$k[x,y,z] \to$ nonzero Tor_3

(3) $H_i(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$ group homology

$= \mathrm{Tor}_i^{\mathbb{Z}[\mathbb{Z}/n\mathbb{Z}]}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$

Group ring: basis $1, g, g^2, \dots, g^{n-1}$, $g^n = 1$

Resolution of $\mathbb{Z}$

$$\cdots \to \mathbb{Z}[G] \to \mathbb{Z}[G] \to \mathbb{Z}[G] \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

$1 \mapsto 1-g$ $\quad 1 \mapsto 1+g+\cdots+g^{n-1}$ $\quad 1-g$ $\quad 1 \mapsto 1$

kernel generated by $1-g$ $\quad$ kernel generated by $1+g+g^2+\cdots+g^{n-1}$ $\quad$ kernel: generated by $1-g$

$\otimes \mathbb{Z}$

$$\cdots \xrightarrow{\times n} \mathbb{Z} \xrightarrow{0} \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \xrightarrow{1 \mapsto 1-g \mapsto 0} \mathbb{Z} \xrightarrow{0} \mathbb{Z} \to 0$$

H_* : $\quad 0 \quad \mathbb{Z}/n\mathbb{Z} \quad 0 \quad \mathbb{Z}/n\mathbb{Z} \quad \mathbb{Z}$

$\quad \uparrow \quad \uparrow \quad \uparrow \quad \uparrow \quad \uparrow$

$\quad H_4 \quad H_3 \quad H_2 \quad H_1 \quad H_0(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$

Homological Algebra 4: Properties of Tor over Rings

$\mathrm{Tor}_i^R(A,B)$ R ring

Check basic properties:

(1) well defined

(2) functorial

(3) symmetry

(4) Long exact sequence

Def over $R=\mathbb{Z}$: $0 \to \mathbb{Z}^m \to \mathbb{Z}^n \to A \to 0$

$\otimes B$ $0 \to B^m \to B^n \to 0$

H_* $\mathrm{Tor}(A,B)$ $A \otimes B$

$\cdots \to R^{n_3} \to R^{n_2} \to R^{n_1} \to R^{n_0} \to A \to 0$

$\otimes B$: $\to B^{n_1} \to B^{n_0} \to 0$

H_*: $\mathrm{Tor}_i^R(A,B)$

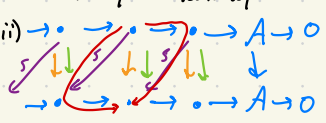
(1) Well defined: $\cdots \to R^{m_2} \to R^{m_1} \to R^{m_0} \to A \to 0$ $d^2 = 0$

$\cdots \to R^{n_2} \to R^{n_1} \to R^{n_0} \to A \to 0$

i) we can find a morphism of these complexes

$\mathrm{Tor}_i(A,B) \to \mathrm{Tor}_i(A,B)$

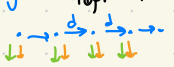
first seq second seq

ii) 

$f \downarrow g$ $f - g = sd + ds$

s is a homotopy from f to g

f, g homotopic → induce same map on homology



$H_n = \frac{\ker d}{\mathrm{im}\, d}$ $f - g = sd + ds$

$f(x) - g(x) = d(sx)$ if $d(x) = 0$

$\otimes B$

$f_2 \otimes B \to f_1 \otimes B \to f_0 \otimes B \to \cdots$ f, g induce same map from $\mathrm{Tor}(A,B)$ to $\mathrm{Tor}'(A,B)$

$G_2 \otimes B \to G_1 \otimes B \to G_0 \otimes B \to \cdots$

$\mathrm{Tor}(A,B) \rightleftarrows \mathrm{Tor}(A,B)$

f ↗ ↙ composition is id $\Rightarrow$ isomorphism ↗ g

(2), (3): Symmetry: $\mathrm{Tor}(A,B)$

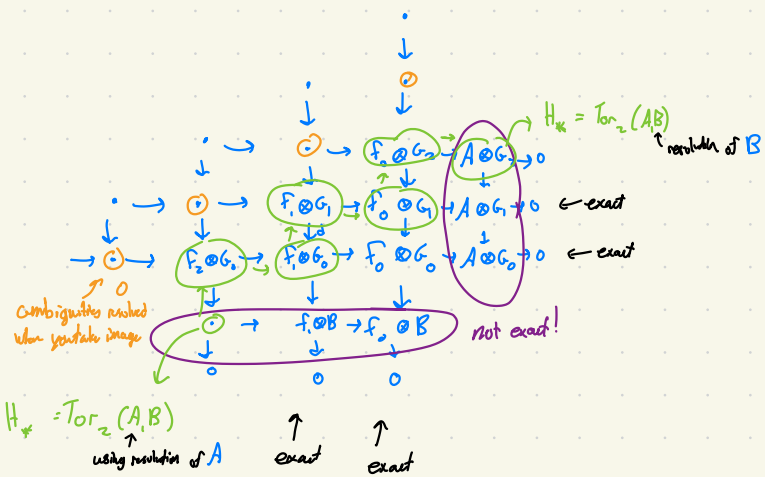
↗ resolution of A $\otimes B$ ↖ resolution of B $\otimes A$

$\cdots \to F_2 \to F_1 \to F_0 \to A \to 0$ exact

F_i, G_i flat

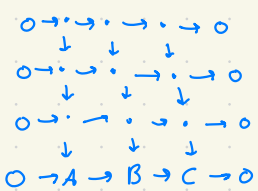
$\cdots \to G_2 \to G_1 \to G_0 \to B \to 0$ exact

Tensor the resolutions:



(4): Long exact sequence: $0 \to A \to B \to C \to 0$ $\otimes M$ $\mathrm{Tor}(\_, M)$

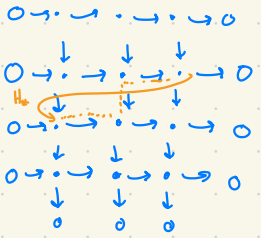
i) Choose compatible resolutions of A, B, C



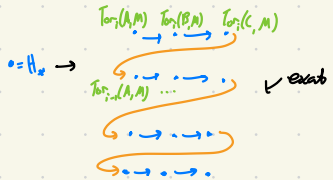
• free

rows, cols exact

$\otimes M$, throw away bottom row



rows still exact,
columns not exact
$H_M = Tor\left(\begin{smallmatrix} A \\ B \\ C \end{smallmatrix}, M\right)$



Homological Algebra 5: Ext(A,B)

$Ext(A,B)$
↑ ↑
Modules over R

$A \otimes_R B \rightarrow Tor_i^R(A,B)$

$Hom_R(A,B) \rightarrow Ext_R^i(A,B)$

(1) Right exact functor $F(A)$

if $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ exact then

$F(A) = M \otimes_R A$ $F(A) \rightarrow F(B) \rightarrow F(C) \rightarrow 0$ exact

Define derived functors $L_i F(A)$

(1) Take resolution of A $\rightarrow R^{n_1} \rightarrow R^{n_0} \rightarrow A \rightarrow 0$

(2) Apply F $\cdots \rightarrow F(R^{n_2}) \rightarrow F(R^{n_1}) \rightarrow F(R^{n_0}) \rightarrow 0$ not exact

(3) Take homology $L_1F(A)$ $L_0F(A)$

(1) $L_0 F = F$ (by right exactness)

(2) L_i well defined

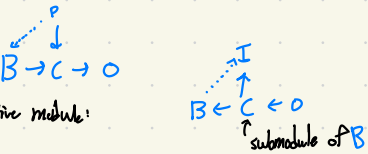
(3) functorial

(4) Long exact sequence

Do not need free modules R^{n_i}

Can use projective modules

$P_2 \rightarrow P_1 \rightarrow P_0 \rightarrow A \rightarrow 0$



Left exact functor:

if $0 \to A \to B \to C \to 0$ exact

then $0 \to F(A) \to F(B) \to F(C)$ exact

Example: Fix X. Then $F(A) := \mathrm{Hom}_R(X, A)$ is left exact

$0 \to \mathrm{Hom}(X,A) \to \mathrm{Hom}(X,B) \to \mathrm{Hom}(X,C)$

$0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$

$X = \mathbb{Z}/2\mathbb{Z}$ $\quad 0 \to \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \to \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \to \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$

$\qquad\qquad\qquad\quad 0 \qquad\qquad 0 \qquad\qquad \mathbb{Z}/2\mathbb{Z}$

Define right derived functor $R^i F(A)$:

(1) Take injective resolution of A

$0 \to A \to I_0 \to I_1 \to I_2 \to \cdots$

(2) Apply F: $0 \to F(I_0) \to F(I_1) \to \cdots$

(3) Take homology $H_* = R^i F(A)$

Properties:

(1) well-defined

(2) $R^0 F = F$

(3) Functorial

(4) Long exact sequence

$F(A) := \mathrm{Hom}_R(X, A)$ $\quad R^i F(A) = \mathrm{Ext}^i_R(X, A)$

Examples:

$R = \mathbb{Z}$ Injective modules are divisible ones (True over any P.I.D.)

$\mathrm{Ext}^i_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$ $(n > 0)$

Injective resolution of $\mathbb{Z}$: injective

$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$

$\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, *) \to \quad 0 \to \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Q}) \to \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \to 0$

$H_* \to \quad (n \neq 0) \to 0 \to \mathbb{Z}/n\mathbb{Z} \to 0$

$\qquad\qquad\quad \mathrm{Ext}^0(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) \quad \mathrm{Ext}^1(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$

$\qquad\qquad\quad = \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$

$\mathrm{Ext}(\mathbb{Z}, \mathbb{Z})$ $\qquad 0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$

$\mathrm{Hom}(\mathbb{Z}, *)$ $\quad 0 \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$

H_* $\qquad\quad \mathbb{Z} \qquad 0$

$\qquad\quad \mathrm{Ext}^0(\mathbb{Z}, \mathbb{Z}) \quad \mathrm{Ext}^1(\mathbb{Z}, \mathbb{Z})$

$\mathrm{Ext}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$ $\quad 0 \to \mathbb{Z}/m\mathbb{Z} \to \mathbb{Q}/\mathbb{Z} \xrightarrow{\times m} \mathbb{Q}/\mathbb{Z} \to 0$

$\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, *)$ $\quad 0 \to \mathbb{Z}/n\mathbb{Z} \xrightarrow{\times m} \mathbb{Z}/n\mathbb{Z} \to 0$

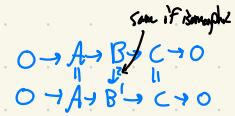
H_* $\quad \mathbb{Z}/(m,n)\mathbb{Z} \qquad \mathbb{Z}/(m,n)\mathbb{Z}$

$\mathrm{Ext}^0(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \quad \mathrm{Ext}^1(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$

Why is Ext called Ext?

Short for extensions

$\mathrm{Ext}^1(C,A)$ classifies extensions

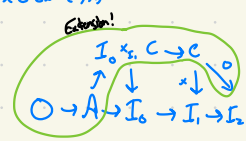


$0 \to A \to B \to C \to 0$

$0 \to \mathrm{Hom}(C,A) \to \mathrm{Hom}(C,B) \to \mathrm{Hom}(C,C) \to \mathrm{Ext}^1(C,A) \to \cdots$

$\mathrm{Id} \longrightarrow$ image

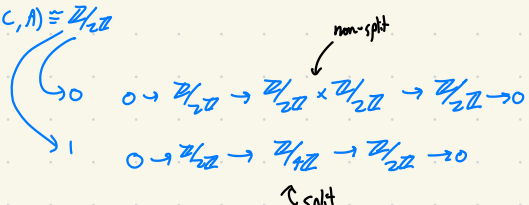
$x \in \mathrm{Ext}^1(C,A)$



$\mathrm{Hom}(C,I_0) \to \mathrm{Hom}(C,I_1) \to \mathrm{Hom}(C,I_2)$

$A = C = \mathbb{Z}/2\mathbb{Z}$

$\mathrm{Ext}^1(C,A) \cong \mathbb{Z}/2\mathbb{Z}$



$\mathrm{Tor}(A,B) \cong \mathrm{Tor}(B,A)$

$\mathrm{Ext}(A,B) \ncong \mathrm{Ext}(B,A)$ in general

$\mathrm{Hom}(C,A)$ contravariant in C (reverse arrows)

$0 \to A \to B \to C \to 0$

$\mathrm{Hom}(A,A) \leftarrow \mathrm{Hom}(B,A) \leftarrow \mathrm{Hom}(C,M) \leftarrow 0$

not onto

$\mathrm{Ext}^i(C,A)$ by using a projective resolution of C

Result same as using injective resolution of A

Example of $Ext^i \neq 0$ $(i>1)$

$R = k[x]/(x^2)$ $\quad Ext^i(C,A)$

$A = C = k = R/(x)$

Projective resolution of C: $\quad R \xrightarrow{\cdot x} R \xrightarrow{\cdot x} R \to k \to 0$

$Hom(x,A) \leftarrow Hom(R,k) \leftarrow Hom(R,k) \leftarrow \cdots$

$\leftarrow k \xleftarrow{0} k \xleftarrow{0} k$

$H_0 \qquad\quad k \quad k \quad k$

$Ext^i(k,k) \cong k$ for all $i \geq 0$

Homological Algebra 6: Injective Modules

Module injective if $\quad 0 \to A \to B$, $A \to I$ (dotted)

Derived functors: (1) Take injective/projective resolution ← can we find this?

(2) Apply functor f

(3) Take H_n

Given M, can we find

(1) Projective $\xrightarrow{\text{onto}} M$? ← easy: free modules are projective

(2) $M \xrightarrow{\text{into}}$ injective ? ← tricky

$0 \to M \to I_0 \cdots \to I_1 \cdots \to I_2$

$I_0 \twoheadrightarrow M$, $I_0 \twoheadrightarrow I_1 \twoheadrightarrow \text{im } I_0$

Look at $R = \mathbb{Z}$

Q: What are injective modules?

A: injective ≡ divisible (over P.I.D.).

↳ if $a \in M$ and $n \in \mathbb{Z}$ $(n \neq 0)$

then $a = bn$ for some $b \in M$

Injective ⇒ divisible:

$0 \to n\mathbb{Z} \to \mathbb{Z}$

$I \to I$, $a \mapsto nb = a$

Divisible ⇒ injective:

$0 \to A \xrightarrow{\cdot n} B$, $A \to I$, $a \mapsto i$, $B \to I$, $nj = i$

(n) = ideal of integers x with $xb \in A$

extends to hom from $\langle 1, b \rangle$ to I — keep repeating for all b (Zorn's lemma)

$\mathbb{Z}$ has enough injectives

↑ $M \subseteq$ some injective

$\mathbb{Q}/\mathbb{Z}$ divisible, so injective

Given M, $\overset{\circ}{m} \in M$ can map $m \mapsto q^{\overset{\circ}{m}} \in \mathbb{Q}/\mathbb{Z}$

Extend to map $M \to \mathbb{Q}/\mathbb{Z}$

$m \to$ non zero

$M \to \prod_{m \in M} \mathbb{Q}/\mathbb{Z}$

product of injectives is injective (easy)

Injectives over Noetherian rings reasonably easy

Injectives over R:

$\mathbb{Z}$-module

$$\mathrm{Hom}_R(M, \mathrm{Hom}_{\mathbb{Z}}(R, I)) \cong \mathrm{Hom}_{\mathbb{Z}}(M, I)$$

R-module

$\mathrm{Hom}_{\mathbb{Z}}(R, I)$ injective R-module if I is injective $\mathbb{Z}$-module

(considered as R-module) (considered as $\mathbb{Z}$-module)

$0 \to A \to B$ $\quad$ $0 \to A \to B$

$\mathrm{Hom}_{\mathbb{Z}}(R, I)$ $\quad$ I

↑ injective

⇒ lots of injective R-modules

Any module is contained in a "smallest" injective module ⊆ any other injective module

(Fails for free/projective: $\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$, $1 \mapsto 1$ or $1 \mapsto 2$)

$A \subseteq B$ called essential extension of A

if any nonzero submodule of B has nonzero intersection with A (can't make any smaller)

$0 \to A \to I$ called injective envelope if

(1) I is injective

(2) $A \subseteq I$ is essential extension

minimal injective module

Over $\mathbb{Z}$: easy

Pick $0 \to M \to I$ $\quad I$ injective

Pick E maximal $\subseteq I$ $\quad E \cap M \neq 0$ (Zorn)

$0 \to M \to I/E$

is essential extension of M

I/E is injective as it is divisible, over $\mathbb{Z}$ divisible $\Rightarrow$ injective

Examples: $\mathbb{Z} \subseteq \mathbb{Q}$ $\quad$ union

$\mathbb{Z}/2\mathbb{Z} \subseteq \mathbb{Z}_{(2)}/\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \subseteq \mathbb{Z}/4\mathbb{Z} \subseteq \mathbb{Z}/8\mathbb{Z} \subseteq \cdots$

Lemma: If I has property:

Every essential extension $I \subseteq J$ is trivial $(I = J)$

Then I is injective.

