Istituzioni di Algebra

A.A. 2025-2026

SIMONE SACCANI

ALGEBRA COMMUTATIVA

Topologia di Zariski

Def A ring (commutative with 1)
$\operatorname{Spec} A = \{\mathfrak{p} \subseteq A \mid \mathfrak{p} \text{ is prime}\}$
Open sets: a basis is given by the principal open sets
$D(a) = \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \not\ni a\}$, $a \in A$

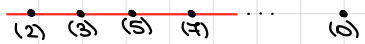
Rmk Closed sets: $\left(\bigcup_{a \in X} D(a)\right)^c = \bigcap_{a \in X} D(a)^c = \bigcap_{a \in X} \{\mathfrak{p} \in \operatorname{Spec} A \mid a \in \mathfrak{p}\} =$

$= \{\mathfrak{p} \mid \mathfrak{p} \ni a \ \forall a \in X\} = \{\mathfrak{p} \mid \mathfrak{p} \supseteq (a : a \in X)\} =: V(I)$
where $I = (a \mid a \in X)$

Ex $\{\mathfrak{p}\}$ is a closed subset $\iff$ $\mathfrak{p}$ is maximal
Pf ($\Longleftarrow$) $\{\mathfrak{p}\} = V(\mathfrak{p}) = \{\mathfrak{q} \in \operatorname{Spec} A \mid \mathfrak{q} \supseteq \mathfrak{p}\} = \{\mathfrak{p}\}$
($\Longrightarrow$) $\{\mathfrak{p}\} = V(I)$ $\mathfrak{p} \in V(I) \Rightarrow I \subseteq \mathfrak{p}$
If $\mathfrak{p} \subseteq \mathfrak{q}$ with $\mathfrak{q}$ prime, then $I \subseteq \mathfrak{q} \Rightarrow \mathfrak{q} \in V(I) = \{\mathfrak{p}\} \Rightarrow \mathfrak{p} = \mathfrak{q} \Rightarrow \mathfrak{p}$ maximal

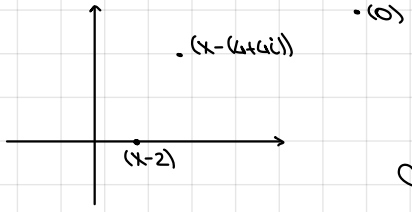
Def Let $\varphi : A \longrightarrow B$ be a ring homomorphism
$\varphi^* : \operatorname{Spec} B \longrightarrow \operatorname{Spec} A$
$\mathfrak{p} \longmapsto \varphi^{-1}(\mathfrak{p})$

Ex φ^* is continuous
Pf We check that $(\varphi^*)^{-1}(D(a))$ is open
$(\varphi^*)^{-1}(D(a)) = \{\mathfrak{p} \in \operatorname{Spec} B \mid \varphi^*(\mathfrak{p}) \in D(a)\} = \{\mathfrak{p} \mid \varphi^*(\mathfrak{p}) \not\ni a\} =$
$= \{\mathfrak{p} \mid \mathfrak{p} \not\ni \varphi(a)\} = D(\varphi(a))$ □

esempio
- $\operatorname{Spec} \mathbb{Q} = \{\cdot\}$
- $\operatorname{Spec} \mathbb{Z} =$ 

$V((0)) = \operatorname{Spec} \mathbb{Z}$
$V((n)) = \{\mathfrak{p} \ni \operatorname{Spec} \mathbb{Z} \mid \mathfrak{p} \ni n\} = \{p \mid n\}$
Closed subsets = finite unions of closed points (or $\operatorname{Spec} \mathbb{Z}$)

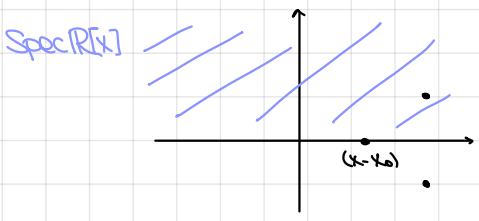
- $\operatorname{Spec} \mathbb{C}[x]$
(0), $(\varphi(x)) = (x - x_0)$ for $x_0 \in \mathbb{C}$



Closed sets: $\emptyset$, $\operatorname{Spec} \mathbb{C}[x]$, finite unions of closed pts

- $\operatorname{Spec} \mathbb{R}[x]$
(0), $(x - x_0)$, $(x^2 + ax + b)$ with $a^2 - 4b < 0$

$x^2 + ax + b$ $\quad \frac{-a \pm \sqrt{\Delta}}{2}$



- $f: \underset{\parallel}{\mathbb{C}[t]} \longrightarrow \frac{\mathbb{C}[x,y]}{(y^2-1)} = B$
  $t \longmapsto x$

  $f^\#: \operatorname{Spec} B \longrightarrow \operatorname{Spec} A$

  $\operatorname{Spec} \mathbb{C}[t]$ — $(t-x_0)$

  $\operatorname{Spec} B$ — $(y-1, x-x_0)$ ↑ $f^\#$ — $(y+1)$ — $(y-1, x-x_0)$

  $\{M \subseteq \mathbb{C}[x,y] \text{ prime} \mid M \supseteq (y^2-1)\} = \{M \mid M \in \{1-h \in M \text{ or } 1+h \in M\}\}$

  $\{M \mid 1-h \in M, M\} \longleftrightarrow \{M \text{ prime of } \frac{\mathbb{C}[x,y]}{(y-1)} \simeq \mathbb{C}[x]\}$

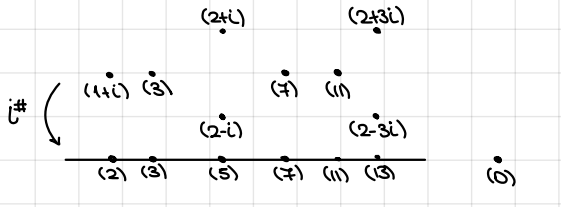
  $(y-1), (y-1, x-x_0) \longleftrightarrow (0), (x-x_0)$

- $\operatorname{Spec} \mathbb{Z}[i] \xrightarrow{i^\#} \operatorname{Spec} \mathbb{Z}$ $\qquad i: \mathbb{Z} \longrightarrow \mathbb{Z}[i]$

  (0), (3), (7), (11), (p) with $p \equiv 3 \ (4)$

  $5 = (2+i)(2-i)$ $\quad 2+i, 2-i$ are prime

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



$(2+i)\mathbb{Z}[i] \cap \mathbb{Z} = (5)$ $\qquad (2+i)(a+bi) = n$

$(2-i)(a-bi) = n$

$n \in (2+i) \cap (2-i) = (2+i)(2-i) = (5)$

Rmk: rings as rings of functions

$S^1 = \{(x,y) \in \mathbb{R}^2 \mid x^2+y^2 = 1\}$

$f(x,y) \in \mathbb{R}[x,y]$ is a function on the circle

$f_1(x,y) \equiv 1$ $\qquad f_2(x,y) = x^2+y^2$

Same function $\iff (f_1 - f_2)(x,y) = 0 \quad \forall (x,y) \in S^1$

$\iff f_1 - f_2 \in (x^2+y^2-1)$

$\mathbb{R}[x,y]/(x^2+y^2-1)$ is the ring of polynomial functions on the variety defined by $x^2+y^2-1=0$

Topological interpretation of known results

- $\{\text{ideals in } A/I\} \longleftrightarrow \{\text{ideals in } A \text{ containing } I\}$

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

  $\pi: A \longrightarrow A/I$, $\quad \pi^\#: \operatorname{Spec} A/I \longrightarrow \operatorname{Spec} A$ (image $\simeq V(I)$)

  $\operatorname{Im} \pi^\# = \{\pi^{-1}(M) \mid M \in \operatorname{Spec} A/I\} =$

  $= \{M \in \operatorname{Spec} A \mid M \supseteq I\} = V(I)$

  Let's check that the topologies agree

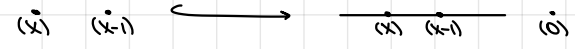
  $\overline{X} \subseteq \operatorname{Spec} A/I$ closed subset, $\overline{X} = V(\overline{J})$ for some $\overline{J} \lhd A/I \longleftrightarrow J \subseteq A, J \supseteq I$

  $V(J) \cap \operatorname{Im} \pi^\# = \{M \in \operatorname{Spec} A \mid M \supseteq J\} \cap V(J) = \{M \in \operatorname{Spec} A \mid M \supseteq J\} =$

  $= \{\pi^\#(M) \mid M \supseteq J\} = V(\overline{J})$

esempio $\pi : \mathbb{C}[x] \longrightarrow \mathbb{C}[x]/(x(x-1))$

$\pi^\# : \operatorname{Spec} \mathbb{C}[x]/(x(x-1)) \hookrightarrow \operatorname{Spec}\mathbb{C}[x]$



- Localization by $S=\{a^n\}$, $a \in A$

$i : A \longrightarrow S^{-1}A$

$a \longmapsto \frac{a}{1}$

$\{\mathfrak{p} \in \operatorname{Spec} S^{-1}A\} \longleftrightarrow \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \cap S = \emptyset\} = \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \not\ni a\} = D(a)$

$i^\# : \operatorname{Spec} S^{-1}A \longrightarrow \operatorname{Spec} A$ (image $D(a)$)

EX $i^\#$ identifies $\operatorname{Spec} S^{-1}A$ with $D(a)$ (as topological spaces)

esempio $A=\mathbb{Z}$, $S=\mathbb{Z}\setminus\{0\}$ $\quad S^{-1}A=\mathbb{Q}$ $\quad i : A \longrightarrow \mathbb{Q}$

$i^\# : \operatorname{Spec}\mathbb{Q} \longrightarrow \{0\} \in \operatorname{Spec} A$

but $\{0\}$ is not open in $\operatorname{Spec}\mathbb{Z}$

- Nilradical : $\sqrt{(0)} = \{a \in A \mid \exists n \in \mathbb{N}_{\geq 1} \text{ s.t. } a^n = 0\}$

FACT $\sqrt{(0)} = \bigcap_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p}$

$\pi : A \longrightarrow A/\sqrt{(0)}$

$\pi^\# : \operatorname{Spec} A/\sqrt{(0)} \xrightarrow{\sim} \operatorname{Spec} A$

Slogan : A and A^{red} have the same spectrum (Δ for us)

- Chinese Remainder Theorem (= disconnected topological spaces)

$A = B \times C \longrightarrow \operatorname{Spec} A = \operatorname{Spec} B \sqcup \operatorname{Spec} C$

Reason : $I \lhd A \Rightarrow I = I_1 \times I_2$ with $I_1 \lhd B$, $I_2 \lhd C$

$A/I \simeq B/I_1 \times C/I_2$ can only be an integral domain

if $B/I_1 = \{1\}$ or $C/I_2 = \{1\}$

$\operatorname{Spec} A = \{B \times I_2 \mid I_2 \in \operatorname{Spec} C\} \sqcup \{I_1 \times C \mid I_1 \in \operatorname{Spec} C\}$

Conversely, suppose $\operatorname{Spec} A$ is disconnected

$\operatorname{Spec} A = V(I) \sqcup V(J)$ for some ideals I, J

1) $V(I) \cap V(J) = \emptyset$: no prime $\mathfrak{p}$ contains both I and J

$\Rightarrow I + J = (1)$ because $I+J$ is not contained in any max ideal

2) $\forall \mathfrak{p} \in \operatorname{Spec} A$ is either in $V(I)$ or in $V(J)$, so

$\forall \mathfrak{p} \quad \mathfrak{p} \supseteq I$ or $\mathfrak{p} \supseteq J \Rightarrow \mathfrak{p} \supseteq I \cap J$

so $(0) = \sqrt{(0)} = \bigcap_{\mathfrak{p}} \mathfrak{p} \supseteq I \cap J$

(↑ if A is reduced)

So I, J satisfy the assumptions of the CRT, and

$A \simeq A/I \times A/J$

⚠ A different point of view

$\operatorname{Spec} A =$ 

I want to find a function f on this top. space that is 0 on one conn. comp. and 1 on the other.

$\begin{cases} f \equiv 0 & (I) \\ f \equiv 1 & (J) \end{cases}$

A anello. $\operatorname{Spec}A$ disconnesso $= V(I) \amalg V(J)$

$\Rightarrow A/\sqrt{(0)} = A^{red} \simeq B \times C$, $e \mapsto (1,0)$, $1-e \mapsto (0,1)$

$\Leftrightarrow \exists \bar{e}, 1-\bar{e} \in A^{red}$ t.c. $\bar{e}(1-\bar{e}) = \bar{0}$

$\Leftrightarrow \exists e \in A$ t.c. $(e(1-e))^N = 0$

Gli ideali $I_1 = e^N$, $I_2 = (1-e)^N$ soddisfano le ipotesi del TCR:

- $I_1 + I_2 = (1)$

  Sia P primo $\supseteq I_1 + I_2 \Rightarrow P \ni e^N, (1-e)^N \Rightarrow P \ni e, 1-e \Rightarrow P \ni 1$ ↯
- $I_1 \cap I_2 = I_1 I_2 = (e^N)((1-e)^N) = 0$

$\Rightarrow A \simeq A/I_1 \times A/I_2$ (con i fattori non banali)

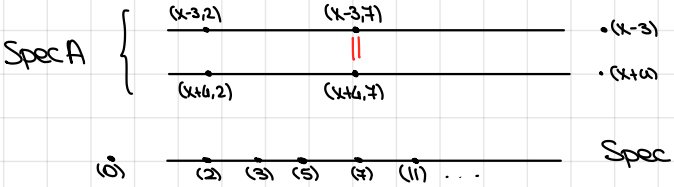
<u>Conclusione</u> A è un prodotto $\Leftrightarrow \operatorname{Spec}A$ è disconnesso

Ex $A = \mathbb{Z}[x]/((x-3)(x+4))$, $S = \{7^k\}_{k \in \mathbb{N}}$

Show that A is not a product but $S^{-1}A$ is.

<u>Sol</u> $i: \mathbb{Z} \hookrightarrow A$

$i^*: \operatorname{Spec}A \longrightarrow \operatorname{Spec}\mathbb{Z}$





$\operatorname{Spec}A = \{\text{primes in } \mathbb{Z}[x] \text{ containing } (x-3)(x+4)\} =$

$= \{\text{primes cont. } (x-3)\} \cup \{\text{primi} \supseteq (x+4)\} =$

$\doteq \operatorname{Spec} \mathbb{Z}[x]/(x-3) \cup \operatorname{Spec} \mathbb{Z}[x]/(x+4) \doteq \operatorname{Spec}\mathbb{Z} \cup \operatorname{Spec}\mathbb{Z} =$

$= \{(x-3), (x-3,p) \mid p \text{ prime of } \mathbb{Z}\} \cup \{(x+4), (x+4,p) \mid p \text{ prime of } \mathbb{Z}\}$

Algebraic version:

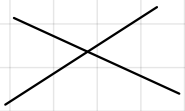
$S^{-1}A \simeq \dfrac{S^{-1}\mathbb{Z}[x]}{((x-3)(x+4))} \simeq \dfrac{S^{-1}\mathbb{Z}[x]}{(x-3)} \times \dfrac{S^{-1}\mathbb{Z}[x]}{(x+4)}$

$(x-3) + (x+4) \overset{?}{=} (1)$ ∥

$(x-3, x+4) = (x-3, 7)$ ≀

$S^{-1}\mathbb{Z} \times S^{-1}\mathbb{Z}$

def X spazio topologico si dice irriducibile se per ogni scrittura $X = C_1 \cup C_2$ come unione di due chiusi si ha $C_1 = X$ o $C_2 = X$.



esempio $\operatorname{Spec} \frac{\mathbb{C}[x,y]}{(xy)} \rightsquigarrow$



$= \{\mathfrak{p} \in \operatorname{Spec} \mathbb{C}[x,y] \mid \mathfrak{p} \supseteq (xy)\}$

$= \{\mathfrak{p} \mid \mathfrak{p} \supseteq (x)\} \cup \{\mathfrak{p} \mid \mathfrak{p} \supseteq (y)\}$

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

$V(x) \subseteq \operatorname{Spec} \mathbb{C}[x,y]/(xy) = V(x) \cup V(y)$

Lemma X top. space, $Y \subseteq X$ irreducible $\Rightarrow \overline{Y}$ irreducible.

DIMOSTRAZIONE

$\overline{Y} = C_1 \cup C_2$ with C_1, C_2 closed in X (or equiv. in $\overline{Y}$).

$\Rightarrow Y = \overline{Y} \cap Y = (\underbrace{C_1 \cap Y}_{\text{closed in } Y}) \cup (\underbrace{C_2 \cap Y}_{\text{closed in } Y}) \Rightarrow C_1 \cap Y = Y$ or $C_2 \cap Y = Y$

wlog $C_1 \cap Y = Y \Rightarrow Y \subseteq C_1 \Rightarrow \overline{Y} \subseteq C_1 \Rightarrow \overline{Y} = C_1$. □

corollario $x \in X \Rightarrow \overline{\{x\}}$ is irreducible

In the example, $V(x) \simeq \operatorname{Spec} \frac{\mathbb{C}[x,y]}{(x)} \simeq \operatorname{Spec} \mathbb{C}[y] = \overline{\{0\}}$

let's check: $\overline{\{0\}} = \bigcap_{\substack{V(I) \ni 0 \\ I \subseteq (0)}} V(I) = V((0)) = \operatorname{Spec} \mathbb{C}[y]$

def An irred. component is an irred. subset, maximal by inclusion.

Teorema let R be a ring

$\{\text{closed subsets of } \operatorname{Spec} R\} \longleftrightarrow \{\text{radical ideals } I \text{ of } R : I = \sqrt{I}\}$

$\alpha: C \longmapsto \bigcap_{\mathfrak{p} \in C} \mathfrak{p}$

$V(I) \longleftarrow I : \beta$

(i) α, β are inclusion-reversing bijections that are mutually inverse

(ii) C irred $\Leftrightarrow \alpha(C)$ is prime

(iii) irred components of $\operatorname{Spec} R \longleftrightarrow$ minimal primes of R

DIMOSTRAZIONE

(i) $C_1 \subseteq C_2 \Rightarrow \alpha(C_1) \supseteq \alpha(C_2)$

$\bigcap_{\mathfrak{p} \in C_1} \mathfrak{p} \supseteq \bigcap_{\mathfrak{p} \in C_2} \mathfrak{p}$

$I_1 \subseteq I_2 \Rightarrow V(I_1) = \{\mathfrak{p} : I_1 \subseteq \mathfrak{p}\}$

$V(I_2) = \{\mathfrak{p} : I_2 \subseteq \mathfrak{p}\}$

(a) $\alpha(\beta(I)) = \alpha(V(I)) = \bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p} = \bigcap_{I \subseteq \mathfrak{p}} \mathfrak{p} = \sqrt{I} = I$

(b) $V(I) = V(\sqrt{I})$ · indeed $\mathfrak{p} \supseteq I \Leftrightarrow \mathfrak{p} \supseteq \sqrt{I}$

So every closed subset is of the form $\beta(\sqrt{I})$, hence β is surjective

(a) $\Rightarrow \beta$ is injective

$\Rightarrow \beta$ is a bijection and (a) $\Rightarrow \alpha$ is the inverse

(ii) Let's first prove that $\forall$ prime $\mathfrak{p}$ we have

$\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$

($\subseteq$) It suffices $\mathfrak{p} \in V(\mathfrak{p})$, true by def.

($\supseteq$) $\overline{\{\mathfrak{p}\}} = \bigcap_{V(I) \supseteq \mathfrak{p}} V(I) = \bigcap_{I \subseteq \mathfrak{p}} V(I) \supseteq V(\mathfrak{p}) \iff V(\mathfrak{p}) \subseteq V(I) \ \forall I \subseteq \mathfrak{p}$

which is true since V reverses inclusions.

($\Leftarrow$) If $\mathfrak{p}$ is prime, $V(\mathfrak{p}) = \overline{\{\mathfrak{p}\}}$ is irred. by the Cor.

($\Rightarrow$) C irred, $I = I(C)$. Let $a, b \in R$ s.t. $ab \in I$

Claim: $C = V(\sqrt{(I,a)}) \cup V(\sqrt{(I,b)})$

$V(I) = C$

To prove ($\subseteq$), take $\mathfrak{p} \in C \iff \mathfrak{p} \supseteq I$. Then

$ab \in I \subseteq \mathfrak{p} \implies a \in \mathfrak{p}$ or $b \in \mathfrak{p}$

$\hookrightarrow (I,a) \subseteq \mathfrak{p} \implies \sqrt{(I,a)} \subseteq \sqrt{\mathfrak{p}} = \mathfrak{p}$

$\implies \mathfrak{p} \in V(\sqrt{(I,a)})$

C irred $\implies$ wlog $V(\sqrt{(I,a)}) = C = V(I)$

$\overset{(i)}{\implies} I = \sqrt{(I,a)} \ni a$, so I is prime.

(iii) Irred. subsets $\longleftrightarrow$ primes (ii)

Maximal under inclusion $\longleftrightarrow$ minimal under inclusion (i)

proposizione R Noetherian ring. $\operatorname{Spec} R$ has finitely many connected components and finitely many irreducible components.

DIMOSTRAZIONE

By Noetherian induction

$X = \{C \subseteq \operatorname{Spec} R$ closed subspaces having infinitely many irred. comp.$\}$

If $X = \emptyset$, we're done.

Otherwise, X has a minimal element.

$C_1 \supsetneq C_2 \supsetneq C_3 \supsetneq \dots$ ($C_i \in X$)

$V(I_1) \supsetneq V(I_2) \supsetneq V(I_3) \supsetneq \dots$

$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots$ cannot go on forever

Let C be minimal.

- C is irreducible: contradiction as $C \in X$
- C is reducible: $C = C_1 \cup C_2$, C_1, C_2 closed $\subsetneq C$

$\implies C_1, C_2 \notin X \implies$ they have finitely many irred. comp.

$\implies C$ has finitely many irred. comp. $\square$

corollario If R is Noetherian, then R has finitely many minimal primes.

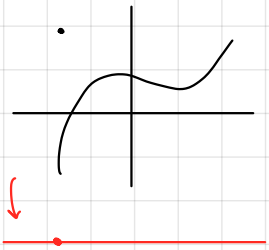
DIMOSTRAZIONE

Minimal primes correspond to irred. comp. $\square$

Dimensione di Krull

Def. Let R be a ring.
A chain of prime ideals in R is a sequence
$P_0 \subsetneq P_1 \subsetneq P_2 \subsetneq \dots \subsetneq P_n$, where each P_i is a prime ideal of R
The length of such chain is n
The Krull dimension of R is the sup of the lengths of all the chains of prime ideals in R.

esempio
- $R = \mathbb{C}[x_1, x_2, x_3, \dots]$ has $\dim R = +\infty$
  $(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \dots$
- $\dim R$ can be infinite if R is Noetherian
- $\dim \mathbb{Q} = 0$, $\dim(\text{field}) = 0$
- $\dim \frac{\mathbb{C}[x]}{(x^n)} = 0$ (only prime ideal is (x))
- $\dim \mathbb{Z} = 1$ $\quad (0) \subsetneq (p)$
- $\dim R = 1$ where R is a PID not a field
- $\dim \mathbb{Z}[x] = 2$
  Prime ideals: (0), (p), $(f(x))$ (f primitive + irred in $\mathbb{Q}[x]$), $(p, g(x))$ (g irred mod p)
- $\dim \mathbb{C}[x,y] = 2$
  Let P be a prime of $\mathbb{C}[x,y]$
  (0), $(x-x_0, y-y_0)$, $(f(x,y))$



$$P \cap \mathbb{C}[x] = \begin{cases} (0) & (1) \\ (x-x_0) & (2) \end{cases}$$

(2): $P \supseteq (x-x_0) \longleftrightarrow$ primes of $\frac{\mathbb{C}[x,y]}{(x-x_0)} \cong \mathbb{C}[y] \supseteq (0), (y-y_0)$
$\Longrightarrow (x-x_0)$, $(x-x_0, y-y_0)$

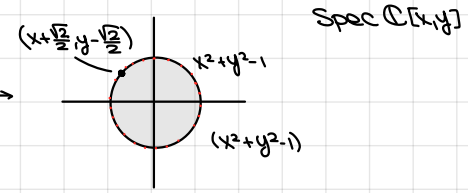
(1): $P \cap \mathbb{C}[x] = (0)$ $\quad S := \mathbb{C}[x] \setminus \{0\}$
$\updownarrow$
prime ideal in $S^{-1}\mathbb{C}[x,y] = \mathbb{C}(x)[y] \supseteq (0), \left(\frac{f(x,y)}{g(x)}\right)$
$\|$

$(0), (f(x,y))$ in $\mathbb{C}[x,y] \longleftrightarrow (0), (f(x,y))$

Prime ideals are (0), $(f(x,y))$, $(x-x_0, y-y_0)$.
In particular they're either maximal or principal.