$0 \to I \to M$

pick max submodule E of M

with $E \cap I = 0$ (Zorn)

$0 \to I \to M/E$

If this is proper $(I \neq M/E)$

Then E not max. So $I \cong M/E$

$M \cong I \oplus E$

So any extension of I splits $\Rightarrow$ I injective ☒

Claim $0 \to M \to I$, I injective

Pick $E \subseteq I$ to be max essential extension of M (Zorn)

$0 \to M \to E \to I$

Want to show: E injective

Suppose $E \subseteq E'$ is essential

$0 \to M \to E \to I$

$\downarrow$ if exists ψ I injective

E'

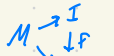
(1) $\ker f \neq 0$ as E is max essential extension

(2) $\ker f \cap E = 0$ as $E \subseteq I$

So $E \subseteq E'$ is not essential —✗—

So E injective envelope.

Injective Envelopes unique up to $\cong$:



I, J injective

$M \subseteq I$, $M \subseteq J$ essential

(1) Can find $f: I \to J$ (J injective)

(2) f injective as $\ker f \cap M = 0$ ($M \subseteq I$ is essential)

(3) $I \leq J$ so $J = I \oplus E$ (I is injective)

(4) $E = 0$ ($M \subseteq J$ is essential)

So f is an isomorphism

Warning: 

isomorphic not canonically

$\mathbb{Z}/2\mathbb{Z} \subseteq \mathbb{Z}[\tfrac{1}{2}]/\mathbb{Z}$

$\uparrow$ automorphism $\to -1$

Nontrivial automorphism which acts trivially on M

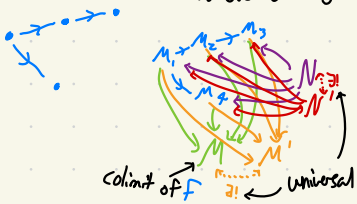
$0 \to M \to I_0 \to I_1 \to \cdots$ (canonical) minimal injective resolution

$0 \to M \to J_0 \to J_1 \to \cdots$

Lecture 46: Limits and colimits of modules

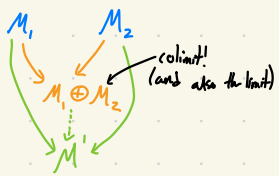
Category C → objects + morphisms

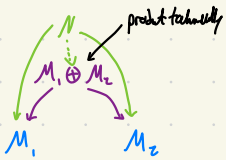
functor $f: C \to$ Modules over a ring R-mod

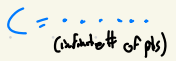


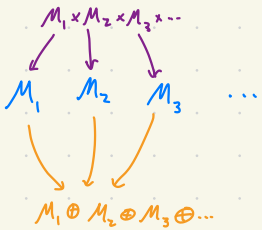
Examples:

$C =$ • •



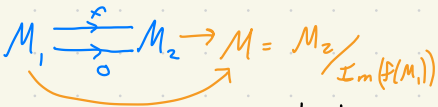






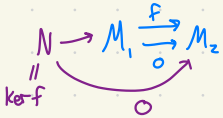
↑ submodule of product, all elements s.t. all but finitely of entries are zero

Categories w/ Morphisms:



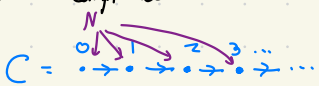
Colimit ~ quotient ↙ =cokernel

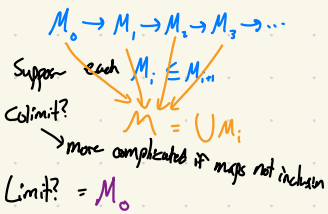
(= if M_1 submodule of M_2)

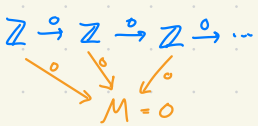


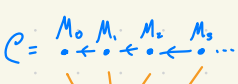
Limit is kernel of morphism

More complicated:







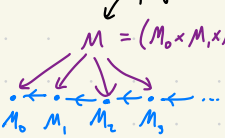


Colimit $M = 0$

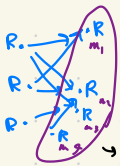
limit? (Direct limit)

projective limit

$M = (M_0 \times M_1 \times M_2 \times \cdots)$ Take elements $(m_0, m_1, \ldots)$ s.t. m_i has image m_j when $(i > j)$



$R/I \leftarrow R/I^2 \leftarrow R/I^3 \leftarrow \cdots$ (construction of p-adics)

$C =$ 

Colimit? Given by generators + relations

→ get an equation

$m_1, m_2, m_3, \ldots \Big/ b(\in M_2) = c(\in M_3)$

Special cases:

Direct limit → special case of limit for directed poset

↳ category of ≤ 1 morphism b/a a, b

can find c with $c > a$ and $c > b$ (for $c \neq a, c \neq b$)

turn poset into category

Projective limit: 

filtered category: Given a, b (1)  can find c w/ maps a, b to c

(2) given $a \overset{f}{\underset{g}{\rightrightarrows}} b$ can find c, h $b \xrightarrow{h} c$ s.t. $hf = hg$

poset: filtered = poset directed

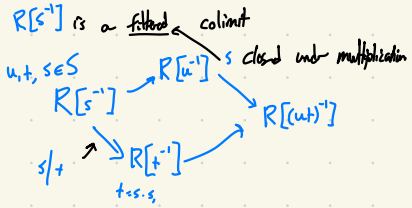
Example: direct sums *not* filtered colimits

Coequalizers *not* filtered

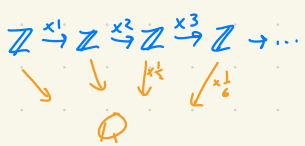
Localization of ring R at multiplication subset S

$R[S^{-1}]$ is a filtered colimit

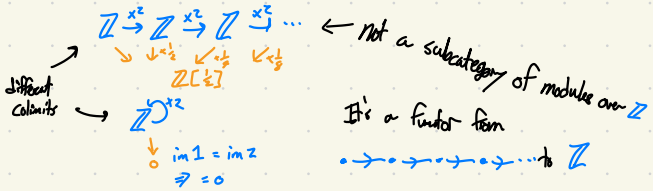
S closed under multiplication



Example: $\mathbb{Q}$ is filtered colimit



Confusing example (warning):



$$0 \to A_i \to B_i \to C_i \to 0$$

$0 \to \lim A_i \to \lim B_i \to \lim C_i \to 0$ exact? Sometimes...

Lecture 47: Colimits and Exactness

$0 \to A_i \to B_i \to C_i \to 0$ exact $\quad i \in J$

$0 \to \underset{J}{\operatorname{colim}}\, A_i \to \underset{J}{\operatorname{colim}}\, B_i \to \underset{J}{\operatorname{colim}}\, C_i \to 0$ exact?

Preserves right exactness.

Method 1: colim is left adjoint to diagonal functor:

Diagonal functor:

Modules $\to$ (J → Modules) $\qquad J: \cdot \rightrightarrows \cdot$

$M \to M \rightrightarrows M$

$\operatorname{colim} \leftarrow A \rightrightarrows B$

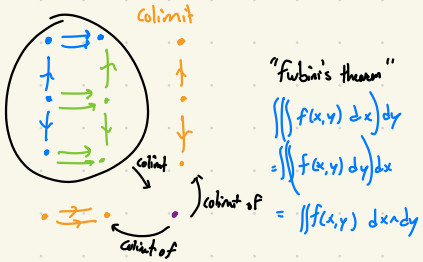
Left adjoints always right exact

Method 2: "colimit commute with colimits"

$0 \to A \to C \to C \to 0$

$C = \operatorname{colim} A \underset{0}{\rightrightarrows} B$

Colimit of a quotient = quotient of colimits



"Fubini's theorem"

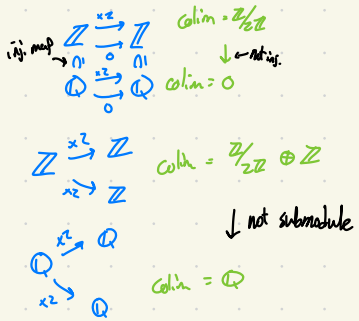
$$\iint f(x,y)\,dx\,dy = \iint f(x,y)\,dy\,dx = \iint f(x,y)\,dx\,dy$$

Colimit functor $\varinjlim_J$ is right exact

so it has a derived functor $\varinjlim_J{}_1$ (not really used...)

Is a colimit of injective maps injective? (is $\varinjlim_J$ (left) exact)

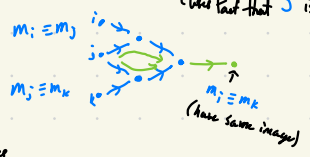
Nope:



A colimit over a filtered category does preserve exactness!

filtered colim of modules M_i is $\left(\text{disjoint union of } M_i\right)\Big/ m_i \equiv m_j$ if $m_i \in M_i,\ m_j \in M_j$ have same image in M_k

key point: $\equiv$ is an equivalence relation ↑ uses fact that J is filtered



filtered colimit of injective maps is injective:

$M_i \subseteq N_i \quad i \in J$

$\varinjlim M_i \subseteq \varinjlim N_i$?

$m_i \in M_i$: image 0 in $\varinjlim N_i$

$m_i \to n_i$ so $m_j = 0$ as map $M_j \to N_j$ injective

$\downarrow \quad \downarrow$

$m_j \to 0$ in N_j so $m_i = 0$ in $\varinjlim M_i$ $\varinjlim_1$ vanishes if J filtered

Warning: we can do the same for limits instead of colim

$\varprojlim$ always left exact... but need not be right exact, even if category is filtered

$\varprojlim'$ need not vanish if J is filtered.

Colimits of flat modules: a filtered colim of flat modules is flat.
(unfiltered need not be flat)

Any module is colim of flat modules

$R^* \to R^* \to M \to 0$ resolution by free modules (⇒ flat)

$M = \operatorname{colim} R^2 \rightrightarrows R^1$

Suppose $M = \operatorname{colim} M_i$ (M_i flat)
(i filtered)

$0 \to A \to B \to C \to 0$ exact

$0 \to A \otimes M_i \to B \otimes M_i \to C \otimes M_i \to 0$ exact (b/c M_i flat)

$0 \to \operatorname{Colim} A \otimes M_i \to \operatorname{Colim} B \otimes M_i \to \operatorname{Colim} C \otimes M_i \to 0$ exact (colim preserves exactness)
(i filtered)

$0 \to A \otimes \operatorname{Colim} M_i \to B \otimes \operatorname{Colim} M_i \to C \otimes \operatorname{Colim} M_i \to 0$ exact ($\otimes$ commutes w/ colim)

So $\operatorname{Colim} M_i$ is flat

Converse: any flat module is filtered colim of f.g. free modules
Lazard's thm

Lecture 48: limits and exactness

$0 \to A_i \to B_i \to C_i \to 0$ exact, $i \in J$

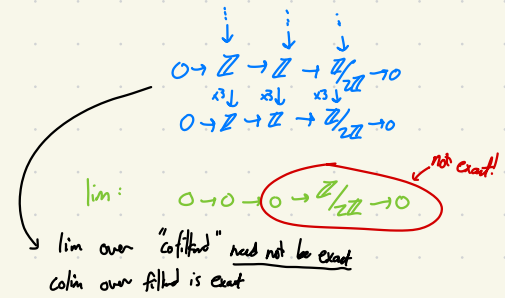
$0 \to \varprojlim A_i \to \varprojlim B_i \to \varprojlim C_i \to 0$ exact?

(1) $\varprojlim$ functor is left exact proof: same as proof that Colim is right exact

$\varprojlim$ has derived functor $\varprojlim'$, if $\varprojlim'(A_i) = 0$, $\varprojlim B_i \to \varprojlim C_i \to 0$ exact

$\varprojlim^n$ can be really weird...

(2) colim need not be left exact lim need not be right exact:



Example: completion of a module M

$\hat{M} = \lim\left(M/I \leftarrow M/I^2 \leftarrow M/I^3 \leftarrow \cdots\right)$

If $0 \to A \to B \to C \to 0$ exact

is $0 \to \hat{A} \to \hat{B} \to \hat{C} \to 0$ exact

↑ may not be surjective

When is $\lim^1(A_i) = 0$?

Answer: vanishes if A_i satisfy Mittag-Leffler condition

M-L condition for: $\cdots \to \bullet_3 \to \bullet_2 \to \bullet_1 \to \bullet_0$

$0 \to \lim A_i \to \lim B_i \to \lim C_i \to 0$

is exact if image of A_j in A_i stabilizes for large j.

$A_i \supseteq \operatorname{Im} A_{i+1} \supseteq \operatorname{Im} A_{i+2} \supseteq \cdots$

eventually all equal

$\operatorname{Im} A_{N+i} = \operatorname{Im} A_{N+i+1} = \cdots$

(Counter) example: $\mathbb{Z} \xleftarrow{\times 3} \mathbb{Z} \xleftarrow{\times 3} \mathbb{Z} \xleftarrow{\times 3} \cdots$

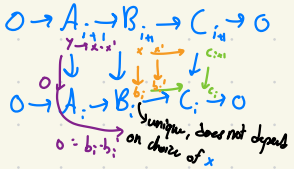
$A_0 \quad A_1 \quad A_2 \quad \cdots$

Case 1: $A_{i+1} \to A_i$ onto for all: (M-L trivial)

So $\lim B_i \to \lim C_i$ is onto.

Case 2: $A_{i+j} \to A_i$ is 0 for j large

Can assume $A_{i+1} \to A_i$ is onto (replace $A_0, A_1, \ldots$ by subsequence)



Choose b_i for all i like this

Easy to check: b_i is image of b_{i+1}

$\lim B_i \to \lim C_i$ also onto.

Case 3: general case

$\cdots A_3 \to A_2 \to A_1 \to A_0$ satisfies ML condition

A_i' = stable limit of A_{i+j}

$\cdots \to A_3' \to A_2' \to A_1' \to A_0'$

all onto

$0 \to A_i' \to A_i \to A_i/A_i' \to 0$ exact

$A_{i+1}' \to A_i'$ is onto (satisfies case 1)

$A_i \to A_i/A_i'$ satisfies case 2

$\lim{}^1(A_i') = 0 = \lim{}^1(A_i/A_i')$

$\lim{}^1(A_i') \to \lim{}^1(A_i) \to \lim{}^1(A_i/A_i')$ exact

$\lim{}^1(A_i') = 0$ so $\lim{}^1(A_i) = 0$

So if A_i satisfy ML condition

$\lim B_i \to \lim C_i$ is onto

Example: Suppose $0 \to A_i \to B_i \to C_i \to 0$

with all A_i finite (or so)

Then $\lim B_i \to \lim C_i$ is onto

$\to$ any decreasing sequence of modules stabilizes.

Lecture 49: Completions

Ring R, ideal I.

Completion $\hat{R}$ is (projective) limit of rings R/I^n

$$R/I \leftarrow R/I^2 \leftarrow R/I^3 \leftarrow \cdots$$
$$a_0 \mapsto a_1 \mapsto a_2$$

Example: $R = k[x]$ $I = (x)$

$$\begin{array}{ccccc} R/I & & R/I^2 & & R/I^3 \\ \| & & \| & & \\ k & & k[x]/x^2 & & k[x]/x^3 \\ a_0 & & a_0 + a_1 x & & a_0 + a_1 x + a_2 x^2 \\ & \searrow & \downarrow & \swarrow & \\ & & (x_2 = 0) & & \end{array}$$

$$a_0 + a_1 x + a_2 x^2 + \cdots$$

$\hat{k[x]} = k[[x]]$

$\hat{k[x,y]} = k[[x,y]]$ $\quad I = (x,y)$

$R = \mathbb{Z}$ $\quad I = (10)$

$\hat{R} =$ $\quad \mathbb{Z}/(10)$ $\quad \mathbb{Z}/(100)$ $\quad \mathbb{Z}/(1000)$ $\cdots$

$\quad\quad 1 \quad\quad 31 \quad\quad 231$

$\cdots .75231$ $\quad \infty$-long decimal integer

Somehow dual to construction of $\mathbb{R}$

10-adic integers $\mathbb{Z}_{10}$

$$\mathbb{Z}/(10^n) \cong \mathbb{Z}/(2^n) \times \mathbb{Z}/(5^n)$$

$$\varprojlim \left(\mathbb{Z}/(10^n)\right) \cong \varprojlim \left(\mathbb{Z}/(2^n) \times \mathbb{Z}/(5^n)\right)$$
$$\cong \varprojlim \left(\mathbb{Z}/(2^n)\right) \times \varprojlim \mathbb{Z}/(5^n)$$

$$\mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_5$$

focus on p-adic integers (for p prime)

$k[x] \sim \mathbb{Z}$ P.I.D.

$(x) \sim (z)$

$\hat{k[x]} = k[[x]] \sim \mathbb{Z}_z$, z-adic integers

$\mathbb{Z}_{10}$ has zero divisors!

$= \mathbb{Z}_2 \times \mathbb{Z}_5$

$(1, 0)$

$\times (0, 1)$

$= (0, 0)$

Alternative construction of completion:

Construct $\mathbb{R}$ from $\mathbb{Q}$

metric on $\mathbb{Q}$: $d(x,y) = |x-y|$

$\mathbb{R}$ = set of cauchy sequences / set of cauchy sequences $\to 0$

Put distance on ring R: $d(x,y) = |x-y|$

what is $|\cdot|$

$|x| = C^{-n}$ if $x \in I^n$, $x \notin I^{n+1}$

$|x| = 0$ if $x \in all\ I^n$ (e.g. $x=0$)

Completion of R in this metric $= \varprojlim \left(R/I^n\right)$

$|x+y| \leq |x| + |y|$

$d(x,y) \leq d(x,z) + d(z,y)$ } reals

R, I $|x+y| \leq \max\{|x|, |y|\}$

$d(x,y) \leq \max\{d(x,z), d(z,y)\}$

ultrametric inequality

(1) Completions of rings are similar to $\mathbb{R}$

Example: can sometimes define powers x^n, gamma functions, bessel functions, for some rings $\hat{R}$

↑ particularly p-adic integers

(2) Easy to solve equations in $\hat{R}$ (Hensel's lemma)

(3) Completion is a stronger version of localization

If $r \in R$ is a unit in $R/\mathfrak{p}^n$, it is a unit in $R/\mathfrak{p}^{2n}$

$1+rs \in \mathfrak{p}^n$

$(1+rs)^2 \in \mathfrak{p}^{2n}$

$= 1 + r(2s+rs^2)$

↑ r unit in $R/\mathfrak{p}^{2n}$

So inverses in $R/\mathfrak{p}^n$ for $n \geq 1$

are compatible, give inverse to r in $\hat{R}$

Suppose $\mathfrak{m}$ maximal ideal

look at completion of R at $\mathfrak{m}$

$\hat{R}$ now local ring

all elements of R not in $\mathfrak{m}$ are units in $R/\mathfrak{m}$ = field

any element of $R/\mathfrak{m}^n$ not in $\mathfrak{m}/\mathfrak{m}^n$ has an inverse.

Get map $R_{\mathfrak{m}} \to \hat{R}$

↑ localization

If R is noetherian + int. domain

$\bigcap \mathfrak{r}^n = 0$ so $R \subseteq \hat{R}$

(fails for prime ideal not maximal) $\mathfrak{p} = (0) \subseteq \mathbb{Z}$ $\hat{\mathbb{Z}} = \mathbb{Z}$, not local ring.

$\mathbb{Z}_{(0)} = \mathbb{Q}$ not subring of completion

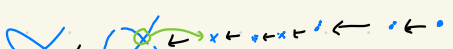
$R = \mathbb{C}[[x^{1/n} \quad n > 0]]$ $\mathfrak{m} = \{x^{1/n}\}$

local, non noetherian completion is just $\mathbb{C}$, $\mathfrak{m}^n = \mathfrak{m}$ for all n

for $\mathfrak{m}$ maximal, $R \to R_{\mathfrak{m}} \to \hat{R} \to \cdots \to R/\mathfrak{m}^3 \to R/\mathfrak{m}^2 \to R/\mathfrak{m} = k$

↑ localization

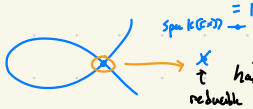
Spectrum:



bigger spectra

$R = k[x,y]/(y^2 - x^3 - x^2)$ $\hat{R}$ $\mathfrak{m} = (x,y)$

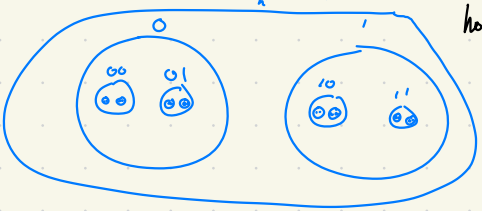
k char $\neq 0$



$\not\subset \cup \not\subset \iff$ completion has zero divisors

If R is integral domain, localization $R[S^{-1}]$ also integral domain
but completion not necessarily

Picture of $\mathbb{Z}_2 = \varprojlim (\mathbb{Z}/2^n)$



homeomorphic to cantor set
or $(\infty$ point set$)^{\aleph_0}$ countable

Lecture 50: Hensel's Lemma

How to find solutions of equations over $\hat{R}$

$\hat{R} = \varprojlim R/I^n$

$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$

$x^3 - 5x - 2 = 0$ have a root in $\mathbb{Q}$?

$x^3 - 5x - 2 = 0$ have a root in $\mathbb{R}$? Yes by IVT

Hensel's lemma: If we can solve an equation mod I^n?
(for suitable n)
We can solve it in $\hat{R}$

Version 1: suppose I ideal of R with completion $\hat{R}$
$f \in \hat{R}[x]$, root a in R/I
$f(a) \equiv 0 \pmod{I}$
Then a can be lifted to a root in $\hat{R}$
provided $f'(a)$ invertible in R/I
$f'(a) \neq 0$ if I maximal
a simple (not double) root

Enough to show:
any root in R/I^n can be lifted to a
root in R/I^{n+1}

$f(a) \in I^n$ (a root mod I^n)

lift a: $f(a+\varepsilon) \in I^{n+1}$ (find ε)

$= f(a) + \varepsilon f'(a) + \cdots$

try $\varepsilon = -\frac{f(a)}{f'(a)}$

$f'(a)(f'(a))^{-1} \equiv 1 \bmod R/I$

for some $f'(a)^{-1}$ in R/I

$f(a+\varepsilon) \in f(a)I \subseteq I^{n+1}$

Example: $\sqrt{7}$ in $\mathbb{Z}_3$

$f(x) = x^2 - 7$ solve $f(x) = 0$ solution $a = 1$ in $\mathbb{Z}/3\mathbb{Z}$

$f'(x) = 2x$

$f'(a) = 2 \not\equiv 0 \bmod 3$

So root $a \pmod 3$ lifts to root in $\mathbb{Z}_3$

$\ldots 2011$

(base 3)

What about $\mathbb{Z}_p^*$ (p odd)

What are the squares?

Hensel $\Rightarrow$ it is square

(1) Number of zeros at the end of p-adic expansion is even

$\ldots 2317000$ (even)

(2) first nonzero digit is a square mod p

$x^2 \equiv b \bmod p$ b square

(2) $x \not\equiv 0 \bmod p$

$2 \neq p$

So $\mathbb{Z}_p^*/\mathbb{Z}_p^{*2} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

What about $p = 2$

$x^2 - a = 0$ in $\mathbb{Z}_2$

problem: root mod 2^n cannot always be lifted to root mod 2^{n+1}

$1^2 \equiv 5 \bmod 2^2$

$a^2 \equiv 5 \bmod 2^3$ no solutions!

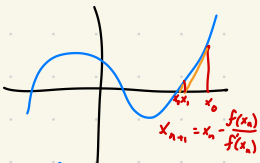
$f'(x) = 2x \equiv 0 \bmod 2$

Suppose in $\mathbb{Z}_p$ $\quad f(a) \equiv 0 \bmod p^{2d+1}$

$f'(a) \not\equiv 0 \bmod p^{d+1}$ $\qquad$ Generic case $d=0$

Then a can be lifted to a root in $\mathbb{Z}_p$

Newton's method



taylor series approx: $f\left(x_n - \frac{f(x_n)}{f'(x_n)}\right)$

$$f(x_{n+1}) = f(x_n) - f'(x_n)\left(\frac{f(x_n)}{f'(x_n)}\right) + \frac{f''(x_n)}{2!}\left(\frac{f(x_n)}{f'(x_n)}\right)^2 + \cdots$$

divisible by p^{2d+1} (*)

small $\quad$ at most p^d

divisible by p^{2d+2}

$\frac{f''(x_n)}{2!}$ has coeffs in $\mathbb{Z}_p$

$\frac{\frac{d^2}{dx^2}x^n}{2!} = \frac{n(n-1)}{2}x^{n-2}$ $\quad$ ($\frac{n(n-1)}{2}$ integer)

$f(x_n) \equiv 0 \bmod p^{d+k}$

$\Rightarrow f(x_n) \equiv 0 \bmod p^{2d+2k}$

When does $b \in \mathbb{Z}_2$ have a square root?

(1) Even # of zeros at the end

(2) last digit is $1 \Rightarrow$ has sqrt iff $\equiv 1 \bmod 2^3$

$f(x) = x^2 - b = 0$

need $f'(x) = 2x \not\equiv 0 \bmod 2^{d+1}$ can take $d=1$

So root exist if $x^2 - b = 0$ has root mod $2^{2d+1} = 2^3$

$\mathbb{Z}_2^*/\mathbb{Z}_2^{*2} \cong \left(\mathbb{Z}/2\mathbb{Z}\right) \times \left(\mathbb{Z}/2\mathbb{Z}\right)$

$\mathbb{Z}_p^*/\mathbb{Z}_2^{*2} \cong \mathbb{Z}/2\mathbb{Z}$

4th roots in $\mathbb{Z}_2^*$

Solve $f(x) = x^4 - b = 0$ assume b odd.

$f'(x) = 4x^3$ $\quad$ want $f'(x) \not\equiv 0 \bmod 2^{d+1}$

take $d=2$

So 4th root exists if $f(x) = x^4 - b = 0$ has root mod $2^{2d+1} = 2^5$

4th powers in $\mathbb{Z}/2^5\mathbb{Z}$: $1, 17$ $\quad$ So b has 4th root if $b \equiv 1 \bmod 2^4$

Lecture 51: Hensel's lemma Continued

Recall I max, R/I field

monic $f(x)$: root a in R/I

can be lifted to a root in $\hat{R}$

Application: what is structure of $\mathbb{Z}_p^* = \varprojlim \mathbb{Z}/(p^n)$

$\ldots 12193$ (base p)

Roots of unity in $\mathbb{Z}_p^*$

$\mathbb{Z}/p\mathbb{Z}$ has $p-1$ roots of unity

$x^{p-1} - 1 = 0$

Roots are distinct $(\text{mod } p)$

Hensel's lemma: all roots lift to $\mathbb{Z}_p$

So in $\mathbb{Z}_p^*$, we have $p-1$ roots of x^{p-1}

they are $\equiv 1, 2, \ldots, p-1 \ (\text{mod } p)$

$\mathbb{Z}_p^* \cong \mathbb{Z}/(p-1)\mathbb{Z} \times$ (elements $\equiv 1 \text{ mod } p$)

$p-1$ roots of 1 ?

p odd: $(\mathbb{Z}_p^* \equiv 1 \text{ mod } p) \underset{\exp}{\overset{\log}{\cong}} (\mathbb{Z}_p \equiv 0 \text{ mod } p)$

$\exp(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$

Convergence: ?

Converges if $p \mid x$ $(p \neq 2)$

How many powers of p in $n!$

$1 \cdot 2 \cdot 3 \cdots n$

$\left[\frac{n}{p}\right]$ of these divisible by p

$\left[\frac{n}{p^2}\right]$ p^2

$\left[\frac{n}{p^3}\right]$ p^3

$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] \leq \frac{n}{p} + \frac{n}{p^2} + \cdots = \frac{n}{p-1}$

if $p \mid x$, $p > 2$, $1 + x + \frac{x^2}{2!} + \cdots$ converges

If $p = 2$, $2^2 \mid x$, $\exp(x)$ converges

If $p \mid x$, $\log(1+x)$ converges

$\mathbb{Z}_p^* \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p \quad p \neq 2$

(roots of unity; torsion free)

$\mathbb{R}^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{R}^+$

$\mathbb{Z}_2^* \cong \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}_2^* \equiv 1 \bmod 4)$

± 1 ; $\cong \mathbb{Z}_2$ under $\cdot$

Variations:

cor: If a is a simple root of $f(x) = 0$ in R/I (f monic)
then a lifts to R (R complete local ring under ideal I)

generalization: Suppose $f(x) = g_0(x) h_0(x)$ in $R/I[x]$
(f monic) Suppose g_0 h_0 coprime in $R/I[x]$
Then factorization lifts $f(x) = g(x)h(x)$ in $R[x]$

Proof: Idea: suppose $f(x) = g_n(x) h_n(x) \pmod{I^n}$
lift g_n, h_n to $g_{n+1} = g_n + a \quad h_{n+1} = h_n + b$
So $f(x) = g_{n+1}(x) h_{n+1}(x) \pmod{I^{n+1}}$
$\Leftrightarrow (g_n(x) + a(x))(h_n(x) + b(x)) = f(x) \bmod I^{n+1}$
$\Leftrightarrow g_0(x)b(x) + h_0(x)a(x) =$ mess in I^n/I^{n+1}
(multiply by mess to cab)
$g_0(x)c(x) + h_0(x)d(x) = 1 \bmod I$
for some c, d
as g_0, h_0 coprime $(\bmod I)$

Henselian local ring: local ring where Hensel's lemma holds
If f monic $= g_0 h_0 \pmod{I}$ (I max ideal)
then factorization lifts to $R[x]$ if
g_0, h_0 coprime

Example: complete local ring

Nagata: any local ring has Henselization
$R \subseteq$ henselization $\subseteq$ completion
(algebraic part of)
(irish)

$R = k[x]$ Henselization: algebraic power series
$\hat{R} = k[[x]]$

$\mathbb{Q} \subseteq$ algebraic numbers $\subseteq \mathbb{C}$
(countable) (uncountable)

Strictly Henselian ring = Henselian local ring wlo R/I (residue field) separably closed

Analogs of local rings for "étale" topology (algebraic geometry) $\varinjlim_{x \in U} \mathcal{O}(U)$.