$(0) \subsetneq (x) \subsetneq (x,y)$
$(0) \subsetneq (x^2+y^2-1) \subsetneq (x-1, y)$ $\quad (*)$
$(0) \subsetneq (f_1(x,y)) \subsetneq (f_2(x,y)) \subsetneq (x-x_0, y-y_0)$
impossible: f_1, f_2 are irred.

$(*) \longleftrightarrow V$



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

Why primes? $\quad \not\supset \not\supset / \supset \cdot$

we don't want chains like these!

Anelli Artiniani

A ring R is Artinian if it satisfies the descending chain condition (DCC) on ideals: every chain $I_1 \supseteq I_2 \supseteq I_3 \supseteq \dots$ is eventually stationary.
Equivalently, there are no infinite chains $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots$

Aim: Artinian $\iff$ Noetherian of dimension 0.
Motivation: R Noeth of dim 0.

$\operatorname{Spec} R =$ 

spectrum of a local Artinian ring

Teorema di struttura per anelli artiniani Every Artinian ring is a finite direct product of local Artinian rings.

Lemma R Artinian domain $\Rightarrow$ R is a field.

DIMOSTRAZIONE
$t \in R \setminus \{0\}$. Consider $(t) \supseteq (t^2) \supseteq (t^3) \supseteq \dots$
By the Artin property, $\exists n$ s.t. $(t^n) = (t^{n+1})$.
$\Rightarrow \exists u \in R^\times$ s.t. $t^{n+1} = ut^n \Rightarrow t^n(t-u) = 0$
$\Rightarrow t = u \in R^\times$ □

corollario Let R be Artinian. Every prime ideal is maximal.

DIMOSTRAZIONE
$P \subset R$ prime. R/P = Artinian domain = field
$\Rightarrow P$ maximal. □

Lemma di Nakayama Let R be a local ring with maximal ideal $\mathfrak{m}$ and let N be a finitely-generated R-module.
If $\mathfrak{m} \cdot N = N$, then $N = (0)$.

Preliminari:

- un A-modulo è Noetheriano/Artiniano se soddisfa ACC/DCC per i sottomoduli
- A è Noetheriano/Artiniano se lo è come A-modulo
  (i sottomoduli sono gli ideali)
- $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ succ. esatta corta
  M Noeth/Artin $\iff$ M', M'' Noeth/Artin
- Per un modulo, Artiniano $\not\Longrightarrow$ Noetheriano
  esempio $M = \mathbb{Q}/\mathbb{Z}[p^\infty] = \{x \in \mathbb{Q}/\mathbb{Z} : \exists n \geq 1 \text{ t.c. } p^n x = 0\}$
- Se $A = K$ è un campo, un A-mod M (cioè un K-sp.vett.)
  è Noetheriano $\iff$ $\dim_K M < +\infty$ $\iff$ è Artiniano
- Sia M un A-modulo e $\mathrm{Ann}_A M := \{a \in A \mid am = 0 \ \forall m \in M\}$
  Allora M è un $A/\mathrm{Ann}_A M$ - modulo: $\overline{a} \cdot m = am$ con $a \in A$ un qualsiasi sollevamento di $\overline{a}$

Oss Un A-modulo è un gruppo abeliano M + un omomorfismo di anelli $\Phi : A \longrightarrow \mathrm{End}_{\mathbb{Z}}(M)$
Allora $\mathrm{Ann}_A M = \ker \Phi$ $\rightsquigarrow$ $\overline{\Phi} : A/\ker\Phi \longrightarrow \mathrm{End}_{\mathbb{Z}} M$

- Conseguenza di Nakayama: (A, m) anello locale con ideale massimale m, N un A-mod fin.gen, e $n_1, \dots, n_r \in A$ t.c. $\overline{n}_1, \dots, \overline{n}_r \in N/mN$ sono generatori
  $\Longrightarrow$ $n_1, \dots, n_r$ sono generatori di N.

DIMOSTRAZIONE
$S = \langle n_1, \dots, n_r \rangle$ $\quad S/mN \cap S = N/mN \Longrightarrow S + mN = N$
$\Longrightarrow N/S = S + mN/S = m(N/S) \overset{\text{Nak}}{\Longrightarrow} N/S = \{0\} \Longrightarrow N = S$.

Teorema A anello Artiniano $\Longrightarrow$ A Noetheriano.

DIMOSTRAZIONE
$\mathcal{C} = \{I \lhd A \mid I \text{ non fin.gen.}\}$. La tesi è che $\mathcal{C} = \emptyset$.
Supponiamo per assurdo $\mathcal{C} \neq \emptyset$: allora ha un el. minimale $I \neq (0)$.

Oss Sia $r \in A$. C'è una successione esatta
$0 \longrightarrow \{i \in I \mid ri = 0\} = I[r] \longrightarrow I \xrightarrow{\cdot r} rI \longrightarrow 0$
Almeno uno fra $I[r]$ e I non è fin.gen
Siccome $I[r], rI \subseteq I$ e se il contenimento è stretto sono fin.gen., allora o $I[r] = I$ o $rI = I$

Conseguenza: $P = \mathrm{Ann}_A I$ è primo: se $xy \in P$, voglio mostrare $x \in P$ o $y \in P$.
Se così non fosse, $xy \cdot I = x(yI) = xI = I$, assurdo.
I è un A-modulo $\Longrightarrow$ I è un A/P - modulo
A artiniano: P primo $\Longrightarrow P$ massimale
$\Longrightarrow I$ è uno sp.vett. su A/P, artiniano
$\Longrightarrow I$ è Noeth. come sp.vett.
$\Longrightarrow I$ è fin.gen. come A/P-mod, quindi come A-mod. ↯ □

proposizione A Artiniano $\Longrightarrow$ A Noetheriano di dim. 0.

proposizione $(A, \mathfrak{m})$ locale Noetheriano di dim 0.
Allora A è Artiniano.

DIMOSTRAZIONE

Dimostriamo che $\mathfrak{m}$ è nilpotente.

Modo 1: considero $\mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \mathfrak{m}^3 \supseteq \dots \supseteq \mathfrak{m}^n$ si stabilizza
$\Longrightarrow \exists n$ t.c. $\mathfrak{m}^n = \mathfrak{m}^{n+1}$. $M := \mathfrak{m}^n$ è fin.gen. e $\mathfrak{m}M = M$
$\Longrightarrow M = (0)$ per Nakayama

Modo che funziona: $\sqrt{(0)} = \bigcap_{\mathfrak{p}} \mathfrak{p} = \mathfrak{m} \Longrightarrow \exists n$ t.c. $\mathfrak{m}^n = (0)$

Per induzione su n: $n=1$, $\mathfrak{m} = (0)$, A è un campo e quindi Artiniano.

- $0 \longrightarrow \underbrace{\mathfrak{m}^n/\mathfrak{m}^{n+1}}_{A\text{-mod}} \longrightarrow \underbrace{A/\mathfrak{m}^{n+1}}_{A} \longrightarrow \underbrace{A/\mathfrak{m}^n}_{A\text{-modulo ma anche } A/\mathfrak{m}^n\text{-mod}} \longrightarrow 0$

  $\Rightarrow A/\mathfrak{m}$-mod
  $\Rightarrow$ sp.vett. di dim. finita perché $\mathfrak{m}^n$ è fin.gen.
  $\Rightarrow$ artiniano come A-mod.

  Per hp. induttivo $A/\mathfrak{m}^n$ è Artiniano (come anello, quindi come $A/\mathfrak{m}^n$-mod, quindi come A-mod)

Per esattezza, A è Artiniano. □

teorema (1) A Noeth, $\dim A = 0 \Longrightarrow A \simeq \prod_{i=1}^{r} A_i$, A_i locale Noeth di dim 0
(2) A Noeth, $\dim A = 0 \Longrightarrow A$ Artiniano

DIMOSTRAZIONE

(1) $\Rightarrow$ (2) facilmente perché ogni A_i è Artiniano per la Prop. precedente

(1) A Noeth $\Longrightarrow A$ ha un n° finito $\mathfrak{m}_1, \dots, \mathfrak{m}_r$ di primi minimali, che sono anche massimali (e anche tutti gli id. primi poiché $\dim A = 0$).
$N := \mathfrak{m}_1 \cdot \dots \cdot \mathfrak{m}_r = \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r = \sqrt{(0)} \Longrightarrow \exists n \geq 1$ t.c. $N^n = (0)$
$\mathfrak{m}_i^n + \mathfrak{m}_j^n = (1)$ perché $\mathfrak{m}_i + \mathfrak{m}_j = (1)$
$A \simeq A/N^n = A/\mathfrak{m}_1^n \cdot \dots \cdot \mathfrak{m}_r^n \simeq \prod_{i=1}^{r} A/\mathfrak{m}_i^n$
Vediamo che $A/\mathfrak{m}_i^n$ è Noeth, locale, 0-dim. □

Domini di valutazione discreta (DVR)

Def. Un DVR è un PID locale che non è un campo.

Esempio $\mathbb{Z}_{(p)}$, $\mathbb{Z}_p$ = anello degli interi p-adici
$\mathbb{C}[[t]] = \{\sum_{n\geq 0} a_n t^n \mid a_n \in \mathbb{C}\}$, locale con ideale (t)

Proposizione Sia $(A, \mathfrak{m})$ dominio locale. Le seguenti sono equivalenti:
(1) A è un DVR
(2) A è Noeth di dim 1, $\mathfrak{m}/\mathfrak{m}^2$ è un $A/\mathfrak{m}$-sp. vett. di dim 1
(3) A è Noeth, $\mathfrak{m}$ è principale e $\mathfrak{m} \neq (0)$.

DIMOSTRAZIONE

(1) $\Rightarrow$ (2) Per def A è PID $\Rightarrow A$ Noeth.
dim ≤ 1 perché è PID e dim $\neq 0$ perché A non è campo.
$\dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = 1$: ha dim ≤ 1 perché $\mathfrak{m}$ è principale (la classe mod $\mathfrak{m}$ genera $\mathfrak{m}/\mathfrak{m}^2$)
e dim $\neq 0$: se $\mathfrak{m}/\mathfrak{m}^2 = (0) \Longrightarrow \mathfrak{m} = \mathfrak{m}^2$
$\overset{\text{Nak}}{\Longrightarrow} \mathfrak{m} = (0)$ ↯

(2) $\Rightarrow$ (3) L'unica parte non banale è che $\mathfrak{m}$ è principale:
se $\mathfrak{m}/\mathfrak{m}^2 = \langle \bar{t} \rangle \overset{\text{Nak}}{\Longrightarrow} \mathfrak{m} = (t)$

Oss $\dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 \underset{(\geq)}{=} \dim A$: regolarità

(3) $\Rightarrow$ (1) Scriviamo $\mathfrak{m} = (t)$. Dimostriamo che ogni elemento di $A\setminus\{0\}$ si scrive in modo unico come $a = ut^n$ con $n \in \mathbb{N}$, $u \in A^\times$.

$a \in A$ ⟨ $a \in \mathfrak{m}$: $a = ta_1$ ⟨ $a_1 \in A^\times$. $u = a_1, n = 1$; $a = t \cdot ta_2$
$a \notin \mathfrak{m} \Longrightarrow a \in A^\times$ $(u = a, n = 0)$

Vediamo che questo procedimento si ferma per Noetherianità:
Considero la catena di ideali $(a) \subseteq (a_1) \subseteq (a_2) \subseteq \dots$
$\exists n$ t.c. $(a_n) = (a_{n+1}) \iff \exists u' \in A^\times$ t.c. $u' a_n = a_{n+1}$
$u' t a_{n+1}$
o $a_{n+1} = 0 \Rightarrow a = 0$, oppure $u't = 1 \Rightarrow t = (u')^{-1}$ è unità, assurdo.
Dimostriamo che A è PID.
Sia I un ideale: $I = \{u_i t^{n_i}\}_{i \in J}$, $u_i \in A^\times$, $n_i \in \mathbb{N}$
Sia $n := \min\{n_i\}$. Allora $t^n \in I$ e viceversa
ogni $u_i t^{n_i} = (u_i t^{n_i - n}) t^n \in (t^n) \Longrightarrow I = (t^n)$.
Inoltre, se $u_1 t^{n_1} = u_2 t^{n_2} \Longrightarrow \underset{\in \mathfrak{m}}{t^{n_2 - n_1}} = u_1 u_2^{-1} \in A^\times \Longrightarrow n_2 = n_1, u_1 = u_2$ □

Oss Ogni ideale è della forma $(t^n) = (t)^n = \mathfrak{m}^n$

Oss Sia A un DVR e $K = \mathrm{Frac}(A) = A[\frac{1}{t}]$
$a \in A$ si scrive $a = ut^n \longrightarrow \frac{u_1 t^{n_1}}{u_2 t^{n_2}} \in A[1/t]$
Inoltre ogni $a \in K$ si scrive in modo unico come $u \cdot t^n$, $n \in \mathbb{Z}$.
Se inoltre $\mathfrak{m} = (t')$, $t' = a_0 t$ e $a = ut^n = (u \cdot u_0^n)(t')^n$, con lo stesso n.

def $v: K^\times \longrightarrow \mathbb{Z}$ la valutazione data da A
$a \longmapsto n$ t.c. $a = ut^n$

def Sia K un campo. Una valutazione discreta su K è una funzione $v: K \longrightarrow \mathbb{Z} \cup \{\infty\}$ surgettiva e t.c.
(i) $v(xy) = v(x) + v(y)$ ($v: K^\times \longrightarrow \mathbb{Z}$ omo di gruppi)
(ii) $v(x+y) \geq \min\{v(x), v(y)\}$
(iii) $v(x) = \infty \iff x = 0$.

<u>Oss</u> la valutazione di un DVR soddisfa queste proprietà:
(i) $v(u_1 t^{n_1} u_2 t^{n_2}) = n_1 + n_2$
(ii) $v(u_1 t^{n_1} + u_2 t^{n_2}) = v(u_2 t^{n_2}(1 + u_2^{-1} u_1 t^{n_1 - n_2})) =$
$= \begin{cases} n_2 & \text{se } n_1 > n_2 \\ \geq n_2 & \text{se } n_1 = n_2 \end{cases}$ con $n_2 \leq n_1$

<u>Oss</u> $A = \mathbb{Z}_{(p)}$ $\mathrm{Frac}(A) = \mathbb{Q}$ $\frac{\alpha}{\beta} = p^n \frac{\alpha}{\beta}$ con $n \in \mathbb{Z}$, $\alpha, \beta \in \mathbb{Z}$, $p \nmid \alpha$, $p \nmid \beta$

def Sia K un campo, v una valutazione discreta.
L'anello di valutazione è $\mathcal{O}_v := \{x \in K \mid v(x) \geq 0\}$

$\mathcal{O}_v$ è un anello locale con ideale massimale $\mathfrak{m}_v := \{x \in K \mid v(x) \geq 1\}$
$\mathcal{O}_v \setminus \mathfrak{m}_v \overset{?}{=} \mathcal{O}_v^\times$
$\forall a$. $v(a) = 0 \implies v(\frac{1}{a}) + v(a) = v(1) = 0 \implies v(\frac{1}{a}) = -v(a) = 0$
$\implies 1/a \in \mathcal{O}_v$

proposizione A è un DVR $\iff \exists K$ campo e una valutazione discreta su K t.c. $A = \mathcal{O}_v$.

DIMOSTRAZIONE
($\Longrightarrow$) ok
($\Longleftarrow$) Devo mostrare che $\mathcal{O}_v$ è DVR: è dominio, locale.
Non è un campo: $\exists a \in K$ t.c. $v(a) = 1$
quindi $a \in \mathcal{O}_v$ ma $\frac{1}{a} \notin \mathcal{O}_v$ poiché $v(\frac{1}{a}) = -1$.
Ogni elemento di K si scrive $x = u a^n$ con $n = v(x)$, $v(u) = 0$
Sia I ideale di $\mathcal{O}_v$, $I = \{u_i a^{n_i}\}_{i \in J}$, $u_i \in \mathcal{O}_v^\times$, $n_i \in \mathbb{N}$
$\implies I = (a^{\min\{n_i\}})$ □

esempio $A = \frac{\mathbb{C}[x,y]}{(y^2-x^3)}$ $\quad m = (x,y)$ $\quad B = A_m$

B è un DVR?

B è Noeth.

A è un dominio? $\iff (y^2-x^3)$ è primo in $\mathbb{C}[x,y]$

$\iff y^2-x^3$ irriducibile ($\mathbb{C}[x,y]$ è UFD).

$y^2-x^3 = \underset{\deg 2\\ \deg 1}{p_1(x,y)}\ \underset{\deg 0\\ \deg 1}{p_2(x,y)}$ li considero come polinomi in y, WLOG monici

$y^2-x^3 = (y^2+a_1(x)y+a_2(x))\cdot b(x) \implies b(x)=1$

$y^2-x^3 = (y-a_1(x))(y-a_2(x)) = y^2-(a_1(x)+a_2(x))y + a_1(x)a_2(x)$

$\implies \begin{cases} 0 = a_1(x)+a_2(x) \\ -x^3 = a_1(x)a_2(x) \end{cases} \implies \begin{cases} a_2(x) = -a_1(x) \\ x^3 = a_1(x)^2 \end{cases}$ assurdo

$\dim A = 1$: le catene di primi di A $\longleftrightarrow$ catena di primi in $\mathbb{C}[x,y]$

$(y^2-x^3) \subsetneq P \implies P$ massimale

Per capire se B è un DVR, devo capire se m_B/m_B^2 come B/m_B sp.vett. ha dim 1

$m_B = mB = (x,y)B$

$m_B/m_B^2 = \frac{(x,y)}{(x^2,xy,y^2)}$

Ora $m_B/m_B^2 \simeq m_A/m_A^2 = \frac{(x,y)}{(x^2,xy,y^2)}$ S.V. su $A/m \simeq \mathbb{C}$

$\overline{p(x,y)} \in A \qquad \overline{q(x,y)} \in m/m^2$

$\overline{p(x,y)}\ \overline{q(x,y)} = p(0,0)\,\overline{q(x,y)}$

$\dim_{\mathbb{C}} m/m^2 \leq 2$

x e y sono lin. indip?

$\lambda\overline{x}+\mu\overline{y} = 0$ in $m/m^2 \iff \lambda x+\mu y \in (x^2,xy,y^2)$ in A

$\iff \lambda x+\mu y \in (x^2,xy,y^2,y^2-x^3)$ in $\mathbb{C}[x,y] \iff \lambda=\mu=0$

Quindi $\dim_{A/m_A} m_A/m_A^2 = \dim_{B/m_B} m_B/m_B^2 = 2 \implies B$ non è DVR.

Es A anello, m massimale, $n \geq 1$

$A/m^n \simeq A_m/(mA_m)^n = S^{-1}(A/m^n)$

con $S = A\setminus m$

Considero

$\varphi: A \longrightarrow A_m \longrightarrow A_m/(mA_m)^n$

$a \longmapsto \frac{a}{1} \longmapsto \overline{\frac{a}{1}}$

Basta mostrare che φ è surgettiva e $\ker\varphi = m^n$.

- surgettiva: prendo $\overline{\frac{a}{s}}$ con $s \notin m$

  Siccome $s\notin m$, $(s,m) = (1) \implies (s)+m = (1) \implies (s)+m^n = 1$

  $\implies \exists\, b s \in (s)\ \exists\, m_n \in m^n$ t.c. $bs+m_n = 1$

  In particolare riducendo mod m^n: $\overline{b}\cdot\overline{s} = \overline{1} \implies b \notin m$

  $\overline{\frac{a}{s}} = \overline{\frac{ab}{bs}} = \overline{\frac{ab}{1}} \in \operatorname{Im}\varphi$

- $\ker\varphi = \{a\in A \mid \frac{a}{1} \in (mA_m)^n\} = \{a\in A \mid a/1 \in m^n A_m\} = \{a\in A \mid \frac{a}{1} = \frac{m}{s},\ m\in m^n,\ s\notin m\} =$

  $= \{a\in A \mid u(as-m_n) = 0 \text{ con } m_n\in m^n,\ s\notin m,\ u\notin m\}$

  $\Downarrow$ mod m^n

  $\overline{u}(\overline{a}\cdot\overline{s}) = 0 \mod m^n$

  $\overline{u},\overline{s}$ invertibili mod $m^n \implies \overline{a} = \overline{0} \mod m^n \implies a \in m^n$

□

Es DVR $\mathbb{C}[X,Y]$ $A=\frac{\mathbb{C}[X,Y]}{(Y^2-X^3-X^2)}$ x,y classi di X,Y

$m=(x,y)$ ideale max di A

$B=A_m$ è Noetheriano, dominio, locale, dim 1

m_B/m_B^2 è s.v. su B/m_B : di che dim è?

m/m^2 " A/m

$\frac{(x,y)}{(x^2,xy,y^2)}$

$$A\times m_A \longrightarrow m_A \longrightarrow m_A/m_A^2$$
$$A\times m_A/m_A^2 \nearrow$$

$\overline{p(x,y)}\cdot\overline{q(x,y)}=p(0,0)\overline{q(x,y)}$

$\overline{p_2y+p_1x+p_0}$

Voglio dim che $\dim_{A/m} m/m^2=2$, cioè x,y sono lin. indip.

$\lambda x+\mu y=0$ in m_A/m_A^2

$\iff \lambda x+\mu y\in m_A^2=(x^2,xy,y^2)$ in A

$\iff \lambda x+\mu y=x^2p_1+xyp_2+y^2p_3$ in A

$\iff \lambda X+\mu Y=X^2p_1+XYp_2+Y^2p_3+(Y^2-X^3-X^2)p_4$ in $\mathbb{C}[X,Y]$

$\iff \lambda=\mu=0$

Es $\mathbb{C}[X,Y]$ $A=\frac{\mathbb{C}[X,Y]}{(Y^2+Y-X^3)}$

$B=A_m$ con $m=(x,y)$

$m_B/m_B^2\simeq m_A/m_A^2=\frac{(x,y)}{(x^2,xy,y^2)}=\frac{(x,y)}{(x^2,xy,x^3+y^2)}=\frac{(x,y)}{(x^2,xy,y)}=\frac{(x,y)}{(x^2,y)}=\frac{(x)}{(x^2,y)}$

$(S=A\setminus m_A \quad m_B=S^{-1}m_A \quad m_B/m_B^2\simeq S^{-1}m_A/S^{-1}m_A^2\simeq S^{-1}m_A/m_A^2=m_A/m_A^2)$

$\Rightarrow \dim_{B/m_B} m_B/m_B^2\le 1$

Se $\dim_{B/m_B} m_B/m_B^2=0 \Rightarrow m_B=m_B^2 \overset{\text{Nak}}{\Rightarrow} m_B=(0)$ ↯

Valutazioni discrete

Se $v(x)\neq v(y)$ allora $v(x+y)=\min\{v(x),v(y)\}$

Supponiamo $v(x)>v(y)$

$v(x+y)\ge\min\{v(x),v(y)\}$

$v(y)=v((x+y)+(-x))\ge\min\{v(x+y),v(-x)\}$

$v(-y)=v(-1)+v(y)=v(y)$ $\qquad 0=v(1)=v((-1)^2)=2v(-1)$

$v(x+y)\ge v(y)$

$v(y)\ge\min\{v(x+y),v(x)\}\overset{\text{per ass. } v(x+y)>v(y)}{>}v(y)$ ↯

$\Rightarrow v(x+y)\le v(y)$

Studiamo ora le valutazioni su $\mathbb{Q}$.

$v:\mathbb{Q}\longrightarrow\mathbb{Z}\cup\{\infty\}$

Oss $v|_{\mathbb{Z}}\ge 0$: $v(1)=0$, $v(2)\ge v(1)\ge 0$, ...