Lecture 52: flatness of completion

ring R, prime $\mathfrak{p}$

$R_{\mathfrak{p}}$ flat R-module

(1) $M \to M_{\mathfrak{p}}$ preserves exactness

(2) $M_{\mathfrak{p}} \cong M \otimes_R R_{\mathfrak{p}}$

$R_{\mathfrak{p}}$ is flat

$\hat{R} = \varprojlim R/I^n$

"Stronger version of localization"

Aim to show $\hat{R}$ flat R-module if R is Noetherian

(1) If $0 \to A \to B \to C \to 0$ exact,

then $0 \to \hat{A} \to \hat{B} \to \hat{C} \to 0$ also exact

if A, B, C f.g. R-modules

$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$] exact but not f.g.

complain at (2) $\quad \mathbb{Z}_2 \to 0 \to 0 \to 0$

$\uparrow$ not injective

if $0 \to A \to B \to C \to 0$ exact

$0 \to A/I^n B \cap A \to B/I^n B \to C/I^n C \to 0$ also exact

why not $A/I^n A$

$I = (2)$ $\quad 0 \to \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$

$\mathbb{Z}/2\mathbb{Z} \xrightarrow{\times 2} \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$

$\uparrow$ not injective

M-L condition: automatically holds: $A/I^n B \cap A \xleftarrow{\text{onto}} A/I^{n+1} B \cap A$

So $0 \to \varprojlim A/I^n B \cap A \to \varprojlim B/I^n B \to \varprojlim C/I^n C \to 0$ exact

$\varprojlim A/I^n B \cap A$ = ?, $\varprojlim B/I^n B$ = $\hat{B}$, $\varprojlim C/I^n C$ = $\hat{C}$

If $\varprojlim A/I^n B \cap A = \varprojlim A/I^n A = \hat{A}$

Artin-Rees lemma: $\Leftarrow$ needs A, B, C f.g. R-modules

$I^n B \cap A$ is stable

$\Rightarrow \varprojlim A/I^n B \cap A = \varprojlim A/I^n A$

$[\, 0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$
$(z)^n \mathbb{Q} \cap \mathbb{Z}$ not stable $]$

So $0 \to \hat{A} \to \hat{B} \to \hat{C} \to 0$ is exact!

cookey: $0 \to A_n \to B_n \to C_n \to 0$ exact

Lemma: If M f.g. over Noetherian ring, then

$$M \otimes_R \hat{R} \cong \hat{M}$$

false if M not f.g.

$M = \mathbb{Q}$ $I = (2)$ $\hat{M} = 0 \neq M \otimes_{\mathbb{Z}} \hat{\mathbb{Z}} = \mathbb{Z}_2$

$M = \mathbb{Z}^{\oplus \infty}$

$M \otimes_{\mathbb{Z}} \hat{\mathbb{Z}} = \hat{\mathbb{Z}}^{\oplus \infty}$ smaller than $\hat{M}$

Proof ($M \otimes_R \hat{R} \cong \hat{M}$ (f.g.))

$0 \to N \to F \to M \to 0$

f.g. module, f.g. free module

$\hat{R} \otimes$ — $\hat{R}$ ⊗ right exact

$\hat{R} \otimes N \to \hat{R} \otimes F \to \hat{R} \otimes M \to 0 \to 0$ (5)

(3) onto, iso (1), (2) onto (diagram commutes + $\cong$)

$0 \to \hat{N} \to \hat{F} \to \hat{M} \to 0 \to 0$

$\hat{F}$ f.g. free

If M f.g., $\hat{R} \otimes M \to \hat{M}$ is onto $\Rightarrow$ (3)

(4) Apply 5-lemma

$\Rightarrow \hat{R} \otimes M \to \hat{M}$ is isomorphism

$\hat{R}$ is flat $\Leftrightarrow \operatorname{Tor}_1^R(\hat{R}, M) = 0$ for all M filtered

Enough to show for M f.g. (Tor_1 commutes with direct limits, any module is a direct limit of its f.g. submodules.)

for f.g. modules $\hat{R} \otimes_R M \cong \hat{M}$

$M \to \hat{M}$ preserves exactness

So $\operatorname{Tor}_1(\hat{R}, M) = 0$ for M f.g.

So for all M, so $\hat{R}$ is flat

How to move modules from R to $\hat{R}$

Bad: take $M \to \hat{M}$

Good: $M \to M \otimes_R \hat{R}$ ← same for f.g.

$I = (2)$

$\hat{M}$ $\quad 0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ exact

$\quad 0 \to \mathbb{Z}_2 \to 0 \to 0 \to 0$ not exact ∴

$\otimes_{\mathbb{Z}} \hat{\mathbb{Z}}$ $\quad 0 \to \mathbb{Z}_2 \to \mathbb{Q}_2 \to \mathbb{Q}_2/\mathbb{Z}_2 \to 0$ exact and much nicer

$\mathbb{Z}_2$

Lecture 53: Dimension introduction survey

idea: $K[x,y,z]$ should have dim 3

Cantor: bijection from $\mathbb{R}$ to $\mathbb{R}^n$ (not continuous)

Peano: continuous map $\mathbb{R}^1 \xrightarrow{\text{onto}} \mathbb{R}^2$ space filling curve

problem: prove $\mathbb{R}^2$ not homeomorphic to $\mathbb{R}^3$ (not trivial)

Lebesgue covering dimension: $\leq n$

if every open cover has a refinement so that each pt in at most $n+1$ sets (make sets smaller)

← can shrink s.t. every pt in at most 3 sets

$\mathbb{R}^n$ has lebesgue covering dim $= n$ (hard to prove!)

Spec R: fails completely!

Classical defn: Brouwer, Menger, Urysohn:

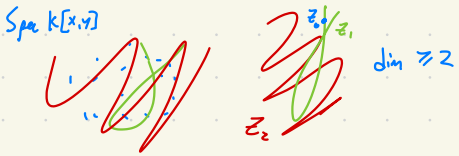
Idea: boundary of X should have smaller dim

Def: A top. space has dim $\leq n$ ($\in \{-1, 0, 1, 2, \dots\}$) if all points have arbitrarily small nbhds with boundary of dim $\leq n$

empty set has dim -1

works for most sets! Difficult to prove $\dim \mathbb{R}^n = n$ though

Krull dimension: $n = \sup\{n \mid \text{exists chain } Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_n \text{ of } n+1 \text{ distinct irreducible subsets}\}$



Works well for Noetherian spaces

Krull dim $\mathbb{R}^n = 0$ ∴ ‖ B-M-U def. (Count this works when Krull fails)

Hausdorff dimension: real, not integer in general

Cover X with balls of radius ε

how many balls needed as $\varepsilon \to 0$?

look at rate $\to N_\varepsilon$

Used for fractals

Deviation of poset P is $\leq \alpha$ (α ordinal)

if for any descending chain $a_0 > a_1 > a_2 > \cdots$ of P

all but a finite number of intervals $[a_i, a_{i+1}]$ have deviation $< \alpha$

Suppose R is noetherian. Look at poset of all ideals.

Works for (1) noncommutative rings

(2) Dimension of modules (different notion from dim of v.s.)

Algebraic definitions:

Idea: Set of high dim should have many functions on it

B = f.g. algebra/k field

integral domain

look at quotient field K of B

dim B := Transcendence degree of K/k [largest # of alg. ind. elements]

$B = k[x,y,z]$ $K = k(x,y,z)$ Tr. deg = 3

"fails" for other rings $\mathbb{Z}$: dim Spec($\mathbb{Z}$) = 1 (Krull)

Tr. deg = 0

Gelfand-Kirillov dim:

f.g. algebras R over field k
↑ can be noncommutative

$$d = \limsup \frac{\log \dim R_n}{\log n}$$

R_n = subspace generated by monomials of deg $\leq n$ in some set of generators (fix this, but independent of choice)

R_n has $\dim \approx n^d$

d need not be an integer
0, 1, ∞, ∉ ℤ

Hilbert polynomial: (local ring R, max ideal $\mathfrak{m}$ ↪ functions on a variety)

$\dim R/\mathfrak{m}^k$

length $R/\mathfrak{m}^k$

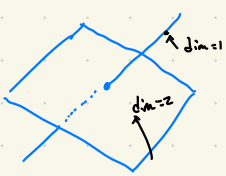
R Noether: length $R/\mathfrak{m}^k$ polynomial in k for k large
↑ degree $d = \dim R$

$\dim k[[x]] = 1$

$k[[x]]/(x^n) \sim k \to$ poly of deg 1

easiest to work with

Dim is local - should really define dim at each point



What about dim of tangent space? → right at nonsingular points, wrong at singular pts (can define singular pt. this way)

Local ring R:

tangent space = (dual) $\mathfrak{m}/\mathfrak{m}^2$ as v.s. over $R/\mathfrak{m}$

↳ # of generators of $\mathfrak{m}$

Gives wrong answer:

$y^2 = x^3$

tangent space has dim = 2

Variation: min num of elements of system of parameters
↑ generates ideal containing $\mathfrak{m}^n$ for $n \gg 1$

good definition yay!

"Homological" definitions

dim beyond which various "homology" groups vanish

$\mathrm{Ext}^i(M,N)$ vanish for $i \geq ?$

$\mathrm{Tor}_i(M,N)$

Min length of projective, injective, flat resolution?

Main 3 defs: (1) Krull
(2) Hilbert polynomials
(3) Systems of parameters

} Same for Noetherian local rings!

Lecture 54: Hilbert Polynomials

Goal: define dim of Noetherian local Ring

Suppose $R = \bigoplus_n R_n$

R_0 Noetherian

R f.g. as algebra over R_0

$\Rightarrow$ R Noetherian (Hilbert's thm)

Suppose $M = \bigoplus_n M_n$ is module

M is f.g. as module

Problem: how fast does M_n grow as $n \to \infty$

↑ what is the size?

"Size" of $M_n = \lambda(M_n) \in \mathbb{Z}$

What is λ? (finite dim. v.s. / R_0)

Easy case R_0 = field $\lambda(M_n) = \dim_{R_0}(M_n)$

Or R_0 = artinian ring $\lambda(M_n) = \text{length}(M_n)$

Need property: $0 \to A \to B \to C \to 0$ (over R_0)

$\lambda(A) + \lambda(C) = \lambda(B)$ "additive"

Poincaré series:

$$P(t) = \sum_{n \geq 0} \lambda(M_n) t^n$$

Theorem: $P(t)$ is a rational function!

$$P(t) = \frac{f(t)}{(1-t^{k_1})(1-t^{k_2})\cdots(1-t^{k_d})}$$

f: polynomial

k_i = degrees of generators of R

Generators of R_0-algebra R are $x_1, \dots, x_s$ with $\deg x_i = k_i$

Induction on s:

$s=0$: trivial. $R = R_0$ $M_n = 0$ $n \gg 0$ $P(t)$ polynomial

$s>0$: $0 \to K_n \to M_n \xrightarrow{\cdot x_s} M_{n+k_s} \to L_{n+k_s} \to 0$

$K = \oplus K_n$ $L = \oplus L_n$

modules over R $x_s = 0$

$\lambda(K_n) - \lambda(M_n) + \lambda(M_{n+k_s}) - \lambda(L_{n+k_s}) = 0$

$P_K(t) - P_M(t) + t^{-k_s} P_M(t) - t^{-k_s} P_L(t) = 0$

$P_M(t) = \frac{P_L(t) - t^{k_s} P_K(t)}{1 - t^{k_s}}$ ← rational fn

Special Case: all x_i have degree 1 ($k_i = 1$)

$P(t) = \frac{\text{poly } t}{(1-t)^s}$

$\frac{1}{(1-t)^s} = \sum_{n \geq 0} t^n \binom{n+s-1}{s-1}$

↑ polynomial in n if $n \geq 0$

So coeffs of t^n in $P(t)$ are polys in n for $n \gg 0$

integer-valued $P(\text{int}) = \text{int}$

What are possible integer-valued polynomials?

obvious examples: $1, t, t^2, t^3$

$\sum n_i t^i$ $n_i \in \mathbb{Z}$

other examples: $\frac{n(n-1)}{2} = \frac{n^2}{2} - \frac{n}{2}$

$\frac{n(n-1)\cdots(n-i+1)}{1 \cdot 2 \cdot \cdots \cdot i} \in \mathbb{Z}$ if $n \in \mathbb{Z}$ $i \geq 0$

$= \binom{n}{i}$

Theorem: Any integer valued polynomial f is an integer linear combination of $\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \cdots$

$\binom{n}{0}$ $\binom{n}{1}$ $\binom{n}{2}$ $\binom{n}{3}$

Proof:

n				
0	1	0	0	0
1	1	1	0	0
2	1	2	1	0
3	1	3	3	1
4	1	4	6	

Given any integer-valued polynomial f of degree d, we can find an integer linear combination of $\binom{n}{0}, \dots, \binom{n}{d}$ of same values at $n = 0, \dots, d$

$f(n) = a_0\binom{n}{0} + a_1\binom{n}{1} + \cdots + a_d\binom{n}{d}$

(degree d) Some $a_0, \ldots, a_d$

for $n = 0, \ldots, d$

So same for all n (forced for this to be int)

Consequence: leading coeff of $f(n)$ is of form $\frac{\text{int}}{d!}$ $x^d + \cdots$

Example: projective variety given by homogeneous ideal $I \subseteq k[x_0, \ldots, x_m]$

$R = k[x_0, \ldots, x_m]/I$ (graded) so $\dim(R_k)$ is poly in k for k large

degree d = dim of variety

$d!$ × leading coeff = degree of variety

$I = (f)$ (f homogeneous, degree m in $n+1$ variables)

$H(k) = \frac{(k+n)\cdots(k+1)}{n!} - \frac{(k+n-m)\cdots(k+1-m)}{n!}$ $\quad k \gg 0$

$\frac{mk^{n-1}}{(n-1)!} + \cdots$

So degree of variety $= m$, dim $= n-1$ } as you'd expect!