Per induzione $v(n)\ge 0\ \forall n>0$ e $v(-n)=v(n)$

Oss Sia $I=\{x\in\mathbb{Z}\mid v(x)\ge 1\}=(p)$

- Se $xy\in I\iff v(xy)\ge 1\iff v(x)+v(y)\ge 1$

  quindi $v(x)\ge 1$ oppure $v(y)\ge 1$

- $x\in I, y\in\mathbb{Z}\Rightarrow xy\in I$ perché $v(xy)=v(x)+v(y)\ge v(x)\ge 1$

Oss Sia $n\in\mathbb{Z}$: $n=p^km$ con $(p,m)=1$

$v(n)=v(p^k)+\underbrace{v(m)}_{=0}=v(p^k)=kv(p)$

$0=v(1)=v(n\cdot\frac{1}{n})=v(n)+v(\frac{1}{n})\Rightarrow v(\frac{1}{n})=-v(n)$

$v(\frac{a}{b})=v(a)-v(b)=(\alpha-\beta)v(p)$

$a=p^\alpha m,\ b=p^\beta\cdot m'$ con $(m,p)=1$, $(m',p)=1$

Siccome v è surgettiva, dev'essere $v(p)=1$

- $\mathbb{C}[|t|]$ è un DVR
  $v(a_0+a_1t+a_2t^2+\dots) = \min\{i \mid a_i \neq 0\}$
  $m=(t)$. A è locale: $A\setminus m = A^\times$

- $A=\mathbb{C}[t]_{(t-t_0)}$ è un DVR
  $v(p(t))$ = molteplicità di t_0 come radice di $p(t)$

$\frac{\mathbb{C}[x,y]}{(y^2+y-x^3)} = A \qquad B = A_{(x,y)}$



$v(f)$ = ordine di annullamento di f in $(0,0)$

$y(y+1)=x^3 \Longrightarrow v(y)+v(y+1)=3v(x) \Longrightarrow v(y)=3v(x)$
$v(y)=3,\ v(x)=1$
$m=(x,y)=(t) \qquad t=xp_1+yp_2$
$1=v(t)\geq \min\{v(xp_1), v(yp_2)\} \geq \min\{v(x), v(y)\}$

Esempio un anello noetheriano di dim. infinita (Nagata)
$A=K[x_1,x_2,\dots]$ anello dei polinomi in infinite variabili
$P_1=(x_1) \quad P_2=(x_2,x_3) \quad P_3=(x_4,\dots,x_7) \quad P_4=(x_8,\dots,x_{15}) \quad \dots \quad P_n=(x_{2^n},\dots,x_{2^{n+1}-1})$
sono tutti ideali primi
$S=A\setminus \bigcup P_i \qquad R:=S^{-1}A$
Dimostreremo che
(1) R è Noetheriano
(2) $I\subseteq \bigcup_{i=1}^{\infty} P_i \Longrightarrow \exists i$ t.c. $I\subseteq P_i$
(3) Gli ideali massimali sono $S^{-1}P_i$
(4) $\dim R=\infty$: $(x_{2^n}) \subsetneq (x_{2^n}, x_{2^n+1}) \subsetneq \dots \subsetneq (x_{2^n},\dots,x_{2^{n+1}-1})$
dà una catena in R di lunghezza 2^n-1

(2) Sia $I\subseteq \bigcup_{i=1}^{\infty} P_i$
$I=\bigcup_{r=1}^{\infty} I\cap K[x_1,\dots,x_r]$
$P_i\cap K[x_1,\dots,x_r]$: se tutte le variabili in P_i hanno indice $>r$, l'intersez. è 0
$I\cap K[x_1,\dots,x_r] \subseteq \bigcup_{i=1}^{2^{r+1}-1} P_i\cap K[x_1,\dots,x_r]$
$\subseteq \bigcup_{i=1}^{2^{r+1}-1} P_i\cap K[x_1,\dots,x_r]$

Lemma A anello, $P_1,\dots,P_r$ primi, I ideale di A
$I\subseteq P_1\cup\dots\cup P_r \Longrightarrow \exists i\in\{1,\dots,r\}$ t.c. $I\subseteq P_i$

$I\cap K[x_1,\dots,x_r] \subseteq P_{j(r)}$
Sia ora $f\in I\setminus\{0\}$, $f\in K[x_1,\dots,x_h]$
Per ogni $r\geq h$, $f\in I\cap K[x_1,\dots,x_r] \Longrightarrow f\in P_{j(r)}$
Questo mi dice che le variabili che generano $P_{j(r)}$ sono fra quelle che compaiono in f.
Allora l'indice $j(r)$ è limitato, quindi c'è un j che si ripete infinite volte.
Dato r, scelgo $r'\geq r$ t.c. $j(r')=j$
$I\cap K[x_1,\dots,x_r] \subseteq I\cap K[x_1,\dots,x_{r'}] \subseteq P_{j(r')} = P_j \quad \forall r$
quindi $I=\bigcup_r I\cap K[x_1,\dots,x_r] \subseteq P_j$

Lemma Sia A anello t.c.
- ogni $x \in A$ appartiene a un n° finito di ideali max
- $\forall m$ id. max di A, A_m è Noetheriano.

Allora A è Noetheriano.

DIMOSTRAZIONE

$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$

Se $I_j = (0)$ $\forall j$, ok

Altrimenti sia $x \in \bigcup I_j \setminus \{0\}$

Siano $m_1, \dots, m_n$ gli ideali max. che lo contengono

$I_h = I_{h+1} \iff S^{-1}I_h = S^{-1}I_{h+1}$ $\forall S = A \setminus m$, m massimale

Questa eguaglianza è (1)=(1) se $x \in S \iff x \notin m$.

Consideriamo $S^{-1}I_h \subseteq S^{-1}I_{h+1} \subseteq \dots$ in A_{m_i}

Siccome ogni A_{m_i} è noetheriano e ne ho un n° finito,

$\exists N$ t.c. $S^{-1}I_h = S^{-1}I_{h+1}$ $\forall h \geq N$ $\forall S = A \setminus m_i$, $i = 1, \dots, n$

$\Rightarrow \forall S = A \setminus m$, m max.

$\Rightarrow \forall h \geq N$ $I_h = I_{h+1}$ □

Vediamo che R soddisfa le ipotesi del criterio.

1) $x \in R$ sta in un n° finito di id. max.

$x = p/q$ $\quad m \ni x \Rightarrow m \ni p = xq$

Ma $p \in R \cap A$ appartiene ad un n° finito di P_i

2) Le localizzazioni $R_m = R_{S^{-1}P_i}$ sono Noetheriane:

$A''_{P_i} \ni \frac{p(x)}{q(x)}$

A_{P_i} = localiz. di $\mathbb{C}[x_j \mid x_j \notin P_i)[x_k \mid x_k \in P_i]$

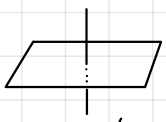
e quindi è Noetheriano.

esempio Anelli con catene massimali di lunghezze diverse

1) $A = A_1 \times A_2$ con $\dim A_1 \neq \dim A_2$

2) Con $\operatorname{Spec} A$ connesso

$\operatorname{Spec} \frac{\mathbb{C}[x,y,z]}{(xz, yz)}$



Primi $\longleftrightarrow$ Primi di $\mathbb{C}[x,y,z]$ che contengono (xz, yz)

$P \supseteq (xz, yz)$: o $P \ni z$ o $P \ni x, y$

$(z) \subsetneq (z, x) \subsetneq (z, x, y)$ $\qquad (x, y) \subseteq (x, y, z)$

Estensioni intere

Def Un'estensione di anelli è semplicemente un contenimento $A \subseteq B$ fra anelli.
$[\phi : A \longrightarrow B : B$ è un A-modulo, $a \cdot b = \phi(a)b]$

Oss $K \subseteq L$ estensione di campi: $\alpha \in L$ è algebrico su K se $\exists p(x) \in K[x] \setminus \{0\}$ t.c. $p(\alpha) = 0 \iff [K(\alpha) : K] < +\infty$
$\iff K(\alpha)$ è un K-modulo fin.gen.

Def $A \subseteq B$ estensione di anelli, $b \in B$.
b è intero su A se $\exists p(x) \in A[x]$ monico t.c. $p(b) = 0$
$A \subseteq B$ è un'estensione intera se $\forall b \in B$ è intero su A.
$A \subseteq B$ è un'estensione finita se B è fin.gen. come A-modulo.

Teorema di Cayley-Hamilton A anello, M A-modulo generato da n elementi, $I \lhd A$, $\phi : M \longrightarrow M$ endomorfismo di A-moduli.
Supponiamo $\phi(M) \subseteq IM$.
(i) $\exists a_1, \dots, a_n \in A$ t.c. $a_i \in I^i$, $\phi^n + a_1\phi^{n-1} + \dots + a_n = 0$
(ii) $I = A$. Ogni $\phi \in \mathrm{End}_A(M)$ soddisfa un polinomio monico.

Def Un A-modulo M è fedele se $a \cdot m = 0 \ \forall m \in M \Longrightarrow a = 0$.
($\varphi : A \longrightarrow \mathrm{End}_{\mathbb{Z}} M$ è iniettivo)

Lemma Sia $A \subseteq B$ estensione di anelli, $b \in B$. Sono equivalenti:
(i) b è intero su A
(ii) $A[b]$ è fin.gen. come A-modulo
(iii) $\exists C \subseteq B$ sottoanello, $A \subseteq C$, $b \in C$ t.c. C è fin.gen. come A-modulo
(iv) $\exists M$ un $A[b]$-modulo fedele che è fin.gen. come A-modulo.

Oss $A[b]$ può essere def. come l'immagine $\varphi : A[x] \longrightarrow B$, $x \longmapsto b$

DIMOSTRAZIONE
(i) $\Rightarrow$ (ii) $\exists n \geq 1$ $\exists a_1, \dots, a_n \in A$ t.c. $b^n + a_1 b^{n-1} + \dots + a_n = 0$
Dico che $A[b]$ è generato da $1, b, b^2, \dots, b^{n-1}$
$b^n = -a_n - \dots - a_1 b^{n-1} \in \langle 1, b, b^2, \dots, b^{n-1} \rangle_A$
Se $b^k \in \langle 1, b, \dots, b^{n-1} \rangle_A$, scrivo $b^k = c_0 + c_1 b + \dots + c_{n-1} b^{n-1}$
$b^{k+1} = b b^k = c_0 b + \dots + c_{n-1} b^n = c_0 b + \dots + c_{n-1}(-a_1 b^{n-1} - \dots - a_n)$
$\in \langle 1, b, \dots, b^{n-1} \rangle_A$

(ii) $\Rightarrow$ (iii) Prendo $C = A[b]$

(iii) $\Rightarrow$ (iv) Prendo $M = C$ che è fin.gen. come A-modulo ed è fedele perché $\alpha \in A[b]$ $\alpha \cdot c = 0$ $\forall c \in C \overset{c=1}{\Longrightarrow} \alpha = 0$

(iv) $\Rightarrow$ (i) La moltiplicazione per b, $[b] : M \longrightarrow M$ è un endomorfismo di un A-mod fin.gen $\overset{CH}{\Longrightarrow} \exists a_1, \dots, a_n \in A$ t.c.

$[b]^n + a_1[b]^{n-1} + \dots + a_n = 0$

$\iff$ l'endomorfismo $[b^n + a_1 b^{n-1} + \dots + a_n] = 0$

$\iff b^n + a_1 b^{n-1} + \dots + a_n = 0$ in $A[b]$ perché M è fedele $\square$

Lemma $A \subseteq B \subseteq C$

(1) B finito su A, C finito su B $\Longrightarrow$ C finito su A

(2) B finito su A $\Longrightarrow$ B intero su A

(3) Se B è intero su A ed è fin.gen. come A-algebra, allora B è finito su A.

(4) B intero su A, C intero su B $\Longrightarrow$ C intero su A.

DIMOSTRAZIONE

(1) $B = \langle b_1, \dots, b_m \rangle_A$, $C = \langle c_1, \dots, c_n \rangle_B$

Dato $c \in C$ $\exists \beta_1, \dots, \beta_n \in B$ t.c. $c = \sum_{i=1}^{n} \beta_i c_i$

Ogni β_i si può scrivere come $\beta_i = \sum_{j=1}^{m} a_{ij} b_j$

$\Longrightarrow c = \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} b_j c_i \Longrightarrow C = \langle a_i b_j \rangle_A$

(2) B finito su A $\Longrightarrow$ dato $b \in B$, b sta in un sottoanello fin.gen. come A-mod (B stesso) $\overset{\text{lemma}}{\Longrightarrow}$ b intero

Oss B fin.gen. come A-algebra vuol dire che $\exists n \geq 1$ t.c. $\exists \Phi : A[x_1, \dots, x_n] \longrightarrow B$ omo surj, $x_i \longmapsto b_i$

esempio $A = \mathbb{Z}[\frac{1}{2}] = S^{-1}\mathbb{Z}$ con $S = \{2^n\}$

è fin. gen. come $\mathbb{Z}$-algebra

ma non è fin. gen. come $\mathbb{Z}$-modulo:

se valesse $A = \langle a_1, \dots, a_n \rangle_{\mathbb{Z}}$ $a_i = \frac{p_i}{2^{n_i}}$

$N = \max\{n_i\} \Longrightarrow \langle a_1, \dots, a_n \rangle \subseteq \frac{1}{2^N}\mathbb{Z}$ ↯

(3) Per induzione sul numero dei generatori

- Se $B = A[b]$, B è un A-mod fin.gen.
- Se $B = A[b_1, \dots, b_{n+1}] = \mathrm{Im}(A[x_1, \dots, x_{n+1}] \longrightarrow B)$, $x_i \longmapsto b_i$

$B = \underbrace{(A[b_1, \dots, b_n])}_{\text{fin.gen. come } A\text{-modulo}}[b_{n+1}] \Longrightarrow$ finita su $A[b_1, \dots, b_n]$

$\Longrightarrow A \subseteq A[b_1, \dots, b_{n+1}]$ è finita per (1).

(4) $c \in C$. Siccome C/B è intera, $\exists b_1, \dots, b_n \in B$ t.c. $c^n + b_1 c^{n-1} + \dots + b_n = 0$

$A \subseteq \underbrace{A[b_1, \dots, b_n]}_{\subseteq B} \subseteq \underbrace{A[b_1, \dots, b_n][c]}_{\subseteq C}$

$A \subseteq A[b_1, \dots, b_n]$: intera + fin.gen. come A-algebra $\Longrightarrow$ finita

$A[b_1, \dots, b_n] \subseteq A[b_1, \dots, b_n][c]$: finita

$\Longrightarrow$ esiste un sottoanello di C che contiene c ed è fin.gen come A-mod

$\Longrightarrow c$ è intero su A $\Longrightarrow$ C/A intera. $\square$

corollario $A \subseteq B$ est. anelli, $C := \{b \in B \mid b \text{ è intero su } A\}$.
Questo C è detto la chiusura intera di A dentro B.
Allora C è un anello.

DIMOSTRAZIONE
$c_1, c_2 \in C$
$A \subseteq A[c_1, c_2]$: è un'est. finita che contiene $c_1 \pm c_2, c_1 c_2$
Allora questi elementi sono interi su A. □

def Un dominio A è integralmente chiuso se coincide con la sua chiusura intera in $Frac(A)$

esempio $\mathbb{Z}$ è integralmente chiuso:
sia $p/q \in \mathbb{Q}$ intero su $\mathbb{Z} \Rightarrow (p/q)^n + a_{n-1}(p/q)^{n-1} + \dots + a_0 = 0$
$x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathbb{Z}[x] \Rightarrow p \mid a_0, q \mid a_n = 1 \Rightarrow p/q \in \mathbb{Z}$

esempio $\mathbb{Z}[\sqrt{5}]$ non è integralmente chiuso:
considero $t := \frac{1+\sqrt{5}}{2}$ che annulla $X^2 - X - 1$
$t \in Frac(A) \setminus A$ è intero su A.

Lemma A UFD $\Rightarrow$ A integralmente chiuso.

DIMOSTRAZIONE
Prendiamo $p/q \in Frac(A)$, con p, q coprimi.
$(p/q)^n + a_{n-1}(p/q)^{n-1} + \dots + a_0 = 0$, $a_0 \neq 0$
Moltiplicando per q^n:
$p^n + a_{n-1}p^{n-1}q + \dots + a_0 q^n = 0$
ma $p^n = -(a_{n-1}p^{n-1}q + \dots + a_0 q^n)$ è divisibile per q ↯
Se q non ha fattori primi, è un'unità $\Rightarrow p/q \in A$ □

Lemma $A \subseteq B$ estensione di anelli.
C chiusura intera di A in B, D chiusura intera di C in B.
Allora $D = C$.

DIMOSTRAZIONE
($\supseteq$) ok
($\subseteq$) $d \in D$ è intero su C : $\exists c_1, \dots, c_n$ t.c. $d^n + c_1 d^{n-1} + \dots + c_n = 0$
Ora c_i è intero su A $\forall i \Rightarrow A \subseteq A[c_1, \dots, c_n] \subseteq A[c_1, \dots, c_n][d]$
(intero) (intero)
$\Rightarrow d$ è intero su $A \Rightarrow d \in C$. □

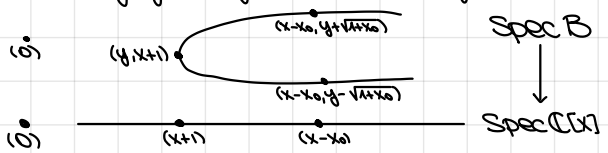
Lemma $A \subseteq B$ estensione intera.
(i) Se S è una parte moltiplicativa di A, $S^{-1}A \subseteq S^{-1}B$ è intera
(ii) Se Q è un ideale primo di B e $P = Q \cap A$, l'estensione $A/P \subseteq B/Q$ è intera

$$\begin{array}{ccccc} A & \hookrightarrow & B & \longrightarrow & B/Q \\ & \searrow & & \nearrow & \\ & & A/P & & \end{array}$$

DIMOSTRAZIONE
(i) Prendiamo $\frac{b}{s} \in S^{-1}B$. Siccome B/A intera,
$b^n + a_{n-1}b^{n-1} + \dots + a_0 = 0$
Divido per s^n: $\left(\frac{b}{s}\right)^n + \frac{a_1}{s}\left(\frac{b}{s}\right)^{n-1} + \dots + \frac{a_0}{s^n} = 0$
trovo che $\frac{b}{s}$ è intero su $S^{-1}A$.
[Più precisamente, uno dovrebbe considerare $x^n + \frac{a_{n-1}}{s}x^{n-1} + \dots + \frac{a_0}{s^n} \in S^{-1}A[x]$]
(ii) $\overline{b} \in B/Q$ è la classe di $b \in B$. Scrivo $b^n + a_{n-1}b^{n-1} + \dots + a_0 = 0$
Riducendo mod Q, trovo $\overline{b}^n + a_{n-1}\overline{b}^{n-1} + \dots + a_0 = 0$ □

Interpretazione geometrica
$A \subseteq B$ estensione intera $\longleftrightarrow$ $\operatorname{Spec} B \longrightarrow \operatorname{Spec} A$
"assomiglia a un rivestimento (ramificato)"

esempio $\mathbb{C}[x] \subseteq \frac{\mathbb{C}[x,y]}{(y^2-(x+1))} = A[y]$
A $\qquad B = A \oplus A = \langle 1, y \rangle_A$
$f(x,y) \in B \rightsquigarrow f(x,y) = f_1(x,y) + y\, f_2(x)$
Com'è fatta $\operatorname{Spec} B \longrightarrow \operatorname{Spec} A$?
Ideali primi: in B, c'è $(0) = (y^2-(x+1))$ e gli ideali primi di $\mathbb{C}[x,y]$ che contengono $y^2-(x+1)$
$(x-x_0, y-y_0) \ni y^2-(x+1) \iff y_0^2-(x_0+1) = 0$



Lemma $A \subseteq B$ est. intera tra domini d'integrità.
A è un campo $\iff$ B è un campo

DIMOSTRAZIONE
($\Longrightarrow$) Sia $b \in B \setminus \{0\}$. Per integralità, $b^n + a_{n-1}b^{n-1} + \dots + a_0 = 0$, $a_0 \neq 0$
$-b \cdot (b^{n-1} + a_{n-1}b^{n-2} + \dots + a_1) = +a_0$
A campo $\Longrightarrow$ $b \cdot [-a_0^{-1}(b^{n-1} + \dots + a_1)] = 1$
quindi b è invertibile.
($\Longleftarrow$) Sia $a \in A \setminus \{0\}$. $\exists b \in B$ t.c. $ab = 1$
$b^n + a_{n-1}b^{n-1} + \dots + a_0 = 0$
Moltiplico per a^{n-1}: $b + a_{n-1} + a_{n-2}a + \dots + a_0 a^{n-1} = 0$
$\Longrightarrow b = -a_{n-1} - a_{n-2}a - \dots - a_0 a^{n-1} \in A$ □

Esempio K estensione finita di $\mathbb{Q}$, $\mathbb{Z} \subset K$
L'anello degli interi di K è la chiusura intera di $\mathbb{Z}$ in K, $\mathcal{O}_K$.
Mostriamo che $\dim \mathcal{O}_K = 1$
(0) è primo in $\mathcal{O}_K$. Sia $P \neq (0)$ un primo di $\mathcal{O}_K$.
Sia $b \in P$ un elemento non nullo
$b^n + a_{n-1}b^{n-1} + \dots + a_0 = 0$, $a_0 \neq 0$
$\mathbb{Z} \ni a_0 = -(b^n + a_{n-1}b^{n-1} + \dots + a_1 b) \in P \implies P \cap \mathbb{Z} \neq (0)$
$\implies P \cap \mathbb{Z} = (p)$ è massimale
$\underbrace{\mathbb{Z}/(p)}_{\mathbb{F}_p \text{ campo}} \subseteq \mathcal{O}_K/P$ è intera
$\implies \mathcal{O}_K/P$ campo $\implies P$ massimale
$\implies \dim \mathcal{O}_K = 1$

Def. Sia $(A, \mathfrak{m})$ un DVR.
Un generatore di $\mathfrak{m}$ si dice un uniformizzante.

Lemma A Noetheriano, M A-modulo, $M \neq (0)$.
Dato $m \in M$, $\mathrm{Ann}(m) = \{a \in A \mid am = 0\}$
$\mathrm{Ann}\, M = \{\mathrm{Ann}(m) \mid m \in M \setminus \{0\}\}$
(i) Gli ideali in $\mathrm{Ann}\, M$ sono propri
(ii) Ogni el. di $\mathrm{Ann}\, M$ è contenuto in un el. massimale di $\mathrm{Ann}\, M$.
(iii) Ogni el. massimale di $\mathrm{Ann}\, M$ è un ideale primo

DIMOSTRAZIONE
(i) $1 \cdot m = 0 \implies m = 0$
(ii) Per Noetherianità
(iii) Sia I un el. massimale, $ab \in I = \mathrm{Ann}(M)$
Se $am = 0 \implies a \in I$
Se $am \neq 0$, considero $\mathrm{Ann}(am) \supseteq (I, b)$
Per massimalità, $I = \mathrm{Ann}(am) \ni b$ □

Teorema Sia A dominio locale Noetheriano di dim 1. Sono equivalenti:
(i) A è un DVR
(ii) A è integralmente chiuso.

DIMOSTRAZIONE
(i) $\implies$ (ii) DVR $\implies$ PID $\implies$ UFD $\implies$ integralmente chiuso.
(ii) $\implies$ (i) Scelgo $t \in \mathfrak{m} \setminus \mathfrak{m}^2$ (se $\mathfrak{m} = \mathfrak{m}^2 \overset{\text{Nak}}{\implies} \mathfrak{m} = (0)$ ↯)
Sia P un ideale massimale della famiglia $\mathrm{Ann}(A/(t))$
Dall'ipotesi $\dim A = 1$ + A locale segue che gli unici ideali primi sono (0) e $\mathfrak{m}$.
Siccome $\mathrm{Ann}(A/(t)) \ni \mathrm{Ann}(\bar{t})$ e (0) non è massimale $\implies P = \mathfrak{m}$.
Quindi $\exists a \in A/(t)$ t.c. $\mathfrak{m} = \{r \in A \mid r\bar{a} = 0 \text{ in } A/(t)\} =$
$= \{r \in A \mid ra \in (t)\} = \{r \in A \mid r\frac{a}{t} \in A\}$
Consideriamo $\left[\frac{a}{t}\right] : \mathfrak{m} \longrightarrow A$ mappa di A-moduli
L'immagine è un ideale.