Lecture 55: dimension of local rings

(1) Brouwer-Menger-Urysohn

$\dim X \le n$ if every pt. has arbitrarily small nbhds with boundary of dim $< n$

$\dim R := \dim \operatorname{Spec} R$

(2) Krull: $Z_0 \subset Z_1 \subset Z_2 \cdots$

Z_i closed, irred, $Z_i \neq Z_{i+1}$

$\sup\{\text{length(chains)}\} = \dim \operatorname{Spec} R = \dim R$

(3) Hilbert: R $\mathfrak{m}$

Look at $\bigoplus \mathfrak{m}^i/\mathfrak{m}^{i+1}$

$R/\mathfrak{m} \oplus \mathfrak{m}/\mathfrak{m}^2 \oplus \cdots$ ← graded

$\dim R/\mathfrak{m}^n$ is poly in n for $n \gg 0$ (as usual)

degree is dim of R

(4) Parameter: system of parameters: generators for an ideal I ($\mathfrak{m} \supseteq I \supseteq \mathfrak{m}^r$ some r)

dim = min (cardinality of)

$R = k[[x,y]]/(y^2 - x^3)$ Spectrum:

(2) Krull: $(0) \subsetneq (x,y)$ dim = 1

length 1

(3) Hilbert: $R/\mathfrak{m}^n$ $\mathfrak{m} = (x,y)$

$R = k[[t^2, t^3]]$ $\mathfrak{m} = (t^2, t^3, t^4, \dots)$

x y

$\dim R/\mathfrak{m}^n = \underbrace{2n-1}_{\text{degree 1}}$ $n > 0$ so dim = 1

(4) $\mathfrak{m}$ needs 2 generators

$\mathfrak{m} \supseteq (t^2 = x) \supseteq \mathfrak{m}^2$

$\{x\}$ is system of parameters

$\uparrow$ dim = 1

Show equivalent: Krull $\le$ Hilbert $\le$ parameter $\le$ Krull and Krull = B-M-U

(for Noetherian local rings)

Non-Noetherian rings: Krull dim $R[x]$ might be $> 1 + \dim R$

dim any ring R = sup dim $R_{\mathfrak{m}}$

Krull $\uparrow$ $\uparrow$ local rings of points

Krull $\le$ BMU $\leftarrow$ for all top spaces

Suppose $Z_0 \subsetneq Z_1 \subsetneq \cdots$ chain of irreducible closed subsets

We show: BMU dim of Z_i at least i:

pick $p \in Z_i \setminus Z_{i-1}$

$\uparrow$ BMU dim $\ge i-1$ by induction b/c this is irred

Z_{i-1} in boundary of any nbhd of $p \in Z_i \setminus Z_{i-1}$

$\hookrightarrow$ Z_i has BMU dim $> \dim Z_{i-1}$

B-M-U $\leq$ Krull (only for Noetherian spaces)

fails in general $X = \mathbb{R}^1$ → BMU = 1, Krull = 0 (Hausdorff)

We show for any closed subset X, $\text{Krull}(X) \geq \text{BMU}(X)$

FTSOC, pick minimal closed subset violating this (Noetherian)

Can assume this is X

Can assume X irreducible (if $X = Y \cup Z$ pick one)

Suppose $\text{BMU}(X) \geq n$. Pick $p \subseteq U$ body U has BMU dim $\geq n-1$

So Krull dim body $\geq n-1$

get chain $Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_{n-1}$ in body

$Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_{n-1} \subsetneq X$ length n ↯

So $\text{Krull}(X) \geq \text{BMU}(X)$

Lecture 56: Hilbert Polynomial vs System of Parameters

Krull → $\dim(R)$ = (today) Show $\dim(R) \leq \dim(R) \leq \dim(R)$ (Krull)

Hilbert — System of parameters

2 diff Hilbert polys for local ring

$\bigoplus R/m^{n+1}$ $\bigoplus m^n/m^{n+1}$

$\deg \lambda(R/m^{n+1}) = 1 + \deg \lambda(m^n/m^{n+1})$

$\dim(R)$

System of parameters: set of generators of ideal q $m \supseteq q \supseteq m^r$

look at $\bigoplus R/q^{n+1}$

$R/q \oplus R/q^2 \oplus \cdots$

↑ artinian bc $q \supseteq m^r$

$\lambda(R/q^{n+1})$ is poly in n $(n \gg 0)$

$\bigoplus q^n/q^{n+1} = R/q \oplus q/q^2 \oplus \cdots$

# of generators of q

= # " " " " $\bigoplus q^n/q^{n+1}$ over R/q

$\deg \lambda(q^n/q^{n+1}) <$ # gens of $\bigoplus q^n/q^{n+1}$

$\deg \lambda(R/q^{n+1}) \leq$ # gens of q (as ideal)

$\deg \lambda\left(R/m^{nr}\right)$ $\deg \lambda\left(R/q^{n+1}\right)$

$R/m^{nr} \xrightarrow{\text{onto}} R/q^n \xrightarrow{\text{onto}} R/m^n$

$\lambda\left(R/m^{nr}\right) \geq \lambda\left(R/q^n\right) \geq \lambda\left(R/m^n\right)$

$f(nr) \geq g(n) \geq f(n)$

f: Hilbert poly of m; g: Hilbert poly using q

f, g have same degree

$\dim(R) = \deg \lambda\left(R/m^{n+1}\right) = \deg \lambda\left(R/q^{n+1}\right) \leq$ # of gens of q $= \dim(R)$

$\dim(R)$: Hilbert; $\dim(R)$: System of parameters

Lecture 57: Krull vs. Hilbert

$\dim \leq \dim \leq \dim \leq \dim$ (today; ✓)

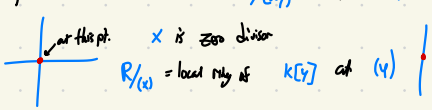
Krull ≤ Hilbert ≤ System of parameters ≤ Krull

Lemma: Suppose $x \in m$ not zero-divisor; m max ideal of Noetherian local ring R

$\text{Hilbert}(R/x) \leq \text{Hilbert}(R) - 1$

[in fact, equality holds]

Example: R = local ring of $k[x,y]/(xy)$ at (x,y)



Proof: $0 \to R \xrightarrow{x} R \to R/xR \to 0$ exact b/c x not zero divisor

$0 \to R/(xR \cap m^n) \to R/m^n \to R/(xR, m^n) \to 0$

$R/(xR \cap m^n)$: not in general R/m^n

$m = (2)$, $n = 1$: $0 \to \mathbb{Z}_{(2)} \to \mathbb{Z}_{(2)} \to \mathbb{Z}/2\mathbb{Z} \to 0$

Hmm $xR \cap m^n$ is stable by strong Artin-Rees.

differs from m^n by (almost) a shift

$m^n \geq xR \cap m^n \geq m^{n+k}$ (fixed k)

$0 \to R/(xR \cap m^n) \to R/m^n \to R/xR \to 0$

So Hilbert polynomials bounded by shift of each other

$f(n) \le g(n) \le f(n+k)$

So have same degree, same leading coeff

So $f-g$ has smaller degree

↑ Hilbert poly of R/xR

has deg < Hilbert poly of R ☒

Krull dim ≤ Hilbert dim:

Suppose krull dim $\ge n$ want to show Hilbert $\ge n$

Pick $P_0 \subsetneq P_1 \subsetneq \dots \subsetneq P_n$ primes

Quotient by P_0 so assume $P_0 = (0)$ ⇒ ring is integral domain.

Pick $x \in P_1 \setminus P_0$ (x not zero divisor)

dim R > dim R/xR by lemma

dim R > Hilbert dim R/xR ≥ Krull dim R/xR ≥ $n-1$

$P_1/(x) \subsetneq \dots \subsetneq P_n/(x)$

dim $R > n-1$

Hilbert → dim $R \ge n$

Lecture 58: System of Parameters vs. Krull

Krull ≤ Hilbert ≤ System of parameters ≤ Krull (today)

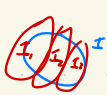
Lemma: (Prime avoidance)

Suppose given (finitely) ideals $P_1, \dots, P_n \subseteq R$

Ideal $I \subseteq R$

Problem: find $x \in I$, $x \notin P_i$

Necessary condition: $I \not\subseteq P_i$



Example: $R = \mathbb{F}_2[x,y]/(x^3, xy, y^2)$ Basis: $1, x, y$

$I = (x,y)$ $I = \{0, x, y, x+y\}$

$P_1 = (x)$ $P_2 = (y)$ $P_3 = (x+y)$

$I \subseteq P_1 \cup P_2 \cup P_3$

Can find x st $x \in I$, $x \notin P_i$ if all P_i are prime.

P_1 not prime: $0 < y^2 \in P_1$

$y \notin P_1$

Proof: Can assume $P_i \not\subseteq P_j$ $i \neq j$

Induction on n (num of idls)

$n=1$: trivial, pick $x \in I$ $x \notin P_1$ bc $I \not\subseteq P_1$

By induction, pick $x \in I$, $x \notin P_1, \dots, P_{n-1}$

If $x \notin P_n$, done.

So can assume $x \in P_n$. pick $y_i \notin P_n$, $y_i \in P_i$ $y \in I$, $y \notin P_n$

not in P_n → $x + y y_1 \dots y_{n-1}$

not in P_i $(i \leq n)$ ↗ in P_n ↑ not in P_n

$y, y_i \notin P_n$

P_n prime

$y_i \in P_i$

$\in I$ ↗ not in P_i $(i \leq n-1)$ In P_i $(i \leq n)$

$x \in I$ $y \in I$

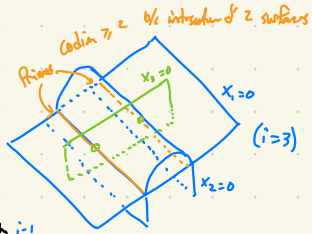
Minimal size of system of parameters $\leq$ krull dim d

Need to find ↗ $(x_1, \dots, x_d)$

Construct as follows: every prime P containing $x_1, \dots, x_i$ has codim $\geq i$

Suppose given $x_1, \dots, x_{i-1}$ find x_i

longest length of $P_0 \subseteq \dots \subseteq P_i = P$



Only finite # of min elements of primes $P_1, P_2, \dots$ containing $x_1, \dots, x_{i-1}$ codim $i-1$

associated prime of $R/(x_1, \dots x_{i-1})$

Now contain m (max idl)

↑ codim $= d > i-1$

So by prime avoidance, can find x_i, $x_i \notin P_1, \dots, P_n$ $x_i \in m$ $(m = I)$

All primes containing $x_1, \dots, x_i$ have codim $\geq i$

finish: show $x_1, \dots, x_d$ is system of parameters.

Any prime containing ↗ has codim $= d = \text{krull}(R)$

only prime of codim $= d$ is max idl m

so $(x_1, \dots, x_d)$ is m-primary so contains power of

max idl m → system of parameters

So min size of system of parameters $\leq$ krull R ☺

⇒ krull = Hilbert = system of parameters yay!

Lecture 59: Krull's principal ideal theorem

Noetherian Local Ring:

Krull = Hilbert = System of parameters

⇒ we can use easiest def to find dim

easy lower bound: $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$ ↑

upper bound: $x_1, \ldots, x_d$ ↑

Application 1: R has same dim as completion $\hat{R}$

$$R/\mathfrak{m}^n \cong \hat{R}/\hat{\mathfrak{m}}^n$$

"Zero of a function have codim 1"

Suppose $x \in$ Noetherian local ring

x not unit or zero divisor

Then $\dim R/x = \dim R - 1$

Cases when zeros do not have codim 1

(1) function x has no zeros at all.

(2) $x \neq 0$, $x = 0$ — x is zero divisor

(3) $x^2 + y^2$ on $\mathbb{R}^2$ ← not whole spectrum of $\mathbb{R}[x,y]$

Corresponds 1-dim pt ⇔ ideal (x^2+y^2)

$(\pm i, 1) \in \mathbb{C}^2 \iff$ ideal (x^2+1, y)

Proof: $\dim(R/x) = \dim(R) - 1$

We have shown $\dim(R/x) \leq \dim R - 1$

to show " $\geq$ "

Pick $x_1, \ldots, x_d$ $d = \dim(R/x)$

↑ system of parameters in R/x

Generate $\mathfrak{m}/(x)$ ~ primary ideal in R/x

Then $x_1, \ldots, x_d, x$ is $\mathfrak{m}$-primary

so $\dim R \leq 1 + \dim(R/x)$

More precise version: Krull's principal ideal theorem:

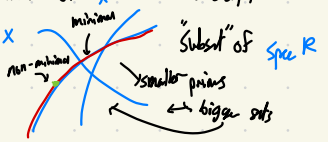
Suppose $x \in R$ not zero divisor (R Noetherian)

All primes *minimal* among ones containing x have codim 1

$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n = P$

max length

Geometric meaning: think of x as a function.

Zeros of x 

Primes containing x $\leftrightarrow$ irreducible subsets of zeros of $x=0$

irred components of zeros of x have codim 1.

Proof: Let $\mathfrak{p}$ minimal among primes containing x

Localize at $\mathfrak{p}$ $\rightarrow$ can assume R local

$\Rightarrow$ can assume $\mathfrak{p}$ is maximal

ideal (x) is $\mathfrak{p}$-primary

so $\{x\}$ is system of parameters for R

$\Rightarrow$ R has $\dim \leq 1$

so $\mathfrak{p}$ has codim 0 or 1

So just need to check $\operatorname{codim} \mathfrak{p} \neq 0$

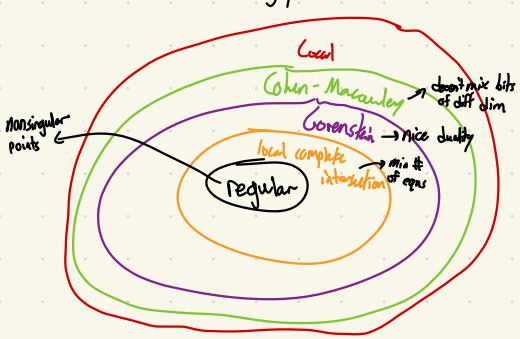
If $\operatorname{codim} \mathfrak{p} = 0$, then $\mathfrak{p}$ is minimal,

so all elements are zero divisors, but $x \in \mathfrak{p}$

and x not a zero divisor.

Lecture 60: Regular Local Rings

R Noetherian local ring, $\mathfrak{m}$ max ideal



Recall: $\dim\left(\mathfrak{m}/\mathfrak{m}^2\right) \geq \dim(R)$

↑ as v.s. over $R/\mathfrak{m}$ ↑ Krull, etc.

Generators for $\mathfrak{m}$ is system of parameters

R is called regular if equality holds.

Examples: $R = k[x,y]/(y^2 - x^3)$ $\leftarrow y^2 = x^3$

localize at origin $\mathfrak{p} = (x,y)$

$\mathfrak{m} = (x,y)$

cotangent space? $\mathfrak{m}/\mathfrak{m}^2$ has dim 2

$\dim R = 1$ $\leftarrow$ ~ point is singular

$R = k[[x_1, \dots, x_n]]$

$\mathfrak{m} = (x_1, \dots, x_n)$

$\mathfrak{m}/\mathfrak{m}^2$ has dim n

$\dim R$? x_n not unit or zero divisor

$\dim R/(x_n) = \dim R - 1$

$= \dim k[[x_1, \dots, x_{n-1}]]$

$\dim R = n$ so R is regular

$k[x_1, \dots, x_n]_{(x_1, \dots, x_n)}$ also regular

$\dim R = \dim \hat{R}$

↑ same cotangent space

Ring S called regular if $S_{\mathfrak{p}}$ regular for all $\mathfrak{p}$

Sufficient to only check $\mathfrak{p}$ maximal

So $k[x_1, \dots, x_n]$ regular.

Complete regular (local) rings: R

Suppose R contains a field mapping isomorphically to $R/\mathfrak{m}$

Ex: $k[[x]]$ $R/\mathfrak{m} = k$

Counterex: $\mathbb{Z}_p$ complete regular local ring doesn't contain field

p-adic

Then $R \cong$ power series ring $k[[x_1, \dots, x_n]]$

Proof: pick $x_1, \dots, x_n$ basis for $\mathfrak{m}/\mathfrak{m}^2$

Get homomorphism

$k[[x_1, \dots, x_n]] \xrightarrow{\text{onto}} R$ ← complete Noetherian local ring

R regular $\Rightarrow$ map is injective

Suppose $a \in$ kernel $k[[x_1, \dots, x_n]]/(a)$ has dim $n-1$

So $\dim R \geq n-1$ but $\dim \mathfrak{m}/\mathfrak{m}^2 = n$, R regular, so kernel must be empty

(not wait) ← otherwise space empty

What about hypersurface $f(x_1,\dots,x_n)$ in $\mathbb{A}^n$

Which points have regular local rings?

Look at point $(0,0,0,\dots)$

What is dimension of local ring $\left(k[x_1,\dots,x_n]/(f)\right)_{(x_1,\dots,x_n)}$

$\dim k[x_1,\dots,x_n] = n$

f not unit or zero divisor.

So $\dim \frac{k[x_1,\dots,x_n]_{(x_1,\dots,x_n)}}{(f)} = n-1$

Dimension of cotangent space $\mathfrak{m}/\mathfrak{m}^2$

$k[x_1,\dots,x_n]_{(x_1,\dots,x_n)}$

$(x_1,\dots,x_n)/(\dots x_i x_j \dots) = n$-dim v.s. spanned by $x_1,\dots,x_n$

hypersurface: $(x_1,\dots,x_n)/(\dots x_i x_j \dots)+(f)$

$= \frac{x_1,\dots,x_n}{\text{linear part of } f}$ ← v.s. spanned by

$\dim = \begin{cases} n & \text{if } f \text{ has no linear part} \\ n-1 & \text{if } f \text{ has a linear part} \end{cases}$

$\dim$ of cotangent space of hypersurface of $f=0$ at a point is either $\begin{cases} n \\ n-1 \leftarrow \text{some partial derivative of } f \text{ is nonzero} \end{cases}$

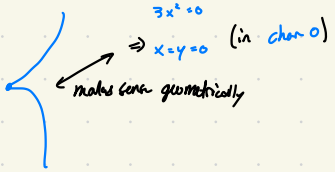
$f = y^2 - x^3$

Singular pts: $y^2 - x^3 = 0$

$2y = 0$

$3x^2 = 0$

$\Rightarrow x = y = 0$ (in char 0)



Lecture 61: Examples of local rings

Non algebraically closed fields in char $p>0$

Variety V over field k

$R = k[x_1,\dots,x_n]/I$

localize at point $(x_1,\dots,x_n) \in k^n$ (alg. closed)

↑ max ideal in non alg. closed

Problem: If local rings at pts are regular, is same true over algebraic closure $\bar{k}$?

$\bar{k}[x_1,\dots,x_n]/I$?

Example: $x^p + y^p = a$

field k char $p>0$, a not p'th power

Max ideal given by (y)

$k[x,y]/(x^p+y^p-a, y) = k[x]/(x^p-a) =$ field

(x^p-a: irreducible)

Localize at y:

Local ring has dim 1, max ideal (y) generated by 1 element,

So ring is regular ✓ cotangent space is one-dimensional

Look at what happens over $\bar{k}$

$\bar{k}[x,y]/(x^p+y^p-a)$

$= \bar{k}[x,y]/(x+y-b)^p$ ← $b^p = a$

has nilpotent elements

Ring is non-regular at every max ideal.

0-dim case:

$x^p - a = 0$ (0-dim)

$(a \neq b^p \quad b \in k)$

$L = k[x]/(x^p-a)$ is a field

$\bar{k}[x]/(x^p-a) = \bar{k}[x]/(x-b)^p$ ← not field, has nilpotent elements

$\| $

$L \otimes_k \bar{k}$

$L \otimes_k M$ L, k, M, fields

$k \subseteq L$, $k \subseteq M$

L finite extension of k

In char 0, $L \otimes_k M$ is product of fields

$L = k[x]/f(x)$ ← irreducible over k

char = 0: all roots are distinct over $\bar{k}$.

$f = f_1(x) f_2(x)$ over M

f_i distinct

$L \otimes_k M = M(x)/f_1(x) \times M(x)/f_2(x) \times \dots$

↑ fields

Stranger in char p:

$L = k[x]/(x^p - a) = M$

$L \otimes_k M = k[x,y]/(x^p - a, y^p - a)$ ← can have multiple roots

↑ not product of fields, has nilpotent elements $(x-y)^p = x^p - y^p = a - a = 0$

In char $p > 0$, $\otimes$ product of two regular rings can be non-regular

Product of two nonsingular varieties can be singular

Zariski: geometrically regular local rings

R over k s.t. $R \otimes_k \bar{k}$ is regular

Example: $k[x]/(x^p - a)$ is regular but not geometrically regular

(Closely related: "smoothness" $R \to S$)

$\mathbb{Z}[\sqrt{-3}]$ order in field $\mathbb{Q}[\sqrt{-3}]$

↑ not UFD: $(1+\sqrt{-3})(1-\sqrt{-3}) = 2 \cdot 2 = 6$

Normalization: $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ ← is an UFD

Maximal ideal of $R = \mathbb{Z}[\sqrt{-3}]$: $\mathfrak{m} = (2, 1+\sqrt{-3})$

$\dim 1$ ← $R/\mathfrak{m} = \mathbb{F}_2$

$R/\mathfrak{m}^2 = \mathbb{Z}_{(2)}[\sqrt{-3}]/(2^2, 2+2\sqrt{-3})$ ← length $= 3$

So $\dim \mathfrak{m}/\mathfrak{m}^2 = 2$

So $\mathbb{Z}[\sqrt{-3}]$ not regular at $(2, 1+\sqrt{-3})$

$\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ is regular (at all max ideals)

localization is D.V.R. ⇒ regular

⇒ makes pts in spec nonsingular

$\mathbb{Z}[\sqrt{-3}] \subseteq \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$

(2) not prime ↑ not regular — (2) prime ideal ↑ regular — inverse image is $(2, 1+\sqrt{-3})$

↑ not inverse image of

$\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]/(2) = \mathbb{F}_2$

Lecture 62: Cohen-Macaulay local rings

Regular → local complete intersection → Gorenstein → Cohen-Macaulay → local

today!

Recall: (R, m) (Noetherian) local ring, max ideal

If $x \in R$ not zero divisor or unit,

$\dim R/x = \dim R - 1$

x_1 not zero divisor, unit in R

x_2 " " " " $R/(x_1)$

x_3 " " " " $R/(x_1, x_2)$

$\vdots$

$x_1, x_2, x_3, \ldots$ is a regular sequence

Length of seq $x_1, \ldots, x_n = n \leq \dim(R)$

Ring is C-M if we can find a regular seq of length $= \dim R$

$\leftrightarrow$ depth $=$ dim

Example: (1) Any local ring of $\dim 0$ is C-M

(2) Any regular local ring is C-M

Regular (local) $\Rightarrow$ integral domain

$R \quad R/m \oplus m/m^2 \oplus \cdots$

$\cong$ polynomial algebra

$=$ integral domain

$\Rightarrow R$ also integral domain

$ab = 0$ in R

$a \in m^i \quad b \in m^j$

$a \notin m^{i+1} \quad b \in m^{j+1}$

image of ab in $m^{i+j}/m^{i+j+1} \neq 0$

x_1 = element of $m \setminus m^2$

$R/(x_1)$ also regular. So repeat.

Not C-M: $R = k[[x,y]]/(x^2, xy)$ $\quad m = (x, y)$

All elements of m are zero divisors $\rightarrow$ depth $R = 0$

but $\dim R = 1$

(Non)-Example: no nilpotent elements

$R = k[x,y,z]/(xz, yz)$

$\hat{R} = k[x,y,z]/(yz, yz)$

Pick non-zero divisor $x_1 = x+z$

$k[x,y,z]/(xz, yz), (x+z)$

$= k[x,y]/(x^2, yx)$

= ring of previous example, all elements of max ideal are zero divisors

depth = 1 but dim = 2

$\Rightarrow$ not C-M

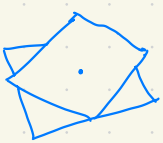
Not equidimensional

in general, CM $\Rightarrow$ equidimensional

$\not\Leftarrow$?

not quite, need more

Example: equidimensional ring, no nilpotents, not C-M



2 planes meet at point in $\mathbb{A}^4$

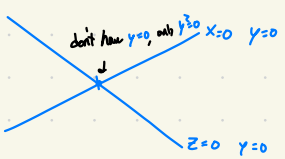
$w=x=0$

$y=z=0$

$k[w,x,y,z]/(wy, wz, xy, xz)$

Pick non zero divisor $x_1 = w-y$ $\quad R = k[w,x,y,z]/(wy, wz, xy, xz)$

$R/_{(x_1)} = k[x,y,z]/(y^2, yz, xy, xz)$



All elements of max ideal of $R/_{(x_1)}$ are zero divisors

depth R = 1 dim = 2

Want to show: any 2 (maximal) regular sequences in Noetherian local ring have same length

define depth for a module m

Regular sequence for M:

$x_1, x_2, \ldots, x_n \qquad x_i \in m$

x_1 not zero divisor of M

x_2 " " " " $M/(x_1)$

$\vdots$

TFAE: (1) There is a regular sequence for M, $x_1, \dots, x_n$ of length n

(2) $\mathrm{Ext}^i(R/\mathfrak{m}, M) = 0 \quad (i < n)$

(3) Any regular sequence can be extended to one of length n

(trivial: (2) $\Rightarrow$ (1), (3) $\Rightarrow$ (2))

Pf (1 $\Rightarrow$ 2): $x_1, \dots, x_n$ regular. Want to show: $\mathrm{Ext}^i(R/\mathfrak{m}, M) = 0 \quad (i < n)$

Induction: $= 0$ for $i < n-1$

$0 \to M \xrightarrow{x_1} M \to M/x_1M \to 0$ exact

(exact b/c x_1 not zero divisor)

$$\mathrm{Ext}^{i-1}(R/\mathfrak{m}, M/x_1M) \to \mathrm{Ext}^i(R/\mathfrak{m}, M) \to \mathrm{Ext}^i(R/\mathfrak{m}, M)$$

0 by induction $\longrightarrow$ injective and zero map

x_1 is 0 on $R/\mathfrak{m}$ $(x_1 \in \mathfrak{m})$

so $\mathrm{Ext}^{n-1}(R/\mathfrak{m}, M) = 0$

(2 $\Rightarrow$ 3): ($\mathrm{Ext}^i(R/\mathfrak{m}, M) = 0$ for $i < n$ $\Rightarrow$ any regular sequence can be extended to length n)

Suppose $n = 1$ so (2) $\Rightarrow \mathrm{Hom}(R/\mathfrak{m}, M) = 0$

So $\mathfrak{m}$ not associated prime of M

zero divisors $= \bigcup$ associated primes $\neq \mathfrak{m}$

So $\mathfrak{m}$ has non zero divisor!

So there is a regular sequence of length 1.

for $n > 1$: pick non zero divisor $x_1 \in \mathfrak{m}$

apply induction to M/x_1M (similar property to (2) with $n-1$)

Corollary 1: any two maximal regular sequences of M (or R) have same length.

Corollary 2: any quotient of regular local ring by regular sequence $x_1, \dots, x_n$ (possibly non-maximal) is C-M.

$R/(x_1, \dots, x_i)$ dim $= \dim R - i$

so this has regular sequence of length $\dim R - i = \dim$

Example: any hypersurface singularity is C-M.

Lecture 63: Koszul complex

R $\qquad$ $R/(x_1, \dots, x_n) \neq 0$

regular sequence $\to x_1, x_2, \dots$

not zero divisor in R, $R/(x_1)$, $R/(x_1, x_2)$

Q: Is a permutation of a regular sequence also regular?

A: No in general $\quad K[x, y, z]/(xz)$

$x-1, \ xy$ regular

$xy, \ x-1$ <u>not</u> regular

(xy: zero divisor!)

True if R is a local ring!

$x_1, \dots, x_n \in m$ (max ideal)

Koszul complex of $(x_1, \dots, x_n)$

$n=1$: x_1 $\qquad 0 \to R \xrightarrow{\cdot x_1} R \to R/(x_1) \to 0$ $\qquad$ exact if x_1 not zero divisor

$n=2$: x_1, x_2 $\qquad 0 \to R \xrightarrow{d} R^2 \xrightarrow{d} R \xrightarrow{d} R/(x_1, x_2) \to 0$

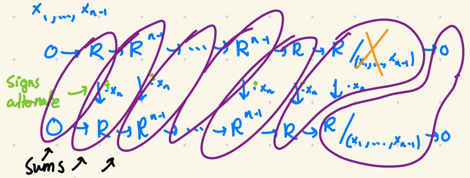
$1 \mapsto (x_1, x_2)$

$(a, b) \mapsto (x_2 a - x_1 b)$ $\quad$ ($d^2 = 0$)

General:

$$0 \to R \to R^n \to R^{\binom{n}{2}} \to \cdots \to R^{\binom{n}{n-2}} \to R^{\binom{n}{n-1}} \to R^{\binom{n}{n}} \to R/(x_1, \dots, x_n) \to 0$$

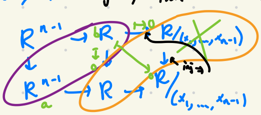
$$\cdots \to \Lambda^2(R) \to \Lambda^1(R) \to R$$



$$0 \to R \to R^n \to \cdots \to R^n \to R \to R/(x_1, \dots, x_n) \to 0$$

Koszul complex doesn't depend on order of $x_1, \dots, x_n$ (up to isomorphism)

If $x_1, \dots, x_n$ is regular, then Koszul complex is exact



x_n injective on $R/(x_1,\dots,x_{n-1})$ $\Rightarrow$ exactness

↳ $x_1,\dots,x_n$ is regular $\Rightarrow$ Koszul complex exact

If $x_1,\dots,x_n$ is regular, we get finite free resolution of module $R/(x_1,\dots,x_n)$

Problem: If Koszul complex is exact, is $x_1,\dots,x_n$ regular

A: No in general (example from beginning of lecture)

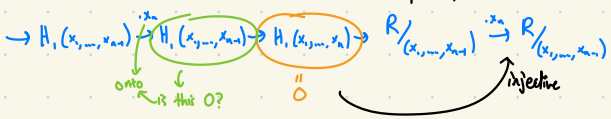
Yes if R is a local ring

R local $\Rightarrow$ permutation of regular seq. is regular

$H_i(x_1,\dots,x_n)$ ith homology of Koszul complex on $x_1,\dots,x_n$

Long exact sequence:

exact by splicing construction



If $x_1,\dots,x_{n-1}$ regular,
so is $x_1,\dots,x_n$

R local: Nakayama's lemma:

If M is f.g. R-module and $\mathfrak{m}M = M$
($\mathfrak{m}$ = max ideal) then $M = 0$

$M = H_1(x_1,\dots,x_{n-1})$

$x_n : M \to M$ onto by assumption

$x_n \in \mathfrak{m}$ local ring → elements of regular sequence must be in max ideal

So $\mathfrak{m}M = M$ so $M = 0$

$H_1(x_1,\dots,x_{n-1}) = 0$ → by induction, $x_1,\dots,x_n$ is regular (order doesn't matter)

Lecture 64: Gorenstein Rings

↑ local, Noetherian

Duality property

0-dim case: $k = R/\mathfrak{m}$ $\mathfrak{m}$ max ideal

$\dim R = 0 \Rightarrow R$ Gorenstein $\iff \mathrm{Hom}_R(k,R)$ is 1-dim (over k as v.s.)