Caso 1 : $\mathrm{Im}[\frac{a}{t}] = A$

$\Rightarrow \exists b \in M$ t.c. $b\frac{a}{t} = 1 \iff t = ab$. Allora $a \notin M$, altrimenti $t = ab \in M^2$. Quindi $a \in A^\times$

$\Rightarrow [\frac{1}{t}] : M \longrightarrow A \Rightarrow \forall m \in M \ \frac{m}{t} \in A \Rightarrow m \in (t)$.

Caso 2 : $\mathrm{Im}[\frac{a}{t}] \subsetneq M$

$[\frac{a}{t}] : M \longrightarrow M \Rightarrow [\frac{a}{t}]$ è endom. di un A-mod fin.gen.

$\Rightarrow \frac{a}{t}$ intero su $A \Rightarrow \frac{a}{t}$ è chiusura intera $= A$

$\Rightarrow M = \{r \in A \mid r\frac{a}{t} \in A\} = A$ ↯ □

corollario $A \subseteq B$ est. intera, $Q \in \mathrm{Spec}B$, $P = Q \cap A$. Allora P è massimale $\iff$ Q è massimale

DIMOSTRAZIONE

$A/P \subset B/Q$ è intera fra domini.

Per il lemma A/P campo $\iff$ B/Q campo □

$A \subseteq B$ intera $\rightsquigarrow$ $\mathrm{Spec}B$ $\quad q$ "sta sopra p"

$\downarrow$

$\mathrm{Spec}A$ $\quad p = q \cap A$ "sta sotto q"

teorema: lying over Sia $A \subseteq B$ un'estensione intera. La mappa $i^\#$ è surgettiva: $\forall p \in \mathrm{Spec}A$ $\exists q \in \mathrm{Spec}B$ t.c. $q \cap A = p$.

DIMOSTRAZIONE

$i_p^{-1}(\tilde{q})$ è max

$$\begin{array}{ccc} A_p & \xrightarrow{i_p} & B_p = S^{-1}B \text{ con } S = A \setminus p \\ {\scriptstyle g_A}\uparrow & \circlearrowright & \uparrow{\scriptstyle g_B} \\ A & \xrightarrow{i} & B \end{array}$$

(B_p: ideale massimale $\tilde{q}$)

i_p intera, $\tilde{q}$ massimale $\overset{\text{es}}{\Rightarrow}$ $i_p^{-1}(\tilde{q})$ è massimale quindi è pA_p

Allora $g_A^{-1}(i_p^{-1}(\tilde{q})) = g_A^{-1}(pA_p) = p$

Ma $g_B \circ i = i_p \circ g_A$

$(i_p \circ g_A)^{-1}(\tilde{q}) = p = (g_B \circ i)^{-1}(\tilde{q}) = i^{-1}(\underbrace{g_B^{-1}(\tilde{q})}_{q})$

Ho costruito $q := g_B^{-1}(\tilde{q}) \in \mathrm{Spec}B$ con la proprietà voluta □

Teorema: going up

$A \subseteq B$ estensione intera.

B $\quad q_1 \subsetneq \dots \subsetneq q_m$

$|$ $\quad$ con $m<n$.

A $\quad p_1 \subsetneq p_2 \subsetneq \dots \subsetneq p_n \qquad p_i = q_i \cap A$ per $i=1,\dots,m$

Allora esistono $q_{m+1} \subsetneq \dots \subsetneq q_n$ t.c.

(i) $q_m \subsetneq q_{m+1}$

(ii) $q_j \cap A = p_j$ per $j = m+1, \dots, n$

DIMOSTRAZIONE

Per induzione + lying over, basta il caso $n=2, m=1$

Consideriamo l'estensione intera $A/q_1 \cap A \subseteq B/q_1$, cioè $A/p_1 \subseteq B/q_1$.

q_1/q_1

$p_1/p_1 \subsetneq p_2/p_1$

Per lying over, esiste un primo $\bar{q}_2$ di B/q_1 la cui contrazione a A/p_1 è p_2/p_1. Ora $\bar{q}_2 = q_2/q_1$ per un certo $q_2 \in \operatorname{Spec} B$ con $q_2 \supseteq q_1$.

Verifichiamo che $q_2 \cap A = p_2$

$$\ker(A \longrightarrow B \longrightarrow B/q_2) = q_2 \cap A$$

$$A \longrightarrow A/p_1 \hookrightarrow B/q_1 \longrightarrow \frac{B/q_1}{q_2/q_1} \simeq B/q_2$$

A/p_1 ha nucleo $A/p_1 \cap \bar{q}_2 = p_2/p_1$

A ha nucleo p_2

le due mappe hanno lo stesso nucleo, quindi $q_2 \cap A = p_2$

Nota: $q_2 \neq q_1$ perché $q_1 \cap A \neq q_2 \cap A$ □

Teorema: incomparabilità

$A \subseteq B$ estensione intera, $q_1 \subsetneq q_2$ ideali primi di B.

Allora $q_1 \cap A \subsetneq q_2 \cap A$.

Oss Fissiamo $\mathfrak{p} \in \operatorname{Spec} A$. Due primi $q_1 \neq q_2$ di B che contraggono a $\mathfrak{p}$ non possono essere contenuti l'uno dentro l'altro.

DIMOSTRAZIONE

$p := q_1 \cap A$. Consideriamo $A/p \subseteq B/q_1$

Ho due ideali primi $q_1/q_1 = 0$ e $q_2/q_1 \neq 0$ di B/q_1.

La tesi è che $q_2/q_1 \cap A/p \neq \{0\}$.

Sia $b \in q_2/q_1$, $b \neq 0$. Siccome l'estensione è intera,

$\exists n \ \exists \bar{a}_1, \dots, \bar{a}_n \in A/p$ t.c. $b^n + \bar{a}_1 b^{n-1} + \dots + \bar{a}_n = 0$

Siccome B/q_1 è dominio, prendendo n minimale posso supporre $\bar{a}_n \neq 0$

$q_2/q_1 \supseteq (b) \ni b(b^{n-1} + \bar{a}_1 b^{n-2} + \dots + \bar{a}_{n-1}) = -\bar{a}_n \in A/p$

cioè $\bar{a}_n \in q_2/q_1 \cap A/p \neq (0)$, come voluto. □

teorema $A \subseteq B$ estensione intera.
Allora $\dim A = \dim B$

DIMOSTRAZIONE
Se $p_1 \subsetneq p_2 \subsetneq \dots \subsetneq p_n$ è una catena di primi in A,
per going up trovo $q_1 \subsetneq q_2 \subsetneq \dots \subsetneq q_n$ in B
$\Rightarrow \dim B \geq \dim A$
Presa $q_1 \subsetneq q_2 \subsetneq \dots \subsetneq q_n$ catena in B,
$q_1 \cap A \subsetneq q_2 \cap A \subsetneq \dots \subsetneq q_n \cap A$ per incomparabilità
$\Rightarrow \dim B \leq \dim A \quad \Rightarrow \dim A = \dim B$ □

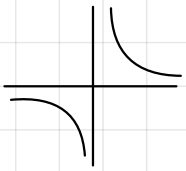
Oss $i: A \hookrightarrow B$ est. intera $\Rightarrow i^*: \operatorname{Spec} B \longrightarrow \operatorname{Spec} A$ è una mappa chiusa
(Facciamo solo il caso Noetheriano)
Sia $q \in \operatorname{Spec} B$. $i^* V(q) = V(q \cap A)$
$i^* V(q) = i^*(\{q' \in \operatorname{Spec} B \mid q' \supseteq q\}) = \{q' \cap A \mid q' \supseteq q\}$
$V(q \cap A) = \{p \in \operatorname{Spec} A \mid p \supseteq q \cap A\}$
L'inclusione ($\subseteq$) è chiara
Viceversa, dato $p \in V(q \cap A)$,
per going-up $\exists q' \supseteq q$ t.c. $q' \cap A = p$

$$\begin{array}{ccc} q & \subseteq & q' \\ | & & | \\ q \cap A & \subseteq & p \end{array}$$

In generale, $V(I) = \bigcup_{\substack{q \supseteq I \\ q \text{ minimale sopra } I}} V(q) = V(q_1) \cup \dots \cup V(q_n)$

L'insieme dei primi minimali sopra I è finito: corrispondono ai primi minimali di B/I (che sono in n° finito per Noetherianità)
$i^*(V(I)) = i^*(V(q_1)) \cup \dots \cup i^*(V(q_n)) = V(q_i) \cup \dots \cup V(q_f)$ è unione finita di chiusi, quindi chiuso.

esempio $\mathbb{C}[x] \subseteq \dfrac{\mathbb{C}[x,y]}{(xy-1)} = \mathbb{C}[x]\left[\frac{1}{x}\right]$



Non è intera: i^* non è surgettiva,
in quanto (x) non è la contrazione di
un primo in $\frac{\mathbb{C}[x,y]}{(xy-1)}$, perché l'unico ideale
che contiene (x) è (1).

Oss $A \subseteq S^{-1}A$, con A dominio, è intera sse è uguaglianza

DIMOSTRAZIONE
$i^*: \operatorname{Spec} S^{-1}A \longrightarrow \operatorname{Spec} A$ è surgettiva
$\{P \in \operatorname{Spec} A \mid P \cap S = \emptyset\} \longrightarrow \{P \in \operatorname{Spec} A\}$
Stiamo dicendo che ogni primo di A interseca S
se $S \Rightarrow$ S non appartiene in alcun massimale $\Rightarrow S \subseteq A^\times$ □

Tornando all'es.
$$\frac{\mathbb{C}[x,y]}{(xy-1)} \simeq \frac{\mathbb{C}[x, x+y]}{(x(t-x)-1)} = \underbrace{\frac{\mathbb{C}[x,t]}{(x^2-tx+1)}}_{\text{intera}} \supseteq \mathbb{C}[t]$$

def $x_1,\dots,x_m$ si dicono algebricamente indipendenti se

$$K[t_1,\dots,t_m] \longrightarrow A$$
$$t_i \longmapsto x_i \qquad \text{è iniettivo}$$

Teorema di normalizzazione di Noether Sia K un campo, A K-algebra fin.gen. Esistono $x_1,\dots,x_m \in A$ algebricamente indipendenti tali che $K[x_1,\dots,x_m] \subseteq A$ sia un'estensione finita.

DIMOSTRAZIONE

Per induzione sul n° di generatori di A

- $n=0$: $A \simeq K$
- $n=1$: $\varphi: K[x] \twoheadrightarrow A$
  Se $\ker\varphi = 0$, $A \simeq K[x]$
  Se $\ker\varphi = (f(x))$, posso supporre f monico
  $A \simeq K[x]/(f(x)) \supseteq K$ è un'estensione finita generata dall'elemento x, che soddisfa un polinomio monico.
- $n \geq 2$: Sia $\varphi: K[t_1,\dots,t_n] \twoheadrightarrow A$
  Se φ è iniettivo, ho finito.
  Se $\ker\varphi \neq (0)$, considero un polinomio $f(t_1,\dots,t_n) \neq 0$ t.c. $f(x_1,\dots,x_n)=0$
  Poniamo $y_i = x_i - a_i x_n$ per $i=1,\dots,n-1$ dove $a_i \in K^x$
  $$0 = f(x_1,\dots,x_n) = f(y_1+a_1x_n, \dots, y_{n-1}+a_{n-1}x_n, x_n)$$
  Se $g := f(t_1+a_1t_n,\dots,t_{n-1}+a_{n-1}t_n,t_n)$ è monico nella variabile t_n, allora
  $$A = K[x_1,\dots,x_n] = K[y_1,\dots,y_{n-1},x_n] = \frac{K[y_1,\dots,y_{n-1}][t_n]}{(g)}$$
  $$K[z_1,\dots,z_m] \underset{\text{finita}}{\subseteq} K[y_1,\dots,y_{n-1}] \underset{\text{finita}}{\subseteq} A$$
  con $z_1,\dots,z_m$ alg. indip.

Scopo: fissare $a_1,\dots,a_{n-1}$ t.c. $f(t_1+a_1t_n,\dots,t_{n-1}+a_{n-1}t_n,t_n)$ abbia come monomio di grado max in t_n un termine della forma $c\,t_n^q$ con $c \in K^x$

Fissiamo un monomio $\gamma t_1^{e_1}\cdot\ldots\cdot t_n^{e_n}$. Sostituendo trovo
$$\gamma(t_1+a_1t_n)^{e_1}\cdot\ldots\cdot(t_{n-1}+a_{n-1}t_n)^{e_{n-1}}\cdot t_n^{e_n}$$
il monomio di grado max in t_n è $\gamma(a_1^{e_1}\cdot\ldots\cdot a_{n-1}^{e_{n-1}})\,t_n^{\sum e_i}$

Sommando sui monomi, se f è di grado totd e se f_d è la parte omogenea di grado d,
$$f(t_1+a_1t_n,\dots,t_{n-1}+a_{n-1}t_n,t_n) = f_d(a_1,\dots,a_{n-1},1)\,t_n^d + \text{termini con } \deg_n < d$$
Se K è infinito, il polinomio f_d non si annulla identicamente su $(K^x)^n \Longrightarrow$ posso trovare $a_1,\dots,a_{n-1}$ t.c. $f_d(a_1,\dots,a_{n-1},1)\neq 0$

Se K è finito, poniamo $y_i = x_i - x_n^{r^i}$, dove r è un intero positivo grande
Stesso conto:
$$\gamma t_1^{e_1}\cdot\ldots\cdot t_n^{e_n} \rightsquigarrow \gamma(t_1-t_n^{r})^{e_1}(t_2-t_n^{r^2})^{e_2}\cdot\ldots\cdot(t_{n-1}-t_n^{r^{n-1}})^{e_{n-1}}t_n^{e_n}$$
Il termine di grado max in t_n è
$$\gamma\, t_n^{e_n+re_1+r^2e_2+\dots+r^{n-1}e_{n-1}}$$
Scegliendo $r >$ tutti gli esponenti di tutti i monomi di f, possiamo garantire di avere un unico monomio γt_n^E di grado massimo. □

esempio Ancora DVR

$\left(\frac{\mathbb{C}[x,y]}{(y^2-x^3-x^2)}\right)_{(x,y)} =: B$ non è DVR

Per la caratterizzazione dei DVR, B non può essere integralmente chiuso

$t := \frac{y}{x} \in Frac(B)$

- t è intero su B:

  $y^2 = x^3+x^2 \longrightarrow \left(\frac{y}{x}\right)^2 = x+1$

  cioè t soddisfa $t^2-(x+1)$

- $t \notin B$: $\frac{y}{x} = t = \frac{a}{s} = \frac{a_1(x)+ya_2(x)}{s_1(x)+ys_2(x)}$ $a \in A$, $s \in A\setminus(x,y)$

  $\Leftrightarrow s_1(x)y + (x^3+x^2)s_2(x) = a_1(x)x + ya_2(x)x$

  Confrontando i coefficienti di y trovo $s_1(x) = xa_2(x)$

  $\Rightarrow s = xa_2(x)+ys_2(x) \in (x,y)$ ↯

- $i: \frac{\mathbb{C}[x,y]}{(y^2-x^3-x^2)} \subseteq \frac{\mathbb{C}[x,y]}{(y^2-x^3-x^2)}\left[\frac{y}{x}\right] \subsetneq Frac A$

  finita; ha dim = 1

  $t = \frac{y}{x}$ $t^2 = \frac{y^2}{x^2} = \frac{x^3+x^2}{x^2} = x+1 \Rightarrow x = t^2-1$, $y = tx = t(t^2-1)$

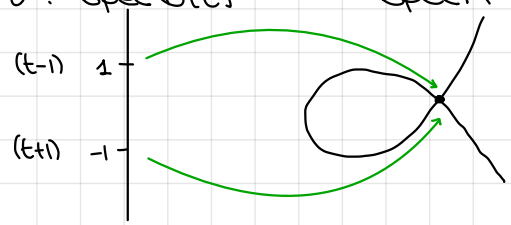
  $\frac{\mathbb{C}[x,y]}{(y^2-x^3-x^2)}\left[\frac{y}{x}\right] \simeq \mathbb{C}[t]$

$i: \frac{\mathbb{C}[x,y]}{(y^2-x^3-x^2)} \longrightarrow \mathbb{C}[t]$

$x \longmapsto t^2-1$

$y \longmapsto t(t^2-1)$

$i^\#: Spec\,\mathbb{C}[t] \longrightarrow Spec A$



$i^\#: (t-t_0) \longmapsto (x-x_0, y-y_0)$

$i^\#(t-t_0) = (x-x_0, y-y_0)$ vuol dire che $(t-t_0)\cap A = (x-x_0, y-y_0)$

$(t-t_0) \supseteq (t^2-1-x_0, t(t^2-1)-y_0)$

Quindi $\begin{cases} t_0^2-1-x_0 = 0 \\ t_0(t_0^2-1)-y_0 = 0 \end{cases}$ $\begin{cases} x_0 = t_0^2-1 \\ y_0 = t_0(t_0^2-1) \end{cases}$

Viceversa, se fisso $M = (x-x_0, y-y_0)$, chi sono i massimali $(t-t_0)$ t.c. $i^\#(t-t_0) = M$?

Se $x_0 \neq 0$, $t_0 = \frac{t_0(t_0^2-1)}{t_0^2-1} = \frac{y_0}{x_0}$

Se invece $x_0 = 0$, $(x, y-y_0) \supseteq (y^2-x^3-x^2) \Leftrightarrow y^2 \in (x, y-y_0) \Leftrightarrow y_0 = 0$

Per questo ideale, $i^\#(t_0-1) = i^\#(t_0+1) = (x,y)$

Sia $D = \mathbb{C}[t^2-1, t(t^2-1)] = \{p(t) \in \mathbb{C}[t] \mid p(1) = p(-1)\}$

$\frac{\mathbb{C}[x,y]}{(y^2-x^3-x^2)}\left[\frac{1}{x}\right] \xrightarrow{\sim} \mathbb{C}[t]\left[\frac{1}{t}\right]$

$x \longmapsto t^2-1$ è ben def

$y \longmapsto t(t^2-1)$

$y/x \longleftarrow t$

Lemma K campo, $A = K[x_1, \dots, x_n]$, $I \trianglelefteq A$ ideale, $I \neq (0)$.
Esiste un isomorfismo $\varphi : A \longrightarrow A$ (come K-algebra) tale che $\varphi(I)$ contenga un polinomio monico in x_n.
Più precisamente, preso $f \neq 0$, $\exists \varphi : A \xrightarrow{\sim} A$ t.c.
$\varphi(f) = c_d(x_1, \dots, x_{n-1}) x_n^d + \dots + c_0(x_1, \dots, x_{n-1})$ a blocchi
$c_d(x_1, \dots, x_{n-1}) \in K$.

DIMOSTRAZIONE
φ manda $x_n \longmapsto x_n$ e $x_i \longmapsto x_i - x_n^{r^i}$ dove r è un intero sufficientemente grande (inversa: $x_i \longmapsto x_i + x_n^{r^i}$) □

Oss
- A K-algebra fin. gen. da n generatori, $K[t_1, \dots, t_m] \subseteq_{\text{finita}} A$ con $m \leq n$.
- $\dim A = \dim K[t_1, \dots, t_m] = m$, quindi m è univocamente determinato da A

Def A anello commutativo, $P \in \operatorname{Spec} A$.
L'altezza di P è la dimensione di A_P, ossia la massima lunghezza di una catena di primi che termina con P.

Lemma In un UFD, i primi di altezza 1 sono principali

DIMOSTRAZIONE
Sia P di altezza 1 (cioè l'unico primo strettamente contenuto in P è (0)).
$P \neq (0)$. Scelgo $x \in P$ e lo scrivo
$P \ni x = u \cdot p_1^{e_1} \cdots p_r^{e_r}$
WLOG $p_1 \in P$, cioè $(0) \subsetneq (p_1) \subseteq P$ e (p_1) è primo
Siccome l'unico primo $\subsetneq P$ è (0), allora $(p_1) = P$. □

Teorema K campo, $\dim K[x_1, \dots, x_m] = m$.

DIMOSTRAZIONE
- $\dim K[x_1, \dots, x_m] \geq m$: basta considerare $(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \dots \subsetneq (x_1, \dots, x_m)$.
- $\dim K[x_1, \dots, x_m] \leq m$: per induzione
  - $m = 0, 1$: chiaro
  - $m \geq 2$: prendiamo una catena di primi
    $(0) \subsetneq P_1 \subsetneq P_2 \subsetneq \dots \subsetneq P_r$ con P_1 principale (come nel lemma)
    Poi il lemma, $P_1 = (f)$. Per il lemma precedente, esiste un automorfismo $\varphi : A \xrightarrow{\sim} A$ t.c. $\varphi(f) = c x_m^d + \dots$
    Sostituendo f con $\frac{1}{c} f$, posso supporre $\varphi(f)$ monico in x_m.

Quozientando per P_1, trovo la catena

$$P/P_1 \subsetneq P_2/P_1 \subsetneq \dots \subsetneq P/P_1$$

di lunghezza $r-1$ in $K[x_1,\dots,x_m]/(f) = \frac{K[x_1,\dots,x_{m-1}][x_m]}{(f)}$

che è un est. intera di $K[x_1,\dots,x_{m-1}]$

Per hp. ind. $\dim K[x_1,\dots,x_{m-1}] = m-1$

Per est. intera, $\dim \frac{K[x_1,\dots,x_{m-1}][x_m]}{(f)} = m-1$

Quindi la catena ha lunghezza $\leq m-1$, cioè

$r-1 \leq m-1 \implies r \leq m$. □

Lemma di Zariski Sia L/K un'estensione di campi con L fin.gen. come K-algebra. Allora l'estensione è finita.

OSS $\mathbb{Q}(\pi)/\mathbb{Q}$ non è fin.gen. come $\mathbb{Q}$-algebra (guardiamo i denominatori)

DIMOSTRAZIONE

Per Noether, $L \supseteq_{\text{finita}} K[t_1,\dots,t_m]$

$\dim L = 0$ perché è un campo

$\implies \dim K[t_1,\dots,t_m] = 0 \implies L/K$ finita □

Corollario: Nullstellensatz debole K campo, A K-algebra fin.gen., M ideale massimale. Allora

(i) A/M è un'est. finita di K.

(ii) Se $K = \overline{K}$, allora $A/M \simeq K$.

(iii) Se $K = \overline{K}$ e $A = K[x_1,\dots,x_n]$, ogni M massimale è della forma $(x_1-a_1,\dots,x_n-a_n)$ per certi $a_1,\dots,a_n \in K$.

OSS $i: K \hookrightarrow A \longrightarrow A/I$ è ancora iniettiva a meno che $I \cap K^\times \neq \emptyset$, nel qual caso $I = (1)$.

DIMOSTRAZIONE

(i) $K \subseteq A/M$ è est. di campi, fin.gen. $\therefore$ applico Zariski

(ii) L'unica est. finita di un campo alg. chiuso è lui stesso.

(iii) $\pi: A \longrightarrow A/M \simeq \overline{K}$ $\therefore$ per costruzione, $x_i - a_i \in \ker \pi$

$x_i \longmapsto a_i \implies (x_i - a_i) \in M \ \forall i$

$\implies (x_1-a_1,\dots,x_n-a_n) \subseteq M$ ed è uguaglianza perché $(x_1-a_1,\dots,x_n-a_n)$ è massimale. □

Teorema: going down

$A \subseteq B$ est. intera di domini con A integralmente chiuso.

$$\begin{array}{ccc} B & & q_1 \\ | & & \\ A & & p_1 \neq p_2 \end{array}$$

Allora $\exists q_2 \in \operatorname{Spec} B$, $q_2 \subsetneq q_1$ tale che $q_2 \cap A = p_2$.

<u>Oss</u> Sotto le ipotesi del Teorema, $i: A \longrightarrow B$ induce $i^{\#}: \operatorname{Spec} B \longrightarrow \operatorname{Spec} A$ che è aperta.

<u>Oss</u>

$$\begin{array}{ccc} B & & \operatorname{Frac} B = L \\ | & & \cup | \\ A & & \operatorname{Frac} A = K \end{array}$$

Dimostreremo il Teorema sotto l'ipotesi che L/K sia finita e separabile

Lemma

$A \subseteq B$ est. intera di domini, $A \in B$ integralmente chiusi. Supponiamo $L := \operatorname{Frac} B / K := \operatorname{Frac} A$ sia di Galois, con G gruppo finito.