Dual of module $D(M) = \mathrm{Hom}_R(M,R)$

R Gorenstein $\Rightarrow D(M)$ behaves well

i.e. $D(D(M)) \cong M$

[General def of dual is $\mathrm{Hom}_R(M,\omega)$ → dualizing module]

← length 5 as module over itself

Examples (0-dim) $R = k[[x]]/(x^5)$

$\mathrm{Hom}_R(k,R)$: $\dim = 1$ spanned by x^4

→ one block on bottom

$R = k[x,y]/(x^2, xy, y^2)$

↑ two blocks on bottom

$\dim \mathrm{Hom}_R(k,R) = 2$

↑ not Gorenstein!

$R = k[x,y]/(x^2, y^2)$

$\dim \mathrm{Hom}_R(k,R) = 1$ ← one on bottom

↳ Gorenstein

"looks the same if you flip it upside down"

Grothendieck:

R has $\dim = d$, Gorenstein if $\mathrm{Ext}^i(k,R)$ is 0 for $i \neq d$, $\dim = 1$ if $i = d$

(Note $\mathrm{Ext}^0 = \mathrm{Hom}$)

Ubiquity of Gorenstein rings

↳ "everywhere present"

Simpler criterion: If $\dim R > 0$, then R is Gorenstein iff R has non zero divisor $x \in m$ s.t. $R/(x)$ is Gorenstein

↑ any non zero divisor will do

Look at $0 \to R \xrightarrow{\cdot x} R \to R/(x) \to 0$

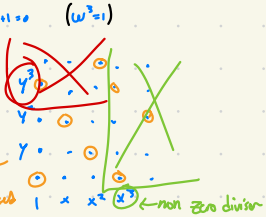
Examples: $k[[x,y]]$ acted on by $\mathbb{Z}/3\mathbb{Z}$

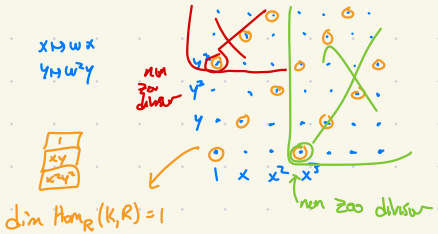
look at fixed subring

$x \mapsto \omega x$ $\quad y \mapsto \omega y$ $\quad \omega^2 + \omega + 1 = 0$ $\quad (\omega^3 = 1)$ $\quad$ (char $k \neq 3$)

$\dim \mathrm{Hom}_R(k,R) = 2$

not Gorenstein





Gorenstein!

Singularities of curves in $\mathbb{A}^2$

$\mathbb{A}^1 \to \mathbb{A}^2$

$t \mapsto (t^4, t^5, t^6, t^7)$

$t \mapsto (t^5, t^6, t^7, t^8)$

$t \mapsto (t^6, t^7, t^8, t^9)$

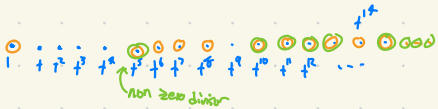
look similar
Hard to tell which is Gorenstein

only Gorenstein one

look at local ring at $(0,0,0,0)$

$R/(t^4)$

$\dim \mathrm{Hom}_{R/(t^4)}(k, R/(t^4)) = 3$ not Gorenstein



$R/(t^5)$:

$\mathrm{Hom}_{R/(t^5)}(k, R/(t^5))$

$t^6 \cdot t^{10} = t^{13} \neq 0$

$t^7 \cdot t^7 = t^{13} = 0$

spanned by

$\dim = 1$

Gorenstein

$R/(t^6)$ 1 t^7 t^8 t^9

t^{16} t^{18}

Hom 2-dim spanned by

Not Gorenstein

Regular rings are Gorenstein.

Koszul complex:

R want: $\mathrm{Ext}^d_R(k,R)$ has length 1

Pick $x_1,\dots,x_d$ basis for $\mathfrak{m}/\mathfrak{m}^2$ (R regular)

Koszul complex:

$$0 \to R \to R^d \to R^{\binom{d}{2}} \to \cdots \to R^d \to R \to R/(x_1,\dots,x_d) \to 0$$

$R/(x_1,\dots,x_d) \cong k$

Use this to compute $\mathrm{Ext}^d_R(k,R)$

Homology of $0 \leftarrow R \leftarrow R^d \leftarrow$ ($\leftarrow (a_1,\dots,a_d)$, $(x_1a_1 + x_2a_2 + \cdots)$)

$= R/(x_1,\dots,x_d) = k$

Lecture 65: Fitting Ideals

↑ Just some guy's name

f.g. module M over any ring R

$\mathrm{Fit}_0(M) \subseteq \mathrm{Fit}_1(M) \subseteq \cdots$

$\mathrm{Fit}_n(M)$ is a sort of obstruction to generating M by n elements

↓ or $R/\mathrm{Fit}_n(M)$ ← vanishes

If M generated by n elements

$\mathrm{Fit}_0(M)$

Presentation:

$$R^{\#} \to R^n \to M \to 0$$

↑ relations (possibly infinitely generated)

↑ basis corresp. generators $g_1,\dots,g_n$ of M

$r_{11}g_1 + \cdots + r_{1n}g_n = 0$

$r_{21}g_1 + \cdots + r_{2n}g_n = 0$

$\begin{pmatrix} r_{11} & \cdots & r_{1n} \\ r_{21} & \cdots & r_{2n} \\ \vdots & & \end{pmatrix}$ n columns, possibly infinite rows

$\mathrm{Fit}_0(M)$ = ideal generated by dets of all $n \times n$ minors

Problem: seems to depend on presentation.

How can you change a presentation?

(1) Add new generator g
add new relation: $g = r_1 g_1 + \cdots + r_n g_n$

(2) Add new relation as linear combination of known relations
(or ∞ # of new relations)

Any 2 presentations are related by these operations and their inverses

$$R^k \to R^m \to M \to 0$$
$$R^k \to R^n \to M \to 0$$

Fitting ideal of M does not change under steps 1 & 2

Step 1:

$$\begin{pmatrix} r_1 & \cdots & r_n & 1 \\ r_{11} & \cdots & r_{1n} & 0 \\ r_{21} & \cdots & r_{2n} & 0 \\ & & & 0 \\ & & & 0 \\ & & & 0 \\ & & & 0 \end{pmatrix}$$

one new row, column

$\det(n \times n)$
$\det(n+1 \times n+1)$ } same dets up to sign

Step 2:

$$\begin{pmatrix} r_{11} & \cdots & r_{1n} \\ r_{21} & \cdots & r_{2n} \\ & & \\ & & \\ & & \\ r_1 & \cdots & r_n \end{pmatrix}$$

Again doesn't change things

Example: M = finite abelian group ($\mathbb{Z}$-module)

$\text{Fitt}_0(M)$? $M = \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots$

$$\begin{pmatrix} n_1 & & \\ & n_2 & \\ & & \ddots \end{pmatrix}$$

$\det = n_1 n_2 \cdots n$

$\text{Fitt}_0(M) = (|M|)$ $\quad \mathbb{Z}/\text{Fitt}_0(M)$ = Cyclic abelian group of same order

$\text{Fitt}_i(M)$ defined in same way $\quad R^k \to R^n \to M \to 0$

$$\begin{pmatrix} r_{11} & \cdots & r_{1n} \\ r_{21} & \cdots & r_{2n} \\ & & \\ & & \end{pmatrix}$$

Take ideal generated by dets of $(n-i)\times(n-i)$ minors.
As before, doesn't depend on presentation

Example: M f.g. abelian group

$$M = \mathbb{Z}^j \oplus \left(\mathbb{Z}/n_1\mathbb{Z}\right) \oplus \cdots \oplus \left(\mathbb{Z}/n_k\mathbb{Z}\right)$$

$$n_1 \mid n_2 \quad n_2 \mid n_3 \quad \cdots$$

Presentation:

$\left.\begin{array}{l} \text{Fitt}_0(M) = 0 \\ \vdots \\ \text{Fitt}_j(M) = 0 \\ \text{Fitt}_{j+1}(M) = (n_1 n_2 \cdots n_k) \\ \text{Fitt}_{j+2}(M) = (n_1 n_2 \cdots n_{k-1}) \\ \text{Fitt}_{j+k}(M) = (1) \end{array}\right\}$ completely determined by sequence of fitting ideals

$\mathbb{Z}/\text{Fitt}_i(M) \overset{(min)}{=}$ size of what is left after killing i elements of M

for any M, M generated by i elements $\Rightarrow \text{Fitt}_i(M) = R$

Converse true for f.g. modules over $\mathbb{Z}$ or local rings.

Lecture 66: Local complete intersection rings

L.C.I.

regular $\subseteq$ L.C.I. $\subseteq$ Gorenstein $\subseteq$ C-M $\subseteq$ local

L.C.I ring: regular local ring R

$R/(x_1, \ldots, x_i)$ $x_1, \ldots, x_i$ is regular sequence

Geometric meaning: variety $\subseteq \mathbb{A}^n$

codim k

needs $\geq k$ equations to define it

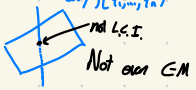
If we can def. local ring at pt with k equations $\Rightarrow$ L.C.I. ring

Examples: (1) Regular $\Rightarrow$ L.C.I.

(2) Any hypersurface sing. is L.C.I.

$R/(x_1)$

$k[[x_1,\dots,x_n]]_{(x)}/f(x_1,\dots,x_n)$

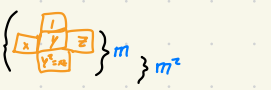
(3) 

Recall L.C.I. $\Rightarrow$ Gorenstein

Problem: find example of Gorenstein ring not L.C.I

Example: $R = k[[x,y,z]]/(x^2, xy, yz, z^2, y^2-x^3)$

Gorenstein: $\dim R = 0$ length $= 5$



V v.s. over k $\quad (\ ,\ )$ ← symmetric bilinear form

$V \otimes V \to k$

$k \oplus V \oplus k$ ← m^2 $\quad V \times V \to k$ is bilinear form

m

Bilinear form on V nondegenerate $\Rightarrow$ ring is Gorenstein

$\dim \mathrm{Hom}_k(k, R) = 1$

Not L.C.I.: informal argument:

$R = k[[x,y,z]]/(\text{ideal})$

Ideal $\subseteq M^2$ $\quad M = (x,y,z)$ in $k[[x,y,z]]$

M^2/M^3 has $\dim = 6$

Spanned by $x^2, xy, y^2, xz, z^2, yz$

Need to kill off 5-dim subspace of $\underbrace{M^2/M^3}_{\text{v.s. over } k}$

Needs ≥ 5 relations

$\dim k[[x,y,z]] = 3$

so if R is L.C.I., we should use at ≤ 3 relations

Theorem: 0-dim Noetherian ring is L.C.I $\Leftrightarrow$ $\mathrm{Fitt}_0(M) \neq 0$

Extension to higher dimensions: (Wiles)

Local ring R with $\dim > 0$ is L.C.I if $R/(x)$ is L.C.I.

x, not unit, zero-divisor

Example: $R = k[x,y,z]/(x^3, xy, yz, z^2, y^5 - xz)$

m = max ideal

$\mathrm{Fitt}_i(m)$ m module with 3 generators x, y, z

relations for m:

	x	y	z	
x	0	0		$x^2 = 0$
y	0	0		$yx = 0$
0	x	0		
0	0	z		$z^2 = 0$
0	z	0		$yz = 0$
0	0	y		
0	y	-x		$y^2 = xz$
-z	y	0		

$R \supseteq m \supseteq m^2$ (length 5, length 4, length 1)

$\mathrm{Fitt}_0(m) = 0$

So R not L.C.I.

$\mathrm{Fitt}_1(m) = (m^2) = (xz)$

2×2 dets

$\mathrm{Fitt}_2(m) = (x, y, z) = m$

1×1 dets

$\mathrm{Fitt}_3(m) = (1) = R$

0×0 dets

Geometric example: 1-dim, reduced (no nilpotents)

R $k[[t^5, t^6, t^7, t^8]]$

Gorenstein (earlier lecture)

Not L.C.I.

Quotient by non zero divisor such as t^5

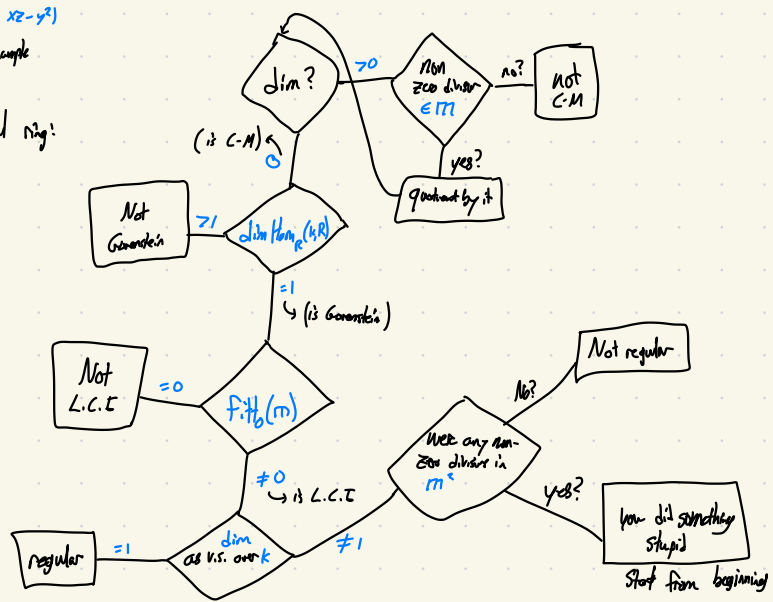
Length $R/(t^5) = 5$ basis $1, t^6, t^7, t^8, t^{14}$

$1 \quad x \quad y \quad z \quad xz = y^2$

$= k[[x,y,z]]/(x^2, xy, yz, z^2, xz - y^2)$

not L.C.I. by previous example

Summarize: how to test a Noetherian local ring:



Lecture 67: The Bernstein-Sato Polynomial: Introduction

* Exterior algebra $\Lambda(V)$

$xy = -yx$

* Ring of differential operators $\mathbb{C}\left[x, \frac{d}{dx}\right]$

Leibniz rule: $\frac{d}{dx} \cdot x = x \cdot \frac{d}{dx} + 1$

* Clifford algebra: $ab + ba = (a,b)$ ← inner product

Non commutative but ab closely related to ba.