(i) G agisce su $\operatorname{Spec} B$

(ii) Fissiamo $P \in \operatorname{Spec} A$. L'azione precedente è transitiva sull'insieme $\{Q \in \operatorname{Spec} B \mid Q \cap A = P\}$.

DIMOSTRAZIONE

(i) Sia $b \in B$ e $\sigma \in G$. Voglio dim. che $\sigma(b) \in B$.

$\sigma|_B : B \longrightarrow B$, $\sigma^{-1}|_B : B \longrightarrow B$.

b soddisfa un'equazione monica a coeff. in A:

$b^n + a_1 b^{n-1} + \dots + a_{n-1} b + a_n = 0$ con $a_1, \dots, a_n \in A$.

Applicando σ trovo

$$0 = \sigma(0) = \sigma(b^n + a_1 b^{n-1} + \dots + a_n) = \sigma(b)^n + \sigma(a_1)\sigma(b)^{n-1} + \dots + \sigma(a_n) = \\ = \sigma(b)^n + a_1 \sigma(b)^{n-1} + \dots + a_n$$

$\Longrightarrow \sigma(b)$ è intero su $A \Longrightarrow \sigma(b) \in \operatorname{Frac} B$ è intero su B.

Poiché B è integralmente chiuso, $\sigma(b) \in B$.

Quindi $\sigma|_B$ è isomorfismo e in part. manda primi in primi.

(ii) Sia $P \in \operatorname{Spec} A$ e $Q \in \operatorname{Spec} B$ t.c. $Q \cap A = P$, $\sigma \in G$.

$\sigma(Q) \cap A = \sigma(Q) \cap \sigma(A) = \sigma(Q \cap A) = \sigma(P) = P$

Mostriamo la transitività: sia $Q_2 \in \operatorname{Spec} B$ t.c. $Q_2 \cap A = P$.

Per assurdo non esista $\sigma \in G$ t.c. $\sigma Q = Q_2$.

Allora $\forall \sigma \in G$ $Q_2 \neq \sigma Q$: per incomparabilità, se volesse $Q_2 \subseteq \sigma Q$, poiché $Q_2 \cap A = Q \cap A$, avrei $Q_2 = \sigma Q$.

Quindi $Q_2 \not\subseteq \bigcup_{\sigma \in G} \sigma Q$ per scansamento.

Scegliamo $b \in Q_2 \setminus \bigcup_{\sigma \in G} \sigma Q$. Considero $a := \prod_{\sigma \in G} \sigma(b)$

a è un elemento di A:

(i) $a \in \mathrm{Frac}A \iff \tau a = a \ \forall \tau \in G$ (l'est. è di Galois)

(ii) a è prodotto di elem di B, ossia prodotto di elem. interi su A

$\Rightarrow a$ è intero su A.

Poiché A è int. chiuso, $a \in A$.

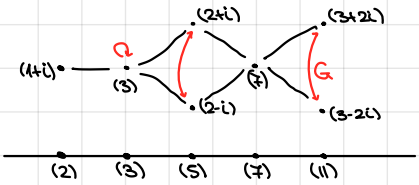
Ora $a \in (b) \subseteq Q_2 \implies a \in Q_2 \cap A = P \subseteq Q$

Allora $\prod_{\sigma \in G} \sigma(b) \in Q \implies \exists \sigma \in G$ t.c. $\sigma(b) \in Q \iff b \in \sigma^{-1} Q$

ma $b \notin \sigma Q \ \forall \sigma$, assurdo. □

esempio

K — finita Galois — $\mathbb{Q}$; $B = \mathcal{O}_K$ = chiusura intera di $\mathbb{Z}$ in K — $\mathbb{Z}$



$\mathrm{Spec}\,\mathbb{Z}[i]$; $\mathrm{Spec}\,\mathbb{Z}$

$K = \mathbb{Q}(i)$ — $\mathbb{Q}$

$\mathbb{Z}[i] \xrightarrow{\sigma} \mathbb{Z}[i] \longrightarrow \mathbb{Z}[i]/(3)$

$\mathbb{Z}[i] \longrightarrow \mathbb{Z}[i]/(3) \xrightarrow{\sim} \mathbb{Z}[i]/(3)$

$\bar{\sigma} : \mathbb{F}_3[i] \longrightarrow \mathbb{F}_3[i]$

DIMOSTRAZIONE

$\tilde{B}$ — B — A ; $\tilde{q}_1 \neq \tilde{q}_2$; $q_1 \neq q_2$; $q_1 \neq q_2$; $p_1 \neq p_2$

$\tilde{L}$ = chiusura di Galois di L/K

$L = \mathrm{Frac}B$ — $K = \mathrm{Frac}A$) supposta finita + separabile

$\tilde{B}$ = chiusura intera di A dentro $\tilde{L}$: dominio integralmente chiuso con $\mathrm{Frac}(\tilde{B}) = \tilde{L}$

Infatti, sia $\ell \in \tilde{L}$: è algebrico su K, quindi posso trovare un pol. monico $f(x) \in K[x]$ t.c. $f(\ell) = 0$.

$$\ell^n + \frac{a_1}{d_1}\ell^{n-1} + \dots + \frac{a_n}{d_n} = 0 \quad \text{con } a_i, d_i \in A$$

Moltiplico per $(d_1 \cdots d_n)^n$:

$$(d_1 \cdots d_n \ell)^n + a_1 d_2 \cdots d_n (d_1 \cdots d_n \ell)^{n-1} + \dots + a_n (d_1 \cdots d_{n-1})^n d_n^{n-1} = 0$$

Quindi $d_1 \cdots d_n \ell$ è intero su $A \implies d_1 \cdots d_n \ell \in \tilde{B}$

$\ell = \frac{d_1 \cdots d_n \ell}{d_1 \cdots d_n} \in \mathrm{Frac}\tilde{B}$, perché $d_1 \cdots d_n \ell \in \tilde{B}$, $d_1 \cdots d_n \in A \subseteq \tilde{B}$

Per lying over, $\exists \tilde{q}_1 \in \mathrm{Spec}\,\tilde{B}$ t.c. $\tilde{q}_1 \cap B = q_1$.

Per going up in $A \subseteq \tilde{B}$ trovo $q_1' \neq q_2'$ primi di $\tilde{B}$ t.c. $q_1' \cap A = p_1$, $q_2' \cap A = p_2$.

Ora $\tilde{q}_1 \cap A = (\tilde{q}_1 \cap B) \cap A = q_1 \cap A = p_1$

Quindi $\tilde{q}_1$ e q_1' sono due ideali primi di $\tilde{B}$ che stanno sopra p_1.

Per il lemma, $\exists \sigma \in \mathrm{Gal}(\tilde{L}/K)$ t.c. $\sigma(q_1') = \tilde{q}_1$.

Allora $\sigma(q_2') \neq \sigma(q_1') = \tilde{q}_1$. Poniamo $q_2 := \sigma(q_2) \cap B \neq \sigma(q_1') \cap B = \tilde{q}_1 \cap B = q_1$

e vale $q_2 \cap A = q_2' \cap A = p_2$. □

Oss K campo, A K-algebra fin. gen.

$K[x_1,\dots,x_n] \subseteq_{\text{finita}} A \implies \dim A = \dim K[x_1,\dots,x_n] = n$ è finita

In particolare, non ci sono catene discendenti infinite di ideali primi.

esempio $K[x] \subseteq \frac{K[x,y]}{(y^2-(x+1))} = A$

Def Sia L/K un'estensione di campi.
Un sottoinsieme di L $\{x_i\}_{i\in I}$ di elementi algebricamente indipendenti e massimale per inclusione è detto base di trascendenza di L/K.

Proprietà
(i) $L/K(x_i)_{i\in I}$ è est. algebrica
(ii) una base di trascendenza esiste sempre
(iii) due qualsiasi basi di trascendenza hanno la stessa cardinalità

Il grado di trascendenza di L/K, $\operatorname{tr.deg}_K(L)$, è la cardinalità di una qualsiasi base di trascendenza.

Oss
- $L/F/K \implies \operatorname{tr.deg}_K(L) = \operatorname{tr.deg}_K(F) + \operatorname{tr.deg}_F(L)$
- $K(x_1,\dots,x_n) = \operatorname{Frac} K[x_1,\dots,x_n]$ ha $\operatorname{tr.deg}_K(L) = n$.

Teorema K campo, A K-algebra fin. gen. che sia un dominio.
(i) $\dim A = \operatorname{tr.deg}_K \operatorname{Frac} A$
(ii) Ogni catena $0 \subsetneq P_1 \subsetneq P_2 \subsetneq \dots \subsetneq P_r$ massimale ha lunghezza $\dim A$
(iii) $\forall P \in \operatorname{Spec} A \quad \operatorname{ht}(P) + \dim A/P = \dim A$
(iv) $\forall P \subseteq Q$ ogni catena massimale $P \subsetneq P_1 \subsetneq \dots \subsetneq P_r = Q$ ha lunghezza $\operatorname{ht}(Q) - \operatorname{ht}(P)$

Def Un anello che soddisfa (iv) si dice catenario

DIMOSTRAZIONE
Fissiamo $A \supseteq_{\text{finita}} K[x_1,\dots,x_n]$, $n = \dim A$
(i) $\operatorname{Frac} A \supseteq K(x_1,\dots,x_n) \implies \operatorname{tr.deg}_K \operatorname{Frac} A = \operatorname{tr.deg}_K K(x_1,\dots,x_n) = n = \dim A$
(ii) Per induzione su n.
- $n=0$: A è un campo
- $n \geq 1$: $0 \subsetneq P_1 \subsetneq \dots \subsetneq P_r$ catena massimale in A
  $0 \subsetneq Q_1 \subsetneq \dots \subsetneq Q_r$ interseco con $K[x_1,\dots,x_n]$

Affermo che Q_1 è minimale tra i primi non nulli:
se avessi $0 \subsetneq Q_0 \subsetneq Q_1$, troverei

$$\begin{array}{ccccc} A & & 0 \subsetneq P_0 & \subsetneq & P_1 \\ | & & | & & | \\ K[x_1,\dots,x_n] & & Q_0 & \subsetneq & Q_1 \end{array}$$

per going down

$K[x_1,\dots,x_n]$ UFD $\Rightarrow$ int. chiuso

e questo contraddice la massimalità della catena

In particolare, $ht(Q_1)=1 \Rightarrow Q_1=(f)$ perché $K[x_1,\dots,x_n]$ è UFD.

$A/P_1 \cong K[x_1,\dots,x_n]/Q_1$ è ancora intera

quindi $\dim A/P_1 = \dim K[x_1,\dots,x_n]/Q_1$

Inoltre $\dim K[x_1,\dots,x_n]/(f) \underset{\text{a meno di iso}}{=} \dim K[x_1,\dots,x_n]/(g)$ con g monico in x_n

quindi è estensione intera di $K[x_1,\dots,x_{n-1}] \Rightarrow$ ha dim $n-1$

$\Rightarrow \dim A/P_1 = n-1$ e A/P_1 è una K-alg. fin.gen. e dominio

$\Rightarrow$ per hp. ind., tutte le sue catene massimali hanno lungh. $n-1$

$P_1/P_1 \subsetneq P_2/P_1 \subsetneq \dots \subsetneq P_r/P_1$ è massimale (per corrispondenza)

$\Rightarrow r-1=n-1 \Rightarrow r=n$

(iii) $ht(P)$ · max. lungh. di una catena $(0)\subsetneq P_1 \subsetneq \dots \subsetneq P_n = P$

$\dim A/P$: max. lungh. di una catena $P=Q_0 \subsetneq Q_1 \subsetneq \dots \subsetneq Q_s$

La catena $0 \subsetneq P_1 \subsetneq \dots \subsetneq P \subsetneq Q_1 \subsetneq \dots \subsetneq Q_s$ ha quindi lungh. $n=r+s$

(iv) $\underbrace{(0)\subsetneq \dots \subsetneq P}_{\text{catena massimale di lungh. } ht(P)} = P_0 \subsetneq P_1 \subsetneq \dots \subsetneq P_n = Q \subsetneq \dots \subsetneq Q_{m+s}$

catena massimale in A/Q: lungh $= \dim A/Q = \dim A - ht(Q)$

$\Rightarrow ht(P) + \text{lungh}(P \to Q) + \dim A - ht(Q) = \dim A$

$\Rightarrow \text{lungh}(P \to Q) = ht(Q) - ht(P)$ □

Oss $\dim A = ht(P) + \dim A/P$

(i) $ht(P) = \dim A - \dim A/P = \text{codim } V(P)$

$\text{Spec}(A/P)$ = chiuso di $\text{Spec}A$ dato dai p.ti che soddisfano le eq. in P $= V(P)$

(ii) è sempre vero che $\dim A \geq ht(P) + \dim(A/P)$ · concatenando

$(0)\subsetneq P_1 \subsetneq \dots \subsetneq P_r = P$ e $P = Q_0 \subsetneq Q_1 \subsetneq \dots \subsetneq Q_s$ trovo una catena in A

di lungh $\leq \dim A$

esempio $R = DVR$ con uniformizzante π (ad es. $R = \mathbb{Z}_{(p)}$)

$A = R[t]$, $P = (1-\pi t)$

$\dim A \geq 2$: c'è la catena $(0) \subsetneq (t) \subsetneq (t, \pi)$

$\dim A/P = \dim R\left[\frac{1}{\pi}\right] = \dim \text{Frac}R = 0$

$ht(P) \leq 1$: $\dim A_P \leq \dim A\left[\frac{1}{\pi}\right] = \dim \text{Frac}R[t] = 1$

A_P è una localizzazione di $A\left[\frac{1}{\pi}\right]$

(In effetti, $ht(P)=1$: $(0)\subsetneq P$

$\dim A/P + htP < \dim A$

(iii) Se A non è dominio, non è detto che tutte le catene massimali abbiano la stessa lunghezza

$\text{Spec}\left(A = \frac{\mathbb{C}[x,y,z]}{(xz, yz)}\right)$ $\quad (z) \subsetneq (z,x) \subsetneq (z,x,y)$

$(x,y) \subsetneq (x,y,z)$

Teorema: Hauptidealsatz — Sia A un anello Noetheriano, $f \in A$, P un primo minimale tra quelli che contengono (f). Allora $ht(P) \leq 1$.

Oss è falso se manca l'ipotesi A Noetheriano.

Interpretazione geometrica

Se A è una k-alg. fin.gen. che è un dominio e $f \in A \setminus \{0\}$,

$V(f)$ = luogo di zeri di f $\longleftrightarrow$ $\operatorname{Spec} A/(f)$

primi minimali su (f) $\longleftrightarrow$ componenti irriducibili di $\operatorname{Spec} A/(f)$

$\dim V(P) = \dim A/P = \dim A - ht(P) \geq \dim A - 1$.

Imporre un'eq.ne fa calare la dimensione al più di 1

Corollario di Krull — A Noeth, $f \in A$, f non divisore di 0, P un primo minimale sopra $f \Rightarrow ht(P) = 1$.

esempio $A = \frac{\mathbb{C}[x,y,z]}{(xz, yz)}$, $f = \bar{z}$, $P = (\bar{z})$ è primo ma $ht(P) = 0$.
(non calla la dimensione ma il n° di componenti irriducibili)

Teorema dell'altezza — A anello Noetheriano, $f_1, \dots, f_r \in A$, P primo minimale sopra $(f_1, \dots, f_r)$. Allora $ht(P) \leq r$.

Lemma — A anello, $Q \in \operatorname{Spec} A$. Per $n \geq 1$ poniamo
$Q^{(n)}$ = contrazione in A dell'ideale $(QA_Q)^n$
è detto n-esima potenza simbolica di Q.

(i) $Q^{(n)} = \{a \in A \mid \frac{a}{1} = \frac{q_n}{s}$ con $q_n \in Q^n$, $s \notin Q\} =$
$= \{a \in A \mid \exists q_n \in Q^n, \exists s, s' \notin Q$ t.c. $s'(sa - q_n) = 0\} =$
$= \{a \in A \mid \exists q_n \in Q^n, \exists s'' \notin Q$ t.c. $s''a = q_n\}$

(ii) $Q^{(n)} A_Q = (QA_Q)^n$

Lemma — (A, P) Noetheriano locale. Sono equivalenti:
$\dim A = 0 \iff A$ Artiniano $\iff P$ nilpotente

DIMOSTRAZIONE

($\Longrightarrow$) $P \supseteq P^2 \supseteq \dots$ stabilizza $\Rightarrow \exists n$ t.c. $P^n = P^{n+1}$
Per Nakayama, $P^n = 0$.

($\Longleftarrow$) Basta mostrare che non ci sono catene di lungh. 1
Per ass: $Q \neq P$. In A/Q ho P/Q che è nilpotente in un dominio
$\Rightarrow P/Q = 0 \Rightarrow P = Q$ ↯

□

DIMOSTRAZIONE

Sia $\mathfrak{p} \in A$, P minimale sopra $(\mathfrak{p})$

Localizzando in P, posso supporre P massimale

Per assurdo, sia $ht(P) \geq 2$: ho una catena

$$P_0 \subsetneq Q \subsetneq P \implies \mathfrak{p} \notin Q, P_0$$

Quozientando per P_0, siamo nel dominio A/P_0:

P/P_0 è minimale sopra $(\bar{\mathfrak{p}})$.

Basta lavorare in un dominio e mostrare che se P è minimale sopra $\mathfrak{p}$, non esiste un primo Q strett. compreso tra (0) e P.

Consideriamo la catena discendente $(Q^{(n)}, \mathfrak{p}) \supseteq (Q^{(n)}, \mathfrak{p}) \supseteq \dots$, che posso vedere in $A/(\mathfrak{p})$

Oss $A/(\mathfrak{p})$ è Artiniano: $P/(\mathfrak{p})$ è minimale e massimale $\implies$ è di dim 0.

Siccome $A/(\mathfrak{p})$ è Artiniano, la catena stabilizza:

$\exists n$ t.c. $(Q^{(n)}, \mathfrak{p}) = (Q^{(n+1)}, \mathfrak{p})$ (interessante: $=$)

Preso $x \in Q^{(n)} \subseteq (Q^{(n)}, \mathfrak{p})$: $\exists q_{n+1} \in Q^{(n)}$, $\exists a \in A$ t.c. $x = q_{n+1} + a\mathfrak{p}$

Affermo che $a \in Q^{(n)}$: $Q^{(n)} \ni x - q_{n+1} = a\mathfrak{p}$

In particolare, $\exists s \notin Q$ t.c. $s(x - q_{n+1}) = \underbrace{(s\cdot\mathfrak{p})}_{\in Q^{(n)}}\, a$ prodotto di due el. $\notin Q$: non sta in Q

Per il lemma, $a \in Q^{(n)}$

$$\implies x \in Q^{(n+1)} + Q^{(n)} \cdot \mathfrak{p} \subseteq Q^{(n+1)} + PQ^{(n)}$$

$$\implies Q^{(n)} \subseteq Q^{(n+1)} + PQ^{(n)}$$

$$\frac{Q^{(n)}}{Q^{(n+1)}} \subseteq P\frac{Q^{(n)}}{Q^{(n+1)}} \overset{\text{Nak}}{\implies} Q^{(n)} = Q^{(n+1)}$$

Ricordando alla localizzazione, $(QA_Q)^n = (QA_Q)^{n+1}$

$$\overset{\text{Nak}}{\implies} (QA_Q)^n = 0 \qquad \begin{array}{ccc} A & \hookrightarrow & A_Q \\ Q & \hookrightarrow & QA_Q \end{array} \qquad Q^n \hookrightarrow (QA_Q)^n = 0$$

Allora $Q^n = 0 \underset{A \text{ dominio}}{\implies} Q = 0$ ↯ □

Lemma A anello Noetheriano, P un primo di altezza 0.
Ogni elemento di P è un divisore di 0.

DIMOSTRAZIONE

A_P è un anello Noetheriano di dimensione 0, quindi è Artiniano.

Per il lemma, $(PA_P)^n = 0$ per qualche $n \geq 1$

Sia $\mathfrak{p} \in P \setminus \{0\}$: $\frac{\mathfrak{p}^n}{1} = 0$ in A_P, cioè $\exists s \notin P$ t.c. $s\mathfrak{p}^n = 0$.

Se $s\mathfrak{p}^{n-1} \neq 0$, $(s\mathfrak{p}^{n-1})\mathfrak{p} = 0 \implies \mathfrak{p}$ è div. di 0.

Se $s\mathfrak{p}^{n-1} = 0$, $n \geq 2$ e $(s\mathfrak{p}^{n-2})\mathfrak{p} = 0$

Itero finché trovo $s\mathfrak{p}^k \neq 0$ e $(s\mathfrak{p}^k)\mathfrak{p} = 0$ □

DIMOSTRAZIONE Cor(Krull)

$ht(P) \leq 1$ per l'Hauptidealsatz.

Se $ht(P) = 0$, tutti gli el. di P sono divisori di 0

ma $\mathfrak{p} \in P$ e non è divisore di 0 ↯ □

ES A dominio Noetheriano (A non un campo) è UFD
se e solo se ogni primo di altezza 1 è principale.

DIMOSTRAZIONE

($\Rightarrow$) fatta

($\Leftarrow$) Le catene di divisibilità stabilizzano

Sia p irriducibile, Q primo minimale sopra (p).

$ht(Q)=1$ per il Corollario di Krull $\Rightarrow Q=(q)$ per ipotesi

$(p)\subseteq(q)$ $\therefore \exists a\in A$ t.c. $p=aq$, ma p è irriducibile.

Quindi uno fra a e q è un'unità:

se $q\in A^\times$, $Q=(1)$ ↯

se $a\in A^\times$, $(p)=(q)=Q$, cioè p genera un ideale primo $\Rightarrow p$ primo $\square$

un po' di teoria dei numeri

ES A dominio Noetheriano, $\dim A=1$, $x\in A\setminus\{0\}$.
Esistono finiti primi che contengono x.

SOL Equivalente: $\operatorname{Spec} A/(x)$ ha finiti primi

$\dim A/(x)=0$ perché le uniche catene in A sono $(0)\subsetneq P$ e $(x)\not\subseteq(0)$.

$\Rightarrow A/(x)$ Artiniano $\Rightarrow A/(x)\simeq$ prodotto finito di anelli Artiniani locali

$\Rightarrow$ finiti ideali primi

ES A dominio integralmente chiuso, $S\subseteq A$ parte moltiplicativa $\Rightarrow S^{-1}A$ è integralmente chiuso

SOL $\left(\frac{p}{q}\right)^n+\frac{a_1}{s_1}\left(\frac{p}{q}\right)^{n-1}+\dots+\frac{a_n}{s_n}=0 \qquad a_i\in A, s_i\in S$

Moltiplico per $(s_1\cdots s_n)^n$:

$$\left(\frac{s_1\cdots s_n p}{q}\right)^n+a_1s_2\cdots s_n\left(\frac{s_1\cdots s_n p}{q}\right)^{n-1}+\pm+(s_1\cdots s_{n-1})^n s_n^{n-1}a_n=0$$

A int. chiuso $\Rightarrow \frac{s_1\cdots s_n p}{q}\in A \Rightarrow \frac{p}{q}\in S^{-1}A$

ES A anello, I_1, I_2 ideali se $\forall P$ primo (risp. $\forall M$ massimale)
$I_1A_P=I_2A_P$, allora $I_1=I_2$

def Un dominio di Dedekind è un dominio Noetheriano
di dim 1 integralmente chiuso.

Teorema A dominio di Dedekind, $I \neq (0)$ ideale.
Allora esistono unici $P_1, \dots, P_r$ ideali primi e $e_1, \dots, e_r \geq 1$ t.c.
$$I = P_1^{e_1} \cdot \dots \cdot P_r^{e_r}$$

DIMOSTRAZIONE
$I \ni x \neq 0 \Rightarrow x$ è contenuto in un n° finito di ideali primi $P_1, \dots, P_s$
$\Rightarrow I$ è contenuto in un n° finito di primi $P_1, \dots, P_r$
Per ogni P_i, A_{P_i} è un DVR (dominio Noeth. locale int. chiuso di dim 1)
$IA_{P_i} = (P_i A_{P_i})^{e_i}$ (in un DVR ogni ideale è potenza del massimale).
Mostriamo $I \overset{?}{=} \prod_{i=1}^{r} P_i^{e_i} =: J$
Nelle localizzazioni:
- $IA_{P_i} = (P_i A_{P_i})^{e_i}$, $JA_{P_i} = (P_i A_{P_i})^{e_i}$ perché $P_j A_{P_i} = (1)$
- per $P \notin \{P_1, \dots, P_r\}$, $IA_P = (1)$ e $JA_P = (1)$

Unicità: $I = P_1^{e_1} \cdots P_r^{e_r} = P_1^{f_1} \cdots P_r^{f_r}$ (ammettendo esponenti nulli)
$IA_{P_i} = (P_i A_{P_i})^{e_i} = (P_i A_{P_i})^{f_i} \Rightarrow e_i = f_i$ □

Def $P \in \mathrm{Spec}(A)$, $x \in A \setminus \{0\}$. $(x)A_P = (PA_P)^e$
$v_P(x) := e$ valutazione P-adica
Dato $\frac{a}{s} \in \mathrm{Frac}(A)$, $v_P\left(\frac{a}{s}\right) = v_P(a) - v_P(s)$

Traccia e norma in un'est. di campi

$L \ni \alpha$ — finita — $K(\alpha)$ — finita — K

$$\mathrm{tr}_{L|K}(\alpha) := \mathrm{tr}_K(\cdot\alpha : L \to L)$$
$$N_{L|K}(\alpha) := \det_K(\cdot\alpha : L \to L)$$

Consideriamo $\cdot\alpha : L \to L$ è K-lineare

$K(\alpha) = K[X]/(\mu_\alpha(X))$ con $\mu_\alpha(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0$ pol. minimo
$L = K(\alpha) \cdot v_1 \oplus \dots \oplus K(\alpha) v_m$ dove $m = [L : K(\alpha)]$, $n = [K(\alpha) : K]$
Scriviamo $\cdot\alpha : K(\alpha) \to K(\alpha)$
$\alpha^n = -a_{n-1}\alpha^{n-1} - \dots - a_0$

$$\begin{pmatrix} 0 & 0 & & -a_0 \\ 1 & 0 & & -a_1 \\ 0 & 1 & \ddots & \vdots \\ \vdots & & & \\ 0 & 0 & \cdots & 1-a_{n-1} \end{pmatrix} = M_\alpha \quad \text{matrice compagna}$$

$\mathrm{tr}_{K(\alpha)|K}(\alpha) = -a_{n-1}$ $\quad N_{K(\alpha)|K}(\alpha) = (-1)^n a_0$
Scriviamo $\cdot\alpha : L \to L$

$$\begin{pmatrix} M_\alpha & & & \\ & M_\alpha & & \\ & & \ddots & \\ & & & M_\alpha \end{pmatrix}$$

$\mathrm{tr}_{L|K}(\alpha) = -m \cdot a_{n-1}$ $\quad N_{L|K}(\alpha) = ((-1)^n a_0)^m$

$\mu_\alpha(X) = (X-\alpha)(X-\alpha_2)\cdots(X-\alpha_n) = X^n - (\alpha + \alpha_2 + \dots + \alpha_n)X^{n-1} + \dots + (-1)^n \alpha\alpha_2 \dots \alpha_n$
$\mathrm{tr}_{K(\alpha)|K}(\alpha)$ = somma radici pol. min.
$N_{K(\alpha)|K}(\alpha)$ = prod. radici pol. min.
Se $L|K$ è di Galois con gruppo G
$\mathrm{tr}_{L|K}(\alpha) = \sum_{g \in G} g(\alpha)$, $N_{L|K}(\alpha) = \prod_{g \in G} g(\alpha)$
Chiamiamo $H = \mathrm{Gal}(L|K(\alpha))$, $\#H = n$.
allora $\sum_{g \in G} g(\alpha) = \sum_{g' \text{ rappr. di } G/H} \sum_{h \in H} (g'h)(\alpha) = n \sum_{g'} g'(\alpha) = n$ (somma radici pol. min)
$= \mathrm{tr}_{L|K}(\alpha)$

proposizione $K/\mathbb{Q}$ est. finita, $\mathcal{O}_K$ chiusura intera di $\mathbb{Z}$ in K.
Allora $\mathcal{O}_K$ è Noetheriano; in effetti, $\mathcal{O}_K$ è uno $\mathbb{Z}$-modulo libero di rango finito.

DIMOSTRAZIONE

- Sostituendo K con la sua chiusura di Galois $\tilde{K}$, posso supporre $K=\tilde{K}$ $(\mathcal{O}_K \subseteq \mathcal{O}_{\tilde{K}} \simeq \mathbb{Z}^n \Rightarrow \mathcal{O}_K \simeq \mathbb{Z}^s)$
- $K=\mathbb{Q}(\alpha)$ per il Teo. dell'elemento primitivo
- α soddisfa $\alpha^n + b_1\alpha^{n-1} + \dots + b_n = 0$ con $b_i \in \mathbb{Q}$
  Se $b_i = a_i/s_i$ con $a_i, s_i \in \mathbb{Z}$, $s_1 \cdots s_n \alpha$ è intero su $\mathbb{Z}$
- $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$ $\qquad \mathbb{Z}^n \subseteq \mathcal{O}_K$
  $\frac{\mathbb{Z}[x]}{(\mu_\alpha(x))} \cong \mathbb{Z}[\alpha]$
- (Truccone) $tr : K \times K \longrightarrow \mathbb{Q}$
  $(x,y) \longmapsto tr_{K/\mathbb{Q}}(xy) = \sum_{g \in Gal(K/\mathbb{Q})} g(xy)$
  è una forma $\mathbb{Q}$-bilineare simmetrica
  è non degenere
  Scriviamo la matrice in base $\{1, \alpha, \dots, \alpha^{n-1}\}$
  $[tr]_{ij} = tr(\alpha^i\alpha^j) = \sum_{g \in G} g(\alpha^i\alpha^j) = \sum_{g \in G} g(\alpha)^i g(\alpha)^j$
  $\#G = [L:K] = n$, li chiamo $g_0, \dots, g_{n-1}$ e pongo $\alpha_k = g_k(\alpha)$
  $[tr]_{ij} = \sum_{k=0}^{n-1} g_k(\alpha)^i g_k(\alpha)^j = \sum_{k=0}^{n-1} M_{ik}\,{}^tM_{kj}$ dove $M_{ik} = \alpha_k^i$
  $= (M \cdot {}^tM)_{ij}$

$$M = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_0 & \alpha_1 & \cdots & \alpha_{n-1} \\ \alpha_0^2 & \alpha_1^2 & \cdots & \alpha_{n-1}^2 \\ \vdots & & & \\ \alpha_0^{n-1} & \alpha_1^{n-1} & \cdots & \alpha_{n-1}^{n-1} \end{pmatrix}$$

  $\det[tr] = (\det M)^2 = \prod_{i<j}(\alpha_j - \alpha_i)^2 \neq 0$
  Quindi tr è non degenere
  $\Rightarrow \exists\, \beta_0, \dots, \beta_{n-1}$ base di K come $\mathbb{Q}$-sp. vett. t.c. $tr(\alpha^i\beta_j) = \delta_{ij}$
  Esiste $N \in \mathbb{Z}\setminus\{0\}$ t.c. $N\beta_0, \dots, N\beta_{n-1} \in \mathcal{O}_K$
  Claim: $\mathcal{O}_K \subseteq \frac{1}{N}\mathbb{Z}[\alpha] \simeq \mathbb{Z}^n$
  Dato $\beta \in \mathcal{O}_K$, lo scrivo $\beta = \beta_0 + \beta_1\alpha + \beta_2\alpha^2 + \dots + \beta_{n-1}\alpha^{n-1}$
  e calcolo $N\,tr(\beta\beta_j) = \sum_{i=0}^{n-1} tr(N\beta_i\alpha^i\beta_j) = \sum_{i=0}^{n-1} \beta_i\, tr(\alpha^i N\beta_j) = N\beta_j$
  $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$
  $\Rightarrow \beta_j \in \frac{1}{N}\mathbb{Z}$ □

Oss $\mathcal{O}_K \simeq \mathbb{Z}^{[K:\mathbb{Q}]}$ sempre

Oss $tr(\mathcal{O}_K) \subseteq \mathbb{Z}$
$x \in \mathcal{O}_K$, $tr_{K/\mathbb{Q}}(x) = \sum_{g \in G} g(x) \in \mathcal{O}_K \cap \mathbb{Q}$
$\mathcal{O}_K \cap \mathbb{Q} = \{\text{sott. di } \mathbb{Q} \text{ interi su } \mathbb{Z}\} = \mathbb{Z}$

ES $A=\mathbb{C}[a_1,a_2,a_3,b_1,b_2,b_3]$

$M=\begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{pmatrix}$ $\quad I=(a_1b_2-a_2b_1,\ a_1b_3-a_3b_1)$

Studiamo i primi minimali sopra I

$V(I)\ni(a_1-\tilde a_1,\dots,b_3-\tilde b_3)$ t.c. $\tilde a_1\tilde b_2-\tilde a_2\tilde b_1=0,\ \tilde a_1\tilde b_3-\tilde a_3\tilde b_1=0$

(1) Trovare i primi minimali sopra I e calcolarne l'altezza

$P_1=(a_1,b_1)$ $\quad P_2=(a_1b_2-a_2b_1,\ a_1b_3-a_3b_1,\ a_2b_3-a_3b_2)$

$P\supseteq I\ni a_3(a_1b_2-a_2b_1)-a_2(a_1b_3-a_3b_1)=a_1(a_3b_2-a_2b_3)$

$a_1\in P$ o $a_3b_2-a_2b_3\in P$

$P_2\subseteq P$

Ammettendo che P_2 primo, P minimale $\Longrightarrow P=P_2$.

$(a_1,a_2b_1,a_3b_1)\subseteq P$

$(a_1,b_1)\subseteq P$ $\quad (a_1,a_2,a_3)\subseteq P$ non è minimale perché contiene P_2

oppure per il Teo. dell'altezza

$ht(a_1,a_2,a_3)=3=\dim A-\dim A/(a_1,a_2,a_3)$

$ht(P_1)=2$ $\quad ht(P_2)=2$

$ht(P_2)=\dim A-\dim A/P_2 \Longrightarrow \dim A/P_2=4$

$\dim(A/P_2)=\operatorname{tr\,deg}_{\mathbb{C}}\operatorname{Frac}(A/P_2)$

classi in A/P_2

$a_1b_2-a_2b_1=0 \rightsquigarrow \overline{b}_2=\overline{a}_2/\overline{a}_1\overline{b}_1$

$a_1b_3-a_3b_1=0 \rightsquigarrow \overline{b}_3=\overline{a}_3/\overline{a}_1\overline{b}_1$

$a_2b_3-a_3b_2=0 \rightsquigarrow \overline{a}_2\overline{a}_3/\overline{a}_1\overline{b}_1-\overline{a}_3\overline{a}_2/\overline{a}_1\overline{b}_1=0$

Dimostriamo che P_2 non si genera con 2 generatori

$\mathfrak{m}=(a_1,a_2,a_3,b_1,b_2,b_3)$ $\quad A/\mathfrak{m}\times P_2/P_2\cap\mathfrak{m}^3\longrightarrow P_2/P_2\cap\mathfrak{m}^3$

$\mathbb{C}\cong A/\mathfrak{m}$

Se P_2 si generasse con 2 polinomi, il $\mathbb{C}$-sp. vett. $P_2/P_2\cap\mathfrak{m}^3$ avrebbe dim ≤ 3, ma i 3 generatori che abbiamo sono lin. indip.

$\lambda_1(a_1b_2-a_2b_1)+\lambda_2(a_1b_3-a_3b_1)+\lambda_3(a_2b_3-a_3b_2)=0 \Longrightarrow \lambda_1=\lambda_2=\lambda_3=0$

Il fatto che ci siano 2 primi minimali sopra I dice che I non è primo.

(P_2 primo: $\mathbb{A}^2\times\mathbb{A}^3\longrightarrow V(P_2)$

$\left(\begin{pmatrix}y\\z\end{pmatrix},\begin{pmatrix}x\\y\\z\end{pmatrix}\right)\longmapsto\begin{pmatrix}ux & uy & uz\\ vx & vy & vz\end{pmatrix}$

$\mathbb{A}^5$ irr. $\Longrightarrow V(P_2)$ irr. $\Longrightarrow P_2$ primo)

ES A dominio in cui ogni ideale primo è principale.
Allora A è PID

ES $A=\mathbb{R}[x,y]/(x^2+y^2+1)$ è PID (ma non Euclideo)

SOL $\dim A = 1$. A è est. intera di $\mathbb{R}[x]$
è dominio, perché x^2+y^2+1 è irr
I primi $\neq(0)$ sono massimali
Sia $P\neq(0)$ primo. A/P è • un campo
• $\mathbb{R}$-algebra fin.gen.
$\Rightarrow A/P$ è est. finita di $\mathbb{R}$
$\Rightarrow A/P \simeq \mathbb{R}$ o $\mathbb{C}$
$1, \bar{x}, \bar{y}$ sono lin.dip in $A/P \Rightarrow \exists a,b,c\in\mathbb{R}$ t.c. $(b,c)\neq(0,0)$
$a\cdot 1 + b\bar{x} + c\bar{y} = 0$ in $A/P \Rightarrow a+bx+cy \in P$

- $\frac{\mathbb{R}[x,y]}{(x^2+y^2+1,\, a+bx+cy)} \underset{0\neq g}{\simeq} \frac{\mathbb{R}[x,y]}{(bg+x,\ cg-(1+x^2+y^2))} \simeq \frac{\mathbb{R}[x,y]/(bg+x)}{((1+b^2+c^2)g^2-1)} \simeq \frac{\mathbb{R}[y]}{(\dots)} \simeq \mathbb{C}$

Quindi $(a+bx+cy)=P$

Teorema dell'altezza A anello Noetheriano, $I=(f_1,\dots,f_n)$, P primo minimale sopra I. Allora $ht(P)\leq n$.

Lemma (A,P) anello Noetheriano locale, $x_1,\dots,x_n\in P$.
P è minimale sopra $(x_1,\dots,x_n) \iff \exists N\geq 1$ t.c. $P^N\subseteq(x_1,\dots,x_n)$

DIMOSTRAZIONE
Se P è minimale, $P/(x_1,\dots,x_n)$ in $A/(x_1,\dots,x_n)$ è sia massimale sia minimale
Quindi $\dim A/(x_1,\dots,x_n)=0 \Rightarrow$ è Artiniano locale
$\Rightarrow P/(x_1,\dots,x_n)$ è nilpotente, quindi $\exists N\geq 1$ t.c. $(P/(x_1,\dots,x_n))^N=0$
cioè $P^N\subseteq(x_1,\dots,x_n)$
Viceversa, se $P^N\subseteq(x_1,\dots,x_n)$, allora $P/(x_1,\dots,x_n)$ è nilpotente
$\Rightarrow$ in $A/(x_1,\dots,x_n)$ l'id. max. è nilpotente: allora
$P/(x_1,\dots,x_n)$ è minimale sopra (0), e tornando in A segue la tesi □

DIMOSTRAZIONE
Per induzione su n
- $n=0$: ovvio
- $n=1$: Hauptidealsatz
- $n\geq 2$: sostituiamo A con A_P. Prendiamo un primo $P'\subsetneq P$.
Basta mostrare che $ht(P')\leq n-1$.
Posso assumere che non esistano ideali primi Q t.c. $P'\subsetneq Q\subsetneq P$:
se ci fosse un tale Q, sostituisco P' con Q e ripeto; il processo termina per Noetherianità.
Per minimalità di P, c'è almeno un x_i (wlog x_n) t.c. $x_i\notin P'$
Dico che $\dim A/(P',x_n)=0$: prendiamo un primo in questo quoziente
Corrisponde a un primo di A, Q t.c. $(P',x_n)\subseteq Q\subseteq P \Rightarrow Q=P$
o $Q=P'$ ma questo non può essere perché $x_n\in Q$
$\Rightarrow$ l'unica catena di primi ha lunghezza zero.
$\Rightarrow P/(P',x_n)$ è nilpotente
$\forall i=1,\dots,n-1 \quad x_i^{N_i}\in(P',x_n)\cdot x_i^{N_i}=y_i+a_i x_n$ con $y_i\in P', a_i\in A$
Mostriamo che P' è minimale sopra $y_1,\dots,y_{n-1}$
- $P/(y_1,\dots,y_{n-1},x_n)$ è nilpotente in $A/(y_1,\dots,y_{n-1},x_n)$:
$P^M\subseteq(x_1,\dots,x_n)$, $\exists N_n$ t.c. $(x_1,\dots,x_n)^{N_n}\subseteq(y_1,\dots,y_{n-1},x_n)$
$\Rightarrow P^{MN_n}\subseteq(y_1,\dots,y_{n-1},x_n)$
- $P/(y_1,\dots,y_{n-1})$ è minimale sopra la classe di x_n in $A/(y_1,\dots,y_{n-1})$
$\Rightarrow ht\ P/(y_1,\dots,y_{n-1})\leq 1$
- $P'/(y_1,\dots,y_{n-1})\subsetneq P/(y_1,\dots,y_{n-1})$ perché uno contiene la classe di x_n e l'altro no
$\Rightarrow ht\ P'/(y_1,\dots,y_{n-1})<ht\ P/(y_1,\dots,y_{n-1})\leq 1$, cioè P' è minimale sopra $(y_1,\dots,y_{n-1})$ □

teorema A anello Noetheriano, P ideale primo con $ht(P)=r$.
Allora esistono $x_1,\dots,x_r \in P$ t.c. P è minimale sopra $(x_1,\dots,x_r)$.

DIMOSTRAZIONE

- $r=0$: vero per def.
- $r=1$: voglio $x_1 \in P$ ma x_1 non contenuto in alcun ideale primo di $ht=0$
  Siano $Q_1,\dots,Q_m$ i primi minimali di A (n° finito perché A è Noeth)
  Si ha $P \not\subseteq Q_i$ perché $ht P_i = 1$ e $ht Q = 0 \Rightarrow P \not\subseteq \bigcup_{i=1} Q_i$
  Scelgo $x \in P \setminus \bigcup Q_i$
  Dico che P è minimale sopra (x) : altrimenti
  $$(x) \subseteq Q \subsetneq P \qquad ht(P)=1 \Rightarrow ht(Q)=0 \Rightarrow Q=Q_i \Rightarrow x \in Q_i \ \lightning$$
- Caso $r \geq 2$: per ricorrenza, costruisco $x_1,\dots,x_r$ t.c. $\forall k=1,\dots,r$ ogni ideale primo sopra $(x_1,\dots,x_k)$ ha altezza $\geq k$ (e quindi $=k$)
  Supponiamo di aver costruito $x_1,\dots,x_k$, $k<r$
  C'è un n° finito di primi minimali sopra $(x_1,\dots,x_k)$ (sono i primi minimali di $A/(x_1,\dots,x_k)$) : $Q_1,\dots,Q_m$. $ht(Q_i) \geq k$, $ht(Q_i) \leq k$ per Teo. altezza $\Rightarrow ht(Q_i)=k$
  In particolare, $P \not\subseteq Q_i$ perché $ht P = r > k \Rightarrow P \not\subseteq \bigcup_{i=1} Q_i$
  Prendo $x_{k+1} \in P \setminus \bigcup_{i=1} Q_i$.
  Come prima, ogni primo minimale sopra $(x_1,\dots,x_{k+1})$ ha altezza almeno $k+1$.
  Infine, P è minimale sopra $x_1,\dots,x_r$: sappiamo che ogni primo minimale sopra $(x_1,\dots,x_r)$ ha altezza r. Se P non fosse minimale, avrei $(x_1,\dots,x_r) \subseteq Q \subsetneq P$, assurdo. □

corollario A anello Noetheriano. Vale la DCC per gli ideali primi : ogni catena $P_1 \supseteq P_2 \supseteq \dots$ di ideali primi deve stabilizzare.

DIMOSTRAZIONE

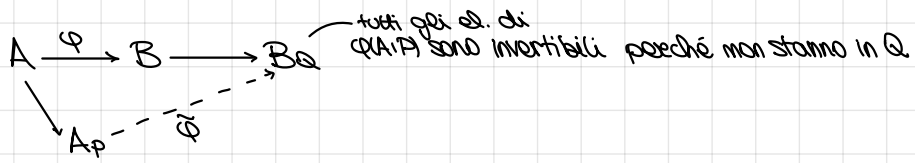
$P_1 = (x_1,\dots,x_r)$ è fin.gen. perché A Noeth., $ht P \leq r$
Se $P_1 \supsetneq P_2 \supsetneq P_3 \supsetneq \dots$, allora $ht P_1 > ht P_2 > ht P_3 > \dots$ $\lightning$ □

corollario (A,P) Noetheriano locale. Allora $\dim A = ht P$ è finita.

Teorema: dimensione della fibra Sia $\varphi: A \to B$ omomorfismo di anelli Noetheriani, $Q \in \operatorname{Spec} B$, $P = \varphi^{-1}(Q)$. Allora $\operatorname{ht} Q \leq \operatorname{ht} P + \dim(B_Q / \varphi(P) B_Q)$

DIMOSTRAZIONE

Possiamo localizzare.