$ab \neq ba$ or $-ba$) plus something "simpler"

→ Bernstein-Sato Polynomial

Gamma function $\Gamma(s) = \int_0^\infty e^{-t} t^{s-1} dt$ (diff, int)

Converges: $\mathrm{Re}(s) > 0$

Integrate by parts: $\Gamma(s) = \frac{1}{s}\Gamma(s+1)$ (meromorphic)

↑ extend Γ to all complex s (possibly with poles)

$\frac{d}{dt} t^{s+1} = (s+1)t^s$ $\quad f(s) = t \quad b(s) = s+1$

Bernstein-Sato poly: $b(s)$

f poly in $x_1, \dots, x_n$

$p(s) f(x)^{s+1} = b(s) f(x)^s$ (b: poly in s)

↑ differential operator in $x_1, \dots, x_n, \frac{d}{dx_1}, \dots, \frac{d}{dx_n}$

Converges for $s > 0$ $\quad \int_{\mathbb{R}^n} \varphi(x) f(x)^s dx \quad f > 0$

$\Rightarrow$ extend to $s \in \mathbb{C}$ ↑ nice fn: smooth, compact support, etc. (somewhat stronger than necessary)

$f(x_1, \dots, x_n) = x_1^2 + \cdots + x_n^2$

$\left(\frac{\partial^2}{\partial x_1^2} + \cdots + \frac{\partial^2}{\partial x_n^2}\right)\left(x_1^2 + \cdots + x_n^2\right)^{s+1} = 4(s+1)\left(s+\frac{n}{2}\right)\left(x_1^2 + \cdots + x_n^2\right)^s$

$b(s) = (s+1)\left(s+\frac{n}{2}\right)$ (leading coeff is 1)

$p(s) = \frac{1}{4} \sum \frac{\partial^2}{\partial x_i^2}$

Example: $f(x,y) = x^2+y^3$

hard to find b-s poly

$b(s) = (s+1)(s+\frac{5}{6})(s+\frac{7}{6})$

Theorem: Every nonzero complex poly f has Bernstein-Sato polynomial

Proof: ideas from commutative algebra

Corollary: Malgrange-Ehrenpreis thm

Every differential operator D with constant coeffs

has a fundamental solution f

$Df = \delta$ (Dirac delta "function") — distribution

in $x_1, \dots, x_n$

Can solve $Df = g$ for reasonable g

Solve $Df = \delta$

Take fourier transform: $\frac{d}{dx} \to x$

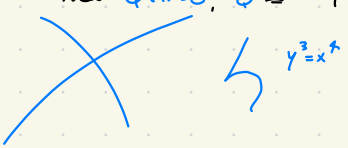
$Q\hat{f} = 1$

poly, distribution

Solve: $\hat{f} = \frac{1}{Q}$? Yes, if Q everywhere nonzero

Problem: what if Q has zeros?

Near $Q(x) = 0$, $\frac{1}{Q}$ not locally integrable.



Sledgehammer: Hironaka's thm

Easier: B-S polynomial

Can assume $Q \geq 0$ $\frac{1}{Q} = \frac{\bar{Q}}{Q\bar{Q}}$ $\} \geq 0$

Q^s is Holomorphic for $Re(s) \geq 0$

Using B-S poly, can continue Q^s as meromorphic function of s to $s \in \mathbb{C}$

taking values in distributions

$\int \varphi Q^{(s)} dx^n$ meromorphic in s for any nice φ

Poles: related to zeros of $b(s+n)$ ← B-S poly

Q^{-1} Q^{-1} might have pole at $s=-1$
(no pole = dark)

$$Q^{s-1} = Q_{-m}s^{-m} + Q_{1-m}s^{1-m} + \cdots + Q_0 s^0 + \cdots$$

Laurent series coeffs Q_k distributions

Multiply by Q:

$$Q^s = QQ_{-m}s^{-m} + \cdots + QQ_0 s^0 + \cdots$$

$= 0 \quad 0 \quad 0 \quad 1 \quad + (\quad)$ ← holomorphic at $s=0$

$$QQ_{-m}=0, \ldots, QQ_{-1}=0, \quad QQ_0 = I$$

Q_0 is an inverse of Q

$\tilde{Q}_0$ is fundamental solution ← fourier transform

$$QQ_{-m} = 0 \quad \cdots \quad QQ_{-1} = 0$$

So many inverses of Q:

$Q_0 + (\text{linear comb. of } Q_{-m}, \ldots, Q_{-1})$

Element of ring has ≤ 1 inverse

$$QA = I \quad QB = I$$
$$B = BQA = A$$

[(1) Product of distributions not always defined]

(2) When product is defined, it need not be associative. ← real reason why we don't get a contradiction

$\frac{1}{x} \times \delta$ ← dirac delta, distribution

$x\delta = 0$ $\quad \frac{1}{x} \cdot x = 1$

$(\frac{1}{x} \cdot x)\delta = \delta$
$\frac{1}{x}(x \cdot \delta) = 0$

Lecture 68: The Bernstein-Sato Polynomial: Bernstein's inequality

Bernstein's inequality: modules over Weyl Algebra

$$A = \mathbb{C}[x_1, \ldots x_n, \partial_1, \ldots, \partial_n]$$ ← non commutative (but close)
$\partial = \frac{\partial}{\partial x_i}$

$x_i x_j = x_j x_i$
$\partial_i \partial_j = \partial_j \partial_i$
$\partial_i x_j = x_j \partial_i$ if $i \neq j$
$\partial_i x_i = x_i \partial_i + 1$ (Leibniz rule)

Module over A: A/I $\longleftrightarrow$ system of diff. eqns.

$\underbrace{\mathrm{Hom}_A(A/I, \text{smooth fns})}_{\text{solutions to diffeqns in } I}$.

Center of A? $A = \mathbb{C}[x_1,\dots,x_n,\partial_1,\dots,\partial_n]$

A: Center of A is $\mathbb{C}$.

Proof: $D \to x_1 D - D x_1$ $\quad D \mapsto x_i D - D x_i$

anything commuting with all x_i, ∂_i is in $\mathbb{C}$

- $\mathbb{C}$-linear map $A \to A$
- Kernel of all is polynomials in $x_1,\dots,x_n$
- Kernel of $D \mapsto \partial_i D - D\partial_i$ (all i)
- is polynomials in $\partial_1,\dots,\partial_n$

(Warning: we make use of $\mathrm{char}\ \mathbb{C} = 0$
In $\mathrm{char} = p > 0$, center contains ∂_i^p bc $x_i\partial_i^p = \partial_i^p x_i$
↑ there are other differential operators "$\frac{\partial^p}{p!}$")

Convert Weyl algebra into commutative algebra:

Bernstein filtration of A:

$A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdots$

$A_0 = \mathbb{C}$

A_i: spanned by all monomials in $x_1,\dots,x_n,\partial_1,\dots,\partial_n$ of degree $\le i$

$A_i A_j \subseteq A_{i+j}$

If $p \in A_i$, $q \in A_j$

$pq - qp \in A_{i+j-1}$

$R = A_0 \oplus A_1/A_0 \oplus A_2/A_1 \oplus \cdots$

This is a commutative, polynomial ring in images of x_i, ∂_i

M is module over A generated by complex v.s. M_0

$M_i = A_i M_0$

$A_i M_j \subseteq M_{i+j}$

$M_0 \oplus M_1/M_0 \oplus M_2/M_1 \oplus \cdots$ "same size as A"

is module over $R = A_0 \oplus A_1/A_0 \oplus \cdots$

"same size as M"

Apply Hilbert polys to M. Assum $\dim_{\mathbb{C}} M_0 < \infty$

$\dim_{\mathbb{C}}(M_i)$ is poly in i for $i \gg 0$

$\dim(M)$ = deg of $\dim_{\mathbb{C}}(M_i)$

↑ ring theoretic def ↑ dim of v.s.

$\text{mult}(M) = \underbrace{\dim(M)! \times \text{leading coeff}}_{\text{integer}}$

$\dim(M)$ and $\text{mult}(M)$ independent of M_0

Changing "basis" of M_0 changes Hilbert poly by at most "finite shift"

So have same degree and leading coeff

In commutative case, M module over $\mathbb{C}[x_1, \dots, x_n]$

$\dim M$ can be any int from 0 to $2n$

Bernstein's inequality: if $M \neq 0$, $\boxed{\dim M \geq n}$ $(\dim M \leq 2n)$

Proof: Key point: map from A_i to $\text{Hom}_{\mathbb{C}}(M_i, M_{2i})$ is injective

Suppose $aM_i = 0$ $a \in A_i$. want to show $a = 0$.

Induction on i. $i < 0$: trivial: $A_i = 0$

Assume true for $i-1$

$a \in A_i$ $aM_i = 0$

commutator → $[a, \partial_j] \in A_{i-1}$ $aM_i = 0$

$[a, \partial_j] M_{i-1} = 0$ so $[a, \partial_j] = 0$ by induction.

Similarly $[a, x_j] = 0$

So $a \in$ center of A.

$a \in \mathbb{C}$

and $aM_i = 0$

so $aM = 0$ $M \neq 0$

$\Rightarrow a = 0$

$A_i \leq \text{Hom}(M_i, M_{2i})$

$\dim_{\mathbb{C}}$ is poly of degree $2n$ ↓ ↑ ↑ dim both poly's of deg = $\dim(M)$ ↓ ring theoretic

poly of $\leq 2\dim(M)$

$\boxed{\dim(M) \geq \frac{2n}{2} = n}$ ∎

If $\dim M = n$ M is called holonomic module.

Lecture 69: Holonomic Modules

Weyl algebra $A = \mathbb{C}[x_1, \dots, x_n, \partial_1, \dots, \partial_n]$ where $\partial_i = \frac{\partial}{\partial x_i}$

M module over A:

Bernstein: $\dim(M) \geq n$ (if $M \neq 0$)

$\dim$ = deg of Hilbert poly

Holonomic = f.g. & $\dim = n$ or 0

Thm: Holonomic modules have finite length

(1) Hilbert poly is additive on exact sequences

→ leading coeff " " "

for Holonomic modules as Hilbert poly has $\dim = n$

So multiplicity is additive

↑ $(\dim)! \times$ leading coeff

always integer ≥ 0

$= 0 \iff$ module $= 0$

≤ length of hol. module ≤ mult. → finite

Suppose M is module over A (not known to be f.g.)

has filtration $M_0 \subseteq M_1 \subseteq \dots$

$\dim_{\mathbb{C}}(M_i) \leq$ poly in i of deg n

Then M is f.g. and so Holonomic

Proof: (1) Every f.g. submodule holonomic of mult $\leq n! \times$ leading coeff of

find chain of f.g. submodules

$M^0 \subseteq M^1 \subseteq M^2 \cdots$ lengths of M_i bounded by

Corollary: $M = \mathbb{C}[x_1, \dots, x_n][\rho^{-1}]$ ← module over A

↑ ρ = some poly

then M is holonomic

Proof: $M_k = \left\{ f/\rho^k \;\middle|\; \deg f \leq (m+1)k \right\}$ $m = \deg \rho$

$A_i M_k \subseteq M_{k+i}$

$\dim(M_k) \leq \binom{(m+1)k+n}{n}$ = poly in k of deg $\leq n$

≤ by previous lemma, M f.g. ⇒ holonomic

Existence of Bernstein Poly of $p \in \mathbb{C}[x_1, \dots, x_n]$

$b(s) = \text{Poly}(x_i, \partial_i, s)\, p^{s+1}$

↑ B-S Poly

Work over field $k = \mathbb{C}(x)$ ← rational functions over s

$\mathbb{C}(s)[x_1, \dots, x_n, p^{-1}]p^{-s}$

↑ Holonomic over $A = \mathbb{C}(x)[x_1, \dots, x_n, \partial_1, \dots, \partial_n]$

Look at $Ap^s \supseteq Ap^{s+1} \supseteq Ap^{s+2} \supseteq \dots$

Decreasing chain in module of finite length

so eventually constant.

$Ap^{s+k} = Ap^{s+k+1}$ for some k

so $p^{s+k} = Q(x_i, \partial_i)p^{s+1+k}$

↑ poly with coeffs in $\mathbb{C}(s)$

so $p^s = Q(x_i, \partial_i)p^{s+1}$

coeffs in $\mathbb{C}(s)$

↑ rational funcs in s

Put $b(s)$ = common denominator

$b(s)p^s$ = poly in $(x_i, \partial_i, s) \times p^{s+1}$

↑ B-S polynomial! ☑

Lecture 20: Dedekind domains: introduction

Example: $\mathbb{Z}[\sqrt{-5}]$ ← non UFD

$m + n\sqrt{-5}$ $\quad m, n \in \mathbb{Z}$

$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

Kummer: $(2) = (2, \overset{A}{1+\sqrt{-5}})(2, \overset{B}{1-\sqrt{-5}})$

Ideals $(3) = (3, \overset{C}{1+\sqrt{-5}})(3, \overset{D}{1-\sqrt{-5}})$

$(1+\sqrt{-5}) = (2, 1+\sqrt{-5})(3, 1+\sqrt{-5})$

$(1-\sqrt{-5}) = (2, 1-\sqrt{-5})(3, 1-\sqrt{-5})$

$(AB)(CD) = (AC)(BD)$

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

Every nonzero ideal is a product of prime ideals in a unique (up to order) way

Dedekind domain

Condition equivalent to:

(1) Noetherian,

(2) Every nonzero prime is maximal, and

(3) Integrally closed $R \subseteq K$

} all 3 must hold

$x^n + r_{n-1}x^{n-1} + \cdots + r_0 = 0$

Standard examples:

(1) Integers of algebraic number field

$\mathbb{Z}$ $\quad \mathbb{Z}[\sqrt{3}] = \mathbb{Z}[x]/(x^2-3)$ $\quad \mathbb{Q}(\sqrt{3})$

(2) Coordinate rings of affine algebraic curves

$k[x] \subseteq k[x,y]/(y^2-x^3+x)$

$k[x]$: affine line

$k[x,y]/(y^2-x^3+x)$: elliptic curve

$k[x,y]/(y^2-x^3+x)$

Noetherian $\iff$ Alg geo: not weird

Nonzero primes maximal $\iff$ $\dim \leq 1$

$0 \subsetneq p_0 \subsetneq p_1 \subsetneq p_2$

$0 \subsetneq p_1$

Integrally closed $\iff$ Normal $\Rightarrow$ Singularities have codim ≥ 2 $\Rightarrow$ Nonsingular

Dedekind domains $\approx$ nonsingular "curves"

$k[x,y]/(y^2-x^3+x)$

$y^2 = x(x-1)(x+1)$

non-unique factorization

$(y) = (y, x+1)(y, x)(y, x-1)$

$(x) = (y, x)^2$ $\quad (x-1) = (y, x-1)^2$ $\quad (x+1) = (y, x+1)^2$

Algebra		Geometry
Ideals	$\iff$	positive divisors $\sum_i n_i p_i$ (p_i: point on curve, $n_i \geq 0$)
Prime ideals $\neq 0$	$\iff$	points p_i
Element f of ring	$\iff$	function on curve
$f \mapsto (f)$	$\iff$	$f \mapsto$ zeros of f

unique factorization

Not quite Dedekind domains:

(1) Not Noetherian

Algebraic:

$\mathbb{Z}_p[p^{1/2}, p^{1/3}, p^{1/4}, \dots]$

↑ p-adic

Geometric:

$K[x] \subseteq K[x^{1/2}] \subseteq K[[x^{1/3}]]$

Puiseaux series $\simeq$ power series w/ nonintegral exponents

$I = (x, x^{1/2}, x^{1/3}, \dots)$

$I^2 = I$

Holomorphic functions

$f = \prod$ uncountably many factors

↑ might be infinite

$(1 - \frac{z}{a_1})\ (1 - \frac{z}{a_2})(\exp \frac{z}{a_2}) \dots$

(2) Not integrally closed

Algebraic:

$\mathbb{Z}[\sqrt{-3}]$

$(2, 1+\sqrt{-3})^2 = (2)(2, 1+\sqrt{-3})$

$\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$

Geometric:

Something with a cusp: $K[x,y]/(y^2 - x^3)$

$t = \frac{y}{x}$ $\quad K[t^2, t^3] \subseteq K[t]$

$(t^2, t^3)^2 = (t^2, t^3)\, t^2$

(3) Nonzero primes need not be maximal

Algebraic:

$\mathbb{Z}[x]$

$(8, 4x, x^2)$

Geometric:

$K[x,y]$

(x^2, x^2y, y^2)

Lasker-Noether thm: every ideal is intersection of primary ideals (vs product of prim ideals)

P.I.D. → U.F.D.s → Krull domains (finitely many codimension 1 degenerations)

P.I.D. → Dedekind domains → Krull domains (finitely many codimension 1 degenerations)