$\operatorname{ht} Q = \dim B_Q$, $\operatorname{ht} P = \dim A_P$

Sostituisco $A \to A_P$, $P \to PA_P$, $B \to B_Q$, $Q \to QB_Q$, $\varphi \to \tilde{\varphi}$

Devo dimostrare che $\dim B \leq \dim A + \dim B/\varphi(P)B$

Scegliamo $a_1, \dots, a_r \in P$ t.c. P è minimale sopra $(a_1, \dots, a_r)$, $r = \dim A$

Scegliamo $\overline{b}_1, \dots, \overline{b}_s \in Q/\varphi(P)B$ t.c. $Q/\varphi(P)B$ è minimale sopra $(\overline{b}_1, \dots, \overline{b}_s)$, $s = \dim B/\varphi(P)B$

$b_1, \dots, b_s \in Q$ che rappresentano $\overline{b}_1, \dots, \overline{b}_s$

Tesi: $\dim B \leq r+s$

$\dim B = \operatorname{ht} Q$: basta mostrare che Q è minimale sopra un ideale con $r+s$ generatori: $I = (\varphi(a_1), \dots, \varphi(a_r), b_1, \dots, b_s)$

Sappiamo che $\exists N$ t.c. $P^N \subseteq (a_1, \dots, a_r) \Rightarrow \varphi(P)^N \subseteq (\varphi(a_1), \dots, \varphi(a_r))$

$\exists M$ t.c. $(Q/\varphi(P)B)^M \subseteq (\overline{b}_1, \dots, \overline{b}_s)$

cioè $Q^M \subseteq (b_1, \dots, b_s) + \varphi(P)B$

$\Rightarrow \exists T$ t.c. $Q^{MT} \subseteq ((b_1, \dots, b_s) + \varphi(P)B)^T \subseteq (b_1, \dots, b_s) + (\varphi(P)B)^N \subseteq (b_1, \dots, b_s) + (\varphi(a_1), \dots, \varphi(a_s))$. □

Interpretazione geometrica

Siano A, B locali, $\varphi: A \to B \rightsquigarrow \varphi^*: \operatorname{Spec} B \to \operatorname{Spec} A$, $Q \mapsto P$

Consideriamo le preimmagini di P

$$(\varphi^*)^{-1}(P) = \{R \in \operatorname{Spec} B \mid \varphi^*(R) = P\} = \{R \in \operatorname{Spec} B \mid \varphi^{-1}(R) = P\} = \{R \in \operatorname{Spec} B \mid \varphi^{-1}(R) \supseteq P\} = \operatorname{Spec} B/\varphi(P)B$$

$\dim B \leq \dim A + \dim (\varphi^*)^{-1}(P)$

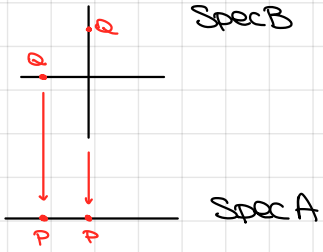
esempio $A = \mathbb{C}[x] \xrightarrow{i} B = \dfrac{\mathbb{C}[x,y]}{(xy)}$ ($(x), (y), (x-x_0, y-y_0)$ con $x_0 y_0 = 0$)

$i^\#: \operatorname{Spec} B \to \operatorname{Spec} A$

$(x-x_0, y-y_0) \mapsto (x-x_0)$

$(x) \mapsto (x)$

$(y) \mapsto (0)$



Teo. fibra: $\operatorname{ht} Q \leq \operatorname{ht} P + \dim B_Q/\varphi(P)B_Q$

- $Q = (x-x_0, y-y_0)$ con $x_0 \neq 0$ $\rightsquigarrow$ $P = (x-x_0)$

  $ht\,Q = 1$

  $ht\,P = 1$

  $$B_{\mathcal{O}(P)B_Q} = \frac{(\mathbb{C}[x,y]/(xy))_{(x-x_0,y)}}{(x-x_0)\,(\mathbb{C}[x,y]/(xy))_{(x-x_0,y)}} \cong \frac{(\mathbb{C}[x,y]/(y))_{(x-x_0,y)}}{(x-x_0)\,(\mathbb{C}[x,y]/(y))_{(x-x_0,y)}} \cong \mathbb{C}$$

  (x è invertito)

- $Q = (x, y-y_0)$ $\rightsquigarrow$ $P = (x)$ con $y_0 \neq 0$

  $ht\,Q = 1$, $ht\,P = 1$

  $$B_{\mathcal{O}(P)B_Q} = \frac{(\mathbb{C}[x,y]/(xy))_{(x,y-y_0)}}{(x)\,(\mathbb{C}[x,y]/(xy))_{(x,y-y_0)}} \cong (\mathbb{C}[y])_{(y-y_0)}$$

- $Q = (x)$ $\rightsquigarrow$ $P = (x)$

  $ht\,Q = 0$, $ht\,P = 1$

  Fibra: $$B_{\mathcal{O}(P)B_Q} = \frac{(\mathbb{C}[x,y]/(xy))_{(x)}}{(x)\,(\mathbb{C}[x,y]/(xy))_{(x)}} \cong \frac{\mathbb{C}[y]_{(0)}}{(0)} = \operatorname{Frac}\mathbb{C}[y]$$

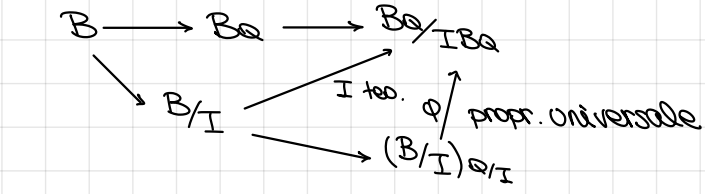
- $Q = (y)$ $\rightsquigarrow$ $P = (0)$

  $ht\,Q = 0$, $ht\,P = 0$

  Fibra: $$B_{\mathcal{O}(P)B_Q} = \frac{(\mathbb{C}[x,y]/(xy))_{(y)}}{(0)} \cong (\mathbb{C}[x,y]/(y))_{(y)} = \operatorname{Frac}\mathbb{C}[x]$$

Lemma B anello, I ideale di B, Q ideale massimale, $I \subseteq Q$.
Allora $(B/I)_{Q/I} \cong B_Q/IB_Q$

DIMOSTRAZIONE



$$\varphi\left(\frac{b}{s}\right) = \frac{\varphi(b)}{\varphi(s)} \mod IB_Q \qquad s \notin Q$$

φ è biiettiva:

- suriettiva: gli el. in B_Q/IB_Q sono classi di $\frac{b}{s}$, $s \notin Q$ e stanno in $\operatorname{Im}\varphi$
- iniettiva: $\varphi(b)/\varphi(s) \in IB_Q$, cioè $\exists i \in I, \exists \frac{c}{t} \in B_Q$ t.c. $\varphi\left(\frac{b}{s}\right) = \frac{c}{t} i$

Teorema A anello Noetheriano. Allora $\dim A[x] = \dim A + 1$.

DIMOSTRAZIONE

($\geq$) Sia $P_0 \subsetneq P_1 \subsetneq \dots \subsetneq P_r$ catena in A

$P_0[x] \subsetneq P_1[x] \subsetneq \dots \subsetneq P_r[x] \subsetneq (P_r, x)$

$\frac{A[x]}{P_i[x]} \simeq (A/P_i)[x]$ dominio ; $\frac{A[x]}{(P_r,x)} \simeq \frac{A[x]/(x)}{(P_r,x)/(x)} \simeq \frac{A}{P_r}$ dominio

($\leq$) Sia Q un primo di $A[x]$

Teo. fibra su $\varphi: A \longrightarrow A[x]$, $P = \varphi^{-1}(Q)$.

$ht\, Q \leq ht\, P + \underbrace{\dim\left(A[x]_Q / \varphi(P) A[x]_Q\right)}_{\text{basta } \leq 1}$

$A[x]_Q / PA[x]_Q \simeq \left(A[x]/PA[x]\right)_{Q/PA[x]} = \left(A/P[x]\right)_{Q/PA[x]}$

Un elemento di A che non sta in P ha una classe in $A[x]/PA[x]$ che non sta in Q

Quindi $\left(A/P[x]\right)_{Q/PA[x]}$ è una localizzazione di $S^{-1}(A/P[x])$ con $S = (A \setminus P)$ mod P

$= (\mathrm{Frac}\, A/P)[x]$

che ha dim. 1 □

Due nozioni di dimensione:

- Krull: $P_0 \subsetneq P_1 \subsetneq \dots \subsetneq P_n$
- (A, P) locale Noetheriano: $ht\, P = \dim A = \min$ n° di generatori di un ideale I t.c. P è min. sopra $I \iff \sqrt{I} = P$

Intuizioni geometriche:

- Krull: $V(P_r) \subsetneq V(P_{r-1}) \subsetneq \dots \subsetneq V(P_0)$
- min n° di generatori:



$P' \in V(I) \iff I \subseteq P'$

$\sqrt{I} = P \iff V(I) = V(P)$ $\quad I = (f_1, \dots, f_r)$

Sto cercando di identificare $\{P\}$ con il minimo n° di equazioni

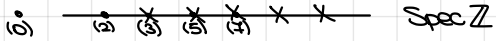
Localizzazioni

A dominio, S generata da una quantità numerabile di elementi $f_1, f_2, f_3, \dots$

$S_j = \{f_1^{e_1} \cdot \dots \cdot f_j^{e_j} \mid e_1, \dots, e_j \geq 0\}$

$\mathrm{Frac}\, A \supseteq S^{-1}A \supseteq \dots \supseteq S_j^{-1}A \supseteq S_{j-1}^{-1}A \supseteq \dots \supseteq S_1^{-1}A \supseteq A$





$\mathrm{Spec}\, \mathbb{Z}_{(2)}$ $\quad 3, 5, 7, 11, \dots$

$\mathrm{Spec}(S^{-1}A) = \mathrm{Spec}(\varinjlim S_j^{-1}A) = \varprojlim S_j^{-1}A$

↳ intersezione

esempio $A = \frac{\mathbb{C}[x,y]}{(y^2 - x(1+x))}$



$A_{(x,y)}$ è un dominio $\Rightarrow \operatorname{Spec} A_{(x,y)}$ è irriducibile
$\overline{\{(0)\}}$

Vorremmo costruire una sorta di "intorno infinitesimo" del punto (0,0) che faccia vedere le due componenti irriducibili che percepiamo nel disegno.

spazio tangente algebrico

def V varietà su $\mathbb{R}$, $P \in V$.
Una derivazione in P è un funzionale lineare
$X : C^\infty(V) \longrightarrow \mathbb{R}$ t.c. $X(fg) = f(P)X(g) + X(f)g(P)$

Oss $X(1) = 0$

proposizione $\operatorname{Der}(\mathbb{R}^n, 0) \xleftrightarrow{\sim} \mathbb{R}^n$

DIMOSTRAZIONE
Dato $v \in \mathbb{R}^n$, considero $X_v : f \longmapsto \sum_{i=1}^n v_i \frac{\partial f}{\partial x_i}(0)$
Viceversa, data $f \in C^\infty(\mathbb{R})$, posso scrivere

$$f = f(0) + \sum_{i=1}^n \frac{\partial f}{\partial x_i}(0) \cdot x_i + \sum_{i,j=1}^n x_i x_j g_{ij}(x) \quad \text{con } g_{ij}(0) = 0 \qquad (*)$$

$$X(P) = X(f(0)) + \sum_{i=1}^n \frac{\partial^2 f}{\partial x_i \partial x_j}(0) X(x_i) + \sum_{i,j=1}^n \left(x_i(0) X(g_{ij}) + X(x_i) g_{ij}(0) \right) =$$

$f(0) \overset{\parallel}{X(1)} = 0$

$$= \sum_{i=1}^n \frac{\partial f}{\partial x_i}(0) \cdot X(x_i) \longrightarrow v = \begin{pmatrix} X(x_1) \\ \vdots \\ X(x_n) \end{pmatrix} \qquad \square$$

Oss Se ripartiamo da $(*)$ e deriviamo in x_i:

$$\frac{\partial f}{\partial x_i}(0) = \frac{\partial f}{\partial x_i}(0) + g_i(0) + \sum_{j=1}^n x_j(0) \frac{\partial g_{ij}}{\partial x_i}(0)$$

Algebrizziamo questa descrizione.

- valutazione: $\mathfrak{m} \subset C^\infty(V)$ con $\mathfrak{m} = \{ f \in C^\infty(V) \mid f(P) = 0 \}$

$$C^\infty / \mathfrak{m} \xrightarrow{\sim} \mathbb{R}$$
$$f(x) \longmapsto f(P) \qquad f(x) = (f(x) - f(P)) + f(P)$$

- $f(x) = f(0) + \underbrace{\sum_{i=1}^n \frac{\partial f}{\partial x_i}(0) \cdot x_i}_{\in \mathfrak{m}} + \underbrace{\sum_{i,j=1}^n x_i g_{ij}(0)}_{\in \mathfrak{m}^2}$

- Cos'è una derivazione? È un'applicazione $\mathbb{R}$-lineare $\mathfrak{m}/\mathfrak{m}^2 \longrightarrow \mathbb{R}$

def A anello, $\mathfrak{m}$ un ideale massimale.
Lo spazio tangente ad A in $\mathfrak{m}$ è

$$\{ \mathfrak{m}/\mathfrak{m}^2 \longrightarrow A/\mathfrak{m} \} = \operatorname{Hom}_{A/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2, A/\mathfrak{m})$$

Oss $dx_1, \dots, dx_n \in \mathfrak{m}/\mathfrak{m}^2$ sono le classi di $x_1, \dots, x_n \in \mathfrak{m}$ nel quoziente $\mathfrak{m}/\mathfrak{m}^2$

Oss
$f = f(P) + \sum_{i=1}^n \frac{\partial f}{\partial x_i}(0) x_i +$ qualcosa in $\mathfrak{m}^2$
$g = g(P) + \sum_{i=1}^n \frac{\partial g}{\partial x_i}(0) x_i +$ qualcosa in $\mathfrak{m}^2$
$fg = f(P)g(P) + \sum_{i=1}^n f(P) \frac{\partial g}{\partial x_i}(0) x_i + \sum_{i=1}^n g(P) \frac{\partial f}{\partial x_i}(0) x_i +$ qualcosa in $\mathfrak{m}^2$
$\Rightarrow X(fg) = f(P)X(g) + X(f)g(P)$

esempio $A=\frac{\mathbb{R}[x,y,z]}{(y^3+x^4+3x-2y+z)}$ $\quad \mathfrak{m}=(x,y,z)$

$\mathrm{Hom}(\mathfrak{m}/\mathfrak{m}^2, A/\mathfrak{m})$ $\qquad \nabla f\begin{pmatrix}0\\0\\0\end{pmatrix}=\begin{pmatrix}3\\-2\\1\end{pmatrix}$ $df\begin{pmatrix}0\\0\\0\end{pmatrix}=(3,-2,1)$

$\mathfrak{m}/\mathfrak{m}^2 = (x,y,z)/(x^2,y^2,z^2,xy,yz,3x-2y+z) \simeq \langle x,y,z\rangle_{\mathbb{R}}/\langle 3x-2y+z\rangle_{\mathbb{R}}$

$\mathrm{Hom}(\mathfrak{m}/\mathfrak{m}^2,\mathbb{R}) = \{\text{appl. lineari } \mathbb{R}^3\to\mathbb{R} \text{ che si annullano in } \begin{pmatrix}3\\-2\\1\end{pmatrix}\} = \langle\begin{pmatrix}3\\-2\\1\end{pmatrix}\rangle^{\perp}$

def Un anello locale Noetheriano $(A,\mathfrak{m})$ si dice regolare se

$\dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = \dim A = \mathrm{ht}\,\mathfrak{m}$

Equivalentemente, $(A,\mathfrak{m})$ regolare $\iff$ $\mathfrak{m}$ generato da $\mathrm{ht}\,\mathfrak{m}$ generatori

- $\dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$ — Nakayama
- $\min$ n° di generatori di $\mathfrak{m}$
- $\mathrm{ht}\,\mathfrak{m}$ — Teo. altezza

def A anello Noetheriano si dice regolare se ogni localizzazione ad un ideale massimale lo è.

Teorema: Auslander-Buchsbaum-Serre $\quad A$ regolare, P primo $\Longrightarrow A_P$ regolare.

Approssimazioni superiori

$\frac{\mathbb{R}[x,y]}{(y^2-x^3(1+x))} \supset \mathfrak{m}=(x,y)$ $\qquad f(x)+yg(x)$

$\mathfrak{m}/\mathfrak{m}^2 = (x,y)/(x^2,xy)$ ha dim. 2 con base $\bar{x},\bar{y}$

$\mathrm{ht}\,\mathfrak{m}=1$

$\mathfrak{m}/\mathfrak{m}^3 = \frac{\{f(x)+yg(x)\mid f(0)=0\}}{(x^3,x^2y,xy^2,y^3)} = \frac{\{f(x)+yg(x)\mid f(0)=0\}}{(x^3,x^2y)}$

$\dim \mathfrak{m}/\mathfrak{m}^3 = 2+2=4$

$\dim \mathfrak{m}/\mathfrak{m}^n = (n-1)+(n-1)=2(n-1)$

Oss Confrontiamo con $\mathbb{C}[x,y] \supset \mathfrak{m}=(x,y)$

$\dim \mathfrak{m}/\mathfrak{m}^n$ = monomi di deg tot ≥ 1 e $\leq n-1$

$= \dim \mathbb{C}\langle x^a y^b \mid 1\leq a+b\leq n-1\rangle = \binom{n+1}{2}-1$

esempio $A=K[x_1,\dots,x_r]$, $\mathfrak{m}=(x_1,\dots,x_r)$

$\mathfrak{m}/\mathfrak{m}^n \longleftrightarrow \{p(x_1,\dots,x_r)\in K[x_1,\dots,x_r] \mid p(0)=0,$ ogni monomio ha deg $\leq n-1\}$

$\dim \mathfrak{m}/\mathfrak{m}^n = \binom{n-1+r}{r}-1 \sim \frac{n^r}{r!}$

Teorema $(A, \mathfrak{m})$ locale Noetheriano.
1) la funzione $n \longmapsto \ell(\mathfrak{m}^n/\mathfrak{m}^{n+1})$ coincide con un polinomio per $n \gg 0$.
2) Questo polinomio è asintotico a $c\,n^d/d!$, $c \in \mathbb{Z}_{>0}$, $d = \operatorname{ht}\mathfrak{m} = \dim A$.

Completamenti

A Noetheriano, $\mathfrak{m}$ ideale
$f \in A \rightsquigarrow \bar{f} \in A/\mathfrak{m}$, $\bar{f} \in A/\mathfrak{m}^2$, $\bar{f} \in A/\mathfrak{m}^3$, ...

Def Il completamento di A in $\mathfrak{m}$ è
$\{(f_i)_{i\in\mathbb{N}} \mid f_i \in A/\mathfrak{m}^i,\ f_i \equiv f_j \bmod \mathfrak{m}^j\ \forall i \geq j\}$

esempio
- $A = K[x_1, \dots, x_n]$, $\mathfrak{m} = (x_1, \dots, x_n)$

  $A/\mathfrak{m}$ $\quad 1$
  $A/\mathfrak{m}^2$ $\quad 1 + x_1 - x_2$
  $A/\mathfrak{m}^3$ $\quad 1 + x_1 - x_2 + x_1^2$
  $\vdots$

  $\hat{A} = K[[x_1, \dots, x_n]]$
- $A = \left(\frac{\mathbb{C}[x,y]}{(y^2 - x^2(1+x))}\right)_{(x,y)}$ $\quad \mathfrak{m} = (x,y)$

  $\hat{A} = \frac{\mathbb{C}[[x,y]]}{(y^2 - x^2(1+x))}$

Oss $\mathbb{C}[[x,y]]$ è locale con id. massimale (x,y)
$\frac{1}{1+g(x,y)} = \sum_{n\geq 0} (-1)^n g(x,y)^n \in \mathbb{C}[[x,y]]$

$\hat{A} = \frac{\mathbb{C}[[x,y]]}{((y - xg(x))(y + xg(x)))}$ $\qquad g(x) = \sqrt{1+x} = \sum_{n\geq 0} \binom{1/2}{n} x^n \in \mathbb{C}[[x,y]]$

Oss $\binom{x}{n} = \frac{x(x-1)(x-2)\cdots(x-n+1)}{n!}$

$\operatorname{Spec}(\hat{A}) \supset V(y - g(x)x)$, $V(y + g(x)x)$

Questi completamenti corrispondono a prendere "intorni infinitesimi" intorno ad $\mathfrak{m}$.

Anelli regolari

def. $(A, \mathfrak{m})$ locale regolare.
Un sistema regolare di parametri è un insieme di generatori $x_1, \dots, x_r$ di $\mathfrak{m}$ con $r = \operatorname{ht} \mathfrak{m}$

proposizione A Noetheriano, P primo minimale sopra $(x_1, \dots, x_r)$, $\operatorname{ht} P = r$.
Allora per ogni $i = 1, \dots, r$ l'ideale $P/(x_1, \dots, x_i)$ ha altezza $r-i$ in $A/(x_1, \dots, x_i)$

DIMOSTRAZIONE
Sia $\overline{P} := P/(x_1, \dots, x_i)$ è minimale sopra $(\overline{x}_{i+1}, \dots, \overline{x}_r)$
quindi $\operatorname{ht} \overline{P} \leq r-i$.
Viceversa, se $h := \operatorname{ht} \overline{P}$, allora $\overline{P}$ è minimale sopra $(\overline{y}_1, \dots, \overline{y}_h)$
$\Rightarrow P$ è minimale sopra $(x_1, \dots, x_i, y_1, \dots, y_h)$
$\Rightarrow \operatorname{ht} P = r \leq i + h \Rightarrow \operatorname{ht} \overline{P} \geq r - i$ □

corollario (A, P) locale regolare, $x_1, \dots, x_r$ sistema regolare di parametri
Allora $A/(x_1, \dots, x_i)$ è regolare, con sistema regolare di parametri $(x_{i+1}, \dots, x_r)$ per ogni $i = 1, \dots, r$

DIMOSTRAZIONE
$\operatorname{ht} P/(x_1, \dots, x_i) = r - i$ ed è generato da $\overline{x}_{i+1}, \dots, \overline{x}_r$ □

teorema Sia (A, P) locale regolare.
Allora A è un dominio.

DIMOSTRAZIONE
Per induzione su $\dim A$
- $\dim A = 0$: P è generato da 0 elementi $\Rightarrow P = (0)$
$\Rightarrow (0)$ è massimale $\Rightarrow A$ campo
- $\dim A = d \geq 1$: prendiamo $x \in P$ che non stia nell'unione dei primi minimali e nemmeno in P^2.
$P \setminus (\bigcup_{i=1}^{s} Q_i \cup P^2) \neq \emptyset$? (Q_i primi minimali)
$\iff P \not\subseteq \bigcup Q_i \cup P^2$ Se $P \subseteq \bigcup Q_i \cup P^2$ avremmo
  - $P \subseteq Q_i$: impossibile perché $1 \leq \operatorname{ht} P \leq \operatorname{ht} Q_i = 0$
  - $P \subseteq P^2$: allora $P = P^2 \overset{\text{Nak}}{\Rightarrow} P = (0)$

$\overline{x} \in P/P^2$ non è zero, e posso completare ad una base dell'A/P-spazio vettoriale P/P^2, diciamo $\overline{x}, \overline{x}_2, \dots, \overline{x}_r$.
Sollevando a $x, x_2, \dots, x_r \in P$, ho un sistema locale di parametri
Considero $A/(x)$, che è regolare con sist. reg. di par. le classi di $x_2, \dots, x_r$ in $A/(x)$
Per ipotesi induttiva, è un dominio, cioè (x) è primo, di altezza $\operatorname{ht}(x) \leq 1$ per Hauptidealsatz, e $\operatorname{ht}(x) \neq 0$ perché $x \notin Q_i$
Prendiamo ora $Q \subsetneq (x)$ ideale primo.
Sia $b \in Q$: allora $b = ax$, con $a \in A$, $x \notin Q \Rightarrow a \in Q$
$\Rightarrow Q \subseteq (x)Q \subseteq PQ \overset{\text{Nak}}{\Rightarrow} Q = (0) \Rightarrow (0)$ è primo e A è dominio. □

Teorema: Auslander-Buchsbaum Sia (A,P) locale regolare. Allora A è UFD.

Oss A locale regolare di $\dim 1 \iff A$ è DVR

Teorema K campo, $A = K[x_1,\dots,x_r]$. Allora tutti gli ideali massimali di A sono generati da $r = \dim A$ elementi (ricordo che $\operatorname{ht} \mathfrak{M} = \dim A$ per ogni massimale $\mathfrak{M}$). In particolare, A è regolare.

DIMOSTRAZIONE

Per induzione su r

- $r=0$: A è un campo
- $r=1$: $K[x]$ è PID.
- Sia $r \geq 2$, $\mathfrak{M}$ ideale massimale. Sia $f \in \mathfrak{M} \setminus \{0\}$.
  A meno di automorfismo di A, posso supporre f monico in x_r.
  Ora $K[x_1,\dots,x_r]/(f)$ è intero se $K[x_1,\dots,x_{r-1}]$
  Sia $N := \mathfrak{M}/(f) \cap K[x_1,\dots,x_{r-1}]$
  Ora $\overline{\mathfrak{M}} = \mathfrak{M}/(f)$ è un ideale massimale di $K[x_1,\dots,x_r]/(f)$, e quindi N è un ideale massimale
  Per ipotesi induttiva, N è generato da $r-1$ elementi $f_1,\dots,f_{r-1}$
  Pensando $f_1,\dots,f_{r-1}$ come elementi di $K[x_1,\dots,x_{r-1}] \subset A$
  abbiamo $(f_1,\dots,f_{r-1})A \subset \mathfrak{M}$. Allora $\mathfrak{M}$ corrisponde ad un ideale di $\frac{K[x_1,\dots,x_r]}{N[x_r]} = \frac{K[x_1,\dots,x_{r-1}][x_r]}{N[x_r]} \simeq \left(\frac{K[x_1,\dots,x_{r-1}]}{N}\right)[x]$,

  che è l'anello di polinomi in 1 variabile sul campo $K[x_1,\dots,x_{r-1}]/N$
  Allora $\mathfrak{M}/N$ è generato da 1 elemento f_r, quindi
  $$\mathfrak{M} = (f_1,\dots,f_r).$$

□

Ex K campo non necess alg. chiuso, $M \subset K[x_1,\dots,x_r]$ ideale massimale
Esiste $(\alpha_1,\dots,\alpha_r) \in \overline{K}^r$ t.c. $M = \{p(x_1,\dots,x_r) \in K[x_1,\dots,x_r] \mid p(\alpha_1,\dots,\alpha_r) = 0\}$

completamenti

Def Un gruppo topologico è un gruppo G munito di una topologia t.c. $m: G\times G \longrightarrow G$ e $i: G \longrightarrow G$ siano continue.

Oss
- i è un omeomorfismo: i^{-1} esiste ed è continua
- Per ogni $g\in G$, la funzione $L_g: \begin{array}{ccc} G & \longrightarrow & G \\ g' & \longmapsto & gg' \end{array}$ è un omeomorfismo
- $\{U_i\}_{i\in I}$ SFI di $\{e\} \Rightarrow \{xU_i\}_{i\in I}$ è SFI di x
- Se U è intorno aperto di e, allora U^{-1} è intorno aperto di e $\Rightarrow U\cap U^{-1}$ è intorno aperto di e

Lemma Sia $H := \bigcap_{\substack{e\in U \\ U \text{ aperto}}} U$. Allora:

(i) $H \trianglelefteq G$.
(ii) $H = \overline{\{e\}}$
(iii) Sia top. su G è $T_2 \iff H = \{e\}$
(iv) G/H è T_2.

DIMOSTRAZIONE

(i) $h_1, h_2 \in H$. $m: G\times G \longrightarrow G$
$h_1h_2 \in H \iff h_1h_2 \in U$ per ogni aperto $U \ni e$
$m^{-1}(U) \ni (e,e) \Rightarrow m^{-1}(U)$ contiene $U_1\times U_2$ con U_1, U_2 intorni aperti di e
$\Rightarrow h_1\in U_1, h_2\in U_2 \Rightarrow h_1h_2 \in m^{-1}(U) \Rightarrow m(h_1,h_2)\in U$
Per l'inverso è analogo
Per la normalità': $\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & gxg^{-1} \end{array}$ è omeomorfismo,

quindi manda gli int. aperti negli int. aperti

(ii) Sia $x\in\overline{\{e\}}$: x è contenuto in tutti i chiusi che contengono e
Se $x\notin H$, $\exists U$ intorno di e t.c. $x\notin U$. Posso supporre $U=U^{-1}$
$x\notin U \iff e\notin xU^{-1} = xU$. Passando al complementare:
$e\in (xU)^c$ chiuso e $x\notin (xU)^c$ ↯
Viceversa, sia $x\in H$: se $x\notin\overline{\{e\}}$, $\exists C$ chiuso con $e\in C, x\notin C \iff e\notin xC^{-1}$
$\Rightarrow e\in (xC^{-1})^c$ aperto, ma $x\notin (xC^{-1})^c \Rightarrow x\notin H$ ↯.

(iii) Se G è T_2, $\overline{\{e\}} = H = \{e\}$.
Viceversa, se $H=\{e\}$, considero $f: \begin{array}{ccc} G\times G & \longrightarrow & G \\ g_1,g_2 & \longmapsto & g_1^{-1}g_2 \end{array}$
Ora $\{e\}$ è chiuso, $f^{-1}(e)$ è un chiuso
cioè la diagonale è chiusa in $G\times G \Rightarrow G$ T_2.

(iv) G/H è $T_2 \iff \overline{H} = \bigcap_{\substack{U\supseteq H \\ U \text{ aperto}}} U/H = \{\bar{e}\}$

□

D'ora in poi: G abeliano, esiste una base numerabile di intorni aperti dell'identità che sono anche sottogruppi, $\{G^n\}_{n\in\mathbb{N}}$

Oss G^0, $G^1 \rightsquigarrow G^0 \cap G^1$, $G^2 \rightsquigarrow G^2 \cap G^1 \cap G^0$, ...
Posso supporre $G^n \supseteq G^{n+1}$

def Una successione di Cauchy in G è una successione $\{g_n\}_{n\in\mathbb{N}} \subseteq G$ t.c.
$\forall m\ \exists n_0 = n_0(m)$ t.c. $\forall n_1, n_2 \geq n_0$ vale $g_{n_1} - g_{n_2} \in G^m$
Due successioni di Cauchy g_n, h_n sono equivalenti se
$g_n - h_n \longrightarrow 0$, cioè $\forall m\ \exists n_0(m)$ t.c. $g_n - h_n \in G^m\ \forall n \geq n_0$
Il completamento di G rispetto alla topologia indotta da G^n è
$\hat{G} = \{\text{successioni di Cauchy}\}/\text{equivalenza}$.
È un gruppo (la somma si fa termine a termine; è compatibile con l'equivalenza) topologico:
come base di intorni dell'identità
$\hat{G}^n = \{$classi di equiv. di suc. di Cauchy ogni cui rappr. $\{g_k\}$ ha la proprietà che $g_k \in G^n$ per ogni $k >> 0\}$

Oss Sia $\pi_n : G \longrightarrow G_n := G/G^n$ la proiezione canonica
Se $\{g_n\}$ è di Cauchy, $\{\pi_n(g_i)\}$ è def. costante (per $i \to +\infty$, n fissato).
Chiamiamo $\pi_n(g_\infty)$ il valore a cui si stabilizza.
$$\varphi : \hat{G} \longrightarrow \prod G_n = \prod G/G^n$$
$$\{g_i\} \longmapsto (\pi_n(g_\infty))_n$$
È ben definita e iniettiva
Se una collezione $(\xi_n) \in \prod G_n$ sta in $\mathrm{Im}\varphi$, allora
$$\begin{array}{ccc} \xi_{n+1} & \longmapsto & \xi_n \\ G/G^{n+1} & \longrightarrow & G/G^n \end{array}$$

def Una sequenza compatibile è un elemento $(\xi_n) \in \prod G/G^n$
tale che $\xi_{n+1} \bmod G^n = \xi_n \quad \forall n \geq 0$.

L'immagine di φ è l'insieme delle successioni compatibili, che denoteremo $\varprojlim G/G^n$
Infatti, se (ξ_n) è compatibile scelgo $\tilde{\xi}_n \in G$ t.c. $\tilde{\xi}_n \equiv \xi_n \bmod G^n$
Dico che $(\tilde{\xi}_n)$ è di Cauchy: $\tilde{\xi}_n - \tilde{\xi}_m \equiv \xi_n - \xi_m \equiv 0 \bmod G^n \quad m \geq n$

proposizione $\hat{G} \cong \varprojlim G/G^n$ come gruppo topologico, dove la topologia su $\varprojlim G/G^n$ è quella di sottospazio (chiuso) del prodotto $\prod G/G^n$

Oss Gli aperti in $\varprojlim G/G^n$: una base di intorni dell'identità è data da $\{\ker \pi_k : \varprojlim G/G^n \longrightarrow G_k\}_k$

def A anello, M A-modulo.
Una filtrazione su M è una successione $M^0 \supseteq M^1 \supseteq M^2 \supseteq \dots$ di sottomoduli di M. Si dice esaustiva se $\bigcup M^i = M$ e separata se $\bigcap M^i = \{0\}$

Poniamo $M_n := M/M^n$, $\phi_n : M/M^{n+1} \longrightarrow M/M^n$

$$M \longrightarrow \hat{M} \cong \varprojlim M_n$$
$$m \longmapsto (m \bmod M^n)_n$$

Il nucleo di $M \to \hat{M}$ è $\bigcap M^n$, quindi è iniettiva $\iff \bigcap M^n = \{0\} \iff$ la top. è T_2
Se $M \to \hat{M}$ è un isomorfismo, si dice che M è completo.

$M^n = I^n M$ topologia I-adica

Oss • $\hat{M}$ ha una topologia con intorni aperti
$\hat{M}^n := \ker(\hat{M} \to M_n)$
• $\hat{M}^n \supset \hat{M}^{n+1}$ $\forall n$ e $\hat{M}/\hat{M}^n \cong M/M^n$
$\|$
$\mathrm{Im}(\hat{M} \to M_n)$, che è surgettiva perché dato $\overline{m} \in M_n$, trovo $m \in M$ che si proietta su $\overline{m}$ e prendo la succ. costante m
• $\hat{\hat{M}} = \varprojlim \hat{M}/\hat{M}^n = \varprojlim M/M^n = \hat{M}$
• A anello: $\hat{A} = \varprojlim A/I^n \subseteq \prod A/I^n$ è un anello

esempio • $A = R[x_1, x_2, \dots, x_r]$
$A^n = (x_1, \dots, x_r)^n$, A/A^n polinomi in $R[x_1, \dots, x_r]$ di grado $\le n-1$
$\varprojlim A/A^n \ni \sum_{i_1, \dots, i_r = 0}^{\infty} c_{i_1, \dots, i_r} x_1^{i_1} \cdots x_r^{i_r}$
da interpretare come $\left(\sum_{i_1 + \dots + i_r \le n-1} c_{i_1, \dots, i_r} x_1^{i_1} \cdots x_r^{i_r} \right)_n$

• Se A è un anello completo rispetto ad $\{A^n\}$, scriveremo $\sum_{i=0}^{\infty} a_i$ con l'ipotesi che tutti gli a_n salvo un n° finito stanno in A^n per indicare la successione coerente $\left(\sum_{i \le n, a_i \in A^n} a_i \right)_{n \in \mathbb{N}}$

• A anello, I ideale di A, M A-modulo, $M^n = I^n M$
$\hat{M} = \varprojlim M/M^n$ è detto il completamento I-adico di M
$A = M = \mathbb{Z}$, $I = (p) \longrightarrow \hat{A} \cong \mathbb{Z}_p$ è l'anello degli interi p-adici
$A = M = \mathbb{Z}$, $M^n = 2\mathbb{Z} \longrightarrow \hat{A} = \varprojlim \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$

proposizione M^n, N^n filtrazioni su M. Supponiamo che
$\forall m \ge 0$ $\exists n_0(m)$ t.c. $N^n \subseteq M^m$ $\forall n \ge n_0$ e
$\forall n \ge 0$ $\exists m_0(n)$ t.c. $M^m \subseteq N^n$ $\forall m \ge m_0$.
Allora i completamenti rispetto M^n e N^n sono isomorfi.

DIMOSTRAZIONE
L'ipotesi significa che le topologie indotte sono la stessa, e il completamento dipende solo dalla topologia. □

Oss Fissiamo A anello, I ideale. Su ogni A-modulo M c'è la topologia I-adica.
Siano M,N due A-moduli, $\varphi: M \to N$ omomorfismo
$$\varphi(I^n M) \subseteq I^n \varphi(M) \subseteq I^n N$$
Allora possiamo definire una mappa $\hat{\varphi}: \hat{M} \to \hat{N}$, $(\xi_n) \mapsto (\varphi_n(\xi_n))$

$\varphi_n : M/I^n M \to N/I^n N$ è ben definita ed è un omomorfismo di moduli
Inoltre la successione $(\varphi_n(\xi_n))$ è coerente:
$$\varphi_n(\xi_{n+1}) \equiv \varphi_n(\xi_n) \mod I^n N$$
$$\varphi_{n+1}(\xi_n + I^n M) \subseteq \varphi_{n+1}(\xi_n) + I^n N$$
Quindi $M \mapsto \hat{M}$, $\varphi \mapsto \hat{\varphi}$ è un funtore sulla categoria degli A-moduli.

teorema A anello Noetheriano, I ideale di A. Se la successione
$$0 \to M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \to 0$$
è esatta e M_1, M_2, M_3 sono finitamente generati, allora
$$0 \to \hat{M}_1 \xrightarrow{\hat{\alpha}} \hat{M}_2 \xrightarrow{\hat{\beta}} \hat{M}_3 \to 0$$
è esatta.

corollario A Noeth, I ideale
(i) Il completamento di I^n/I^{n+1} è I^n/I^{n+1} $\forall n \geq 0$
(ii) $\hat{A}/\hat{I} \cong A/I$ e $\hat{I}^n/\hat{I}^{n+1} \cong I^n/I^{n+1}$ $\forall n \geq 0$.

DIMOSTRAZIONE
(i) $M := I^n/I^{n+1}$ $\quad M^{(i)} = I^i I^n/I^{n+i} = 0$ $\forall i \geq 1$
$\varprojlim M/M^{(i)}$ = succ. coerenti in $(0) \times \prod_{i \geq 1} M = \{(m_i) \mid m_{i+1} = m_i\} \cong I^n/I^{n+1}$
(ii) $0 \to I^{n+1} \to I^n \to I^n/I^{n+1} \to 0$ esatta
$\Rightarrow 0 \to \widehat{I^{n+1}} \to \widehat{I^n} \to \widehat{I^n/I^{n+1}} \to 0$ esatta, quindi
$I^n/I^{n+1} = \widehat{I^n}/\widehat{I^{n+1}} = \hat{I}^n/\hat{I}^{n+1}$ □

Lemma $\hat{A}^n \cong \hat{A}^n$

DIMOSTRAZIONE
$$\hat{A}^n = \varprojlim (A^n/I^k A^n) = \varprojlim (A/I^k)^n = \hat{A}^n$$ □

proposizione A Noetheriano, I ideale rispetto a cui si completa, J ideale.
- $\hat{J}$ = ideale generato da J in $\hat{A}$ $=: J\hat{A}$
- in particolare, $\hat{A/J} \cong \hat{A}/J\hat{A}$

DIMOSTRAZIONE

- A Noeth $\Rightarrow$ J fin gen, $J=(x_1,\dots,x_n)$

$$0 \longrightarrow K \longrightarrow A^n \xrightarrow{\beta} J \longrightarrow 0 \quad \text{esatta}$$

$K = \ker\beta$ $\quad (a_1,\dots,a_n) \longmapsto \sum_{i=1}^n a_i x_i$ $\quad \iota: A \longrightarrow \hat{A}$

$$\Rightarrow \quad 0 \longrightarrow \hat{K} \longrightarrow \hat{A}^n \xrightarrow{\hat{\beta}} \hat{J} \longrightarrow 0 \quad \text{è esatta}$$

$$(\hat{a}_1,\dots,\hat{a}_n) \longmapsto \sum_{i=1}^n \hat{a}_i\,\iota(x_i)$$

$$\Rightarrow \hat{J} = (\iota(x_1),\dots,\iota(x_n))\hat{A}$$

- Per def ho $\quad 0 \longrightarrow J \longrightarrow A \longrightarrow A/J \longrightarrow 0$ esatta

$$\Rightarrow \quad 0 \longrightarrow \hat{J} \longrightarrow \hat{A} \longrightarrow \hat{A/J} \longrightarrow 0 \quad \text{è esatta}$$

$$\Rightarrow \quad \hat{A/J} \cong \hat{A}/J\hat{A}$$

□

esempio $A = K[x,y]$, $I=(x,y)$, $J=(y^2-x^3-x^2)$

$$\hat{A/J} \cong \hat{A}/J\hat{A} = K[[x,y]]/(y^2-x^3-x^2)$$

proposizione A Noetheriano. Allora $A[[x]]$ è Noetheriano.

DIMOSTRAZIONE

Chiamiamo $v(\sum_{i=0}^{+\infty} a_i x^i) = \min\{i : a_i \neq 0\}$ e $lc(\sum_{i=0}^{+\infty} a_i x^i) = a_{v(\sum a_i x^i)}$

Sia I un ideale di $A[[x]]$: mostriamo che è fin.gen.

Sia $I_r = \{lc(f) \mid f \in I, v(f) = r\} \cup \{0\}$

(Sono ideali: se $i_1, i_2 \in I_r$, allora $i_1 = lc(f_1)$, $i_2 = lc(f_2)$ e
0 $i_1 + i_2 = 0$ $i_1 + i_2 = lc(f_1 + f_2)$ che ha $v(f_1+f_2) = r$.
Se $i \in I_r$, $i = lc(f)$, allora $\forall a \in A$ o $a \cdot i = 0$ o $a \cdot i = lc(a \cdot f)$)

$I_r \subseteq I_{r+1}$: se $i \in I_r$, $i = lc(f)$, $v(f) = r$ e $i = lc(xf)$ con $v(xf) = r+1$

A Noeth $\Rightarrow$ I_r stabilizza a n_0: $I_n = I_{n_0}$ $\forall n \geq n_0$

Prendo a_{ij} generatori di I_i per $i = 1, \dots, n_0$ con $1 \leq j \leq l(i) < +\infty$
e $f_{ij} \in I$ con $v(f_{ij}) = i$ e $lc(f_{ij}) = a_{ij}$.

Dimostriamo che gli f_{ij} generano I

Dato $f \in I$, $f \neq 0$, e scrivo $f = a_r x^r + a_{r+1} x^{r+1} + \dots$

- Se $r \leq n_0$, $a_r \in I_r = (a_{r,1}, \dots, a_{r,l(r)})$
  Scrivo $a_r = \sum_{j=1}^{m} c_j a_{rj} \longrightarrow lc\Big(\sum_{j=1}^{m} c_j \underbrace{f_{r,j}}_{(f_{r,j})}\Big) = a_r$
  $f - \sum_{j=1}^{m} c_j f_{r,j} = a'_{r+1} x^{r+1} + a'_{r+2} x^{r+2} + \dots$
- Se $r > n_0$, $a \in I_r = I_{n_0}$: scrivo $a_r = \sum_{j=1}^{m} c_j a_{n_0,j}$
  e $f - \sum_{j=1}^{m} c_j x^{r-n_0} f_{n_0,j} = a'_{r+1} x^{r+1} + \dots$

Quindi posso trovare iterativamente dei $c_j^{(r)} \in A$ t.c.

$$f - \sum_{r=0}^{n_0} \sum_{j=1}^{m} c_j^{(r)} f_{r,j} - \sum_{r=n_0+1}^{+\infty} \sum_{j=1}^{m} c_j^{(r)} x^{r-n_0} f_{n_0,j} = 0$$

$$\Rightarrow f = \sum_{r=0}^{n_0} \sum_{j=1}^{m} \underbrace{c_j^{(r)} f_{r,j}}_{(f_{r,j})} + \sum_{j=1}^{m} \Big(\underbrace{\sum_{r=n_0+1}^{+\infty} c_j^{(r)} x^{r-n_0}}_{\in A[[x]]} \Big) f_{n_0,j}$$

$\Rightarrow I = (f_{r,j})$ è fin.gen. □

proposizione A Noetheriano, $I = (a_1, \dots, a_n)$. Allora
(i) $\hat{A} \cong A[[x_1, \dots, x_n]] / (x_i - a_i \mid i = 1, \dots, n)$
(ii) $\hat{A}$ è Noetheriano.

DIMOSTRAZIONE

$B := A[x_1, \dots, x_n] \xrightarrow{\varphi} A$ $\qquad I = (x_1, \dots, x_n)$
$x_i \longmapsto a_i$

$J = \ker \varphi = (x_i - a_i \mid i = 1, \dots, n)$
$f(x_1, \dots, x_n) = (x_1 - a_1) g_1 + h(x_2, \dots, x_n) = (x_1 - a_1) g_1 + \dots + (x_n - a_n) g_n + a$
$0 = \varphi(f(x_1, \dots, x_n)) = a \Rightarrow f \in (x_i - a_i \mid i = 1, \dots, n)$

Ho la succ. esatta $0 \longrightarrow J \longrightarrow B \longrightarrow A \longrightarrow 0$ di B-moduli
$\Rightarrow$ $0 \longrightarrow \hat{J} = J\hat{B} \longrightarrow \hat{B} \longrightarrow \hat{A} \longrightarrow 0$ è esatta
$\Rightarrow \hat{A} \cong \hat{B} / J\hat{B} \cong K[[x_1, \dots, x_n]] / (x_i - a_i \mid i = 1, \dots, n)$

(ii) Per induzione, $A[[x_1, \dots, x_n]]$ è Noeth $\Rightarrow$ $\hat{A}$ è Noeth □

Oss Se R è completo rispetto alla topologia m-adica, dove m è massimale, allora R è locale.

DIMOSTRAZIONE

$R = \hat{R} = \varprojlim R/m^n$

Dimostriamo che gli el. di $R \setminus m$ sono invertibili.

Sia $a \in R \setminus m$. La classe $\bar{a} \in R/m$ è invertibile:

sia $b \in R$ t.c. $ab \in 1+m$ Scrivo $ab = 1-m$ con $m \in m$.

Basta dim. che $1-m$ è invertibile. Il suo inverso è $1+m+m^2+m^3+\ldots = \sum_{i=0}^{+\infty} m^i$

Basta vedere che $(1-m)\sum_{i=0}^{n-1} m^i \equiv 1$ in R/m^n $\forall n$

$1 - m^n$

Sugli interi p-adici

p primo, $\mathbb{Z}_p$ completamento p-adico di $\mathbb{Z}$

$$\mathbb{Z}/p\mathbb{Z} \longleftarrow \mathbb{Z}/p^2\mathbb{Z} \longleftarrow \mathbb{Z}/p^3\mathbb{Z} \longleftarrow \ldots$$
$$a_0 \qquad a_0 + pa_1 \qquad a_0 + pa_1 + p^2a_2$$

$$\longrightarrow \mathbb{Z}_p = \{ \sum_{i=0}^{+\infty} a_i p^i \text{ con } a_i \in \{0, \ldots, p-1\} \} = \mathbb{Z}[[X]]/(X-p)$$

esempio $p=5$ $\quad (2+p)(3+p) = 6 + 5p + p^2 = 1 + 6p + p^2 = 1 + p + 2p^2$

$$\mathbb{Z}[[X]]/(X-p) \longrightarrow \mathbb{Z}_p$$
$$\sum_{n=0}^{+\infty} a_n X^n \longmapsto \sum_{n=0}^{+\infty} a_n p^n$$

esempio $p=2$ "Quanto fa" $1+2+4+\ldots = \sum_{n=0}^{+\infty} 2^n$ in $\mathbb{Z}_2$

$\frac{1}{1-2} = -1$

$$\mathbb{Z}[[X]]/(X-2) \xrightarrow{\phi} \mathbb{Z}_2$$
$$\frac{1}{1-X} = \sum_{n \geq 0} X^n \longrightarrow \sum 2^n = \phi\left(\frac{1}{1-X}\right) = -1$$

$$\sum_{n \geq 0} 2^n = -1 \iff \underbrace{1+1+2+4+8+16+\ldots = 0}_{\text{è } 0 \bmod 2^n \ \forall n}$$

Valutazione

$$v_p\left(\sum_{n=0}^{+\infty} a_n p^n\right) = \min\{n \mid a_n \neq 0\}$$
$$a_n \in \{0, \ldots, p-1\}$$

- $v(ab) = v(a) + v(b)$ $\quad \Longrightarrow \mathbb{Z}_p$ è dominio
- $v(a+b) \geq \min\{v(a), v(b)\}$, con $=$ se $v(a) \neq v(b)$

$\mathbb{Z}_p$ è locale, Noetheriano, il suo ideale massimale è (p)

$\mathbb{Z}_p$ è un DVR

Lemma $f(x) \in R[x]$. Allora $\exists g(x,t) \in R[x,t]$ t.c.
$f(x+t) = f(x) + f'(x)t + t^2 g(x,t)$

DIMOSTRAZIONE
Per linearità, basta $f = c_n x^n$
$c_n(x+t)^n = c_n\left(x^n + n \cdot t x^{n-1} + t^2 \sum_{j=2}^{n} \binom{n}{j} t^{j-2} x^{n-j}\right)$ □

Lemma di Hensel R anello completo rispetto alla topologia data da un ideale massimale m, $f(x) \in R[x]$, $a_1 \in R$ t.c. $f(a_1) \equiv 0 \pmod m$. Supponiamo $f'(a_1) \notin m$.
Allora $\exists! a \in R$ t.c. $f(a) = 0$ e $a \equiv a_1 \bmod m$.

DIMOSTRAZIONE
$R = \hat{R} = \varprojlim R/m^n$, $a = (a_n)$
$f(a_1) = 0 \implies f(a_1) \equiv 0 \bmod m^2 \implies f(a_2) \equiv 0 \bmod m^2$
Devo scegliere $a_2 = a_1 + m$ per qualche $m \in m$
$0 \equiv f(a_2) \equiv f(a_1+m) \equiv f(a_1) + m f'(a_1) + m^2 g(a,m) \equiv f(a_1) + m f'(a_1) \bmod m^2$
Devo prendere $m \equiv -f(a_1)/f'(a_1) \bmod m^2$ ($f'(a_1) \notin m$, quindi invertibile)

In generale, prendiamo $a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$
Allora $f(a_{n+1}) = f\left(a_n - \frac{f(a_n)}{f'(a_n)}\right) =$
$= f(a_n) - \frac{f(a_n)}{f'(a_n)} f'(a_n) + \left(-\frac{f(a_n)}{f'(a_n)}\right)^2 (\dots)$
Se $f(a_n) \equiv 0 \pmod{m^i} \implies f(a_{n+1}) \equiv 0 \bmod m^{2i}$
Per induzione
- $f(a_n) \in m^n$
- $a_{n+1} \equiv a_n \bmod m^n$
- $f'(a_n) \equiv f'(a_1) \notin m$ ed è invertibile

$\implies$ la successione $a = (a_n)_{n \in \mathbb{N}}$ è compatibile e $f(a) = 0$.
Siano $a \neq b$ due soluzioni di $f(x) = 0$ con $a \equiv b \equiv a_1 \pmod m$
$\exists n$ t.c. $a - b \in m^n \setminus m^{n+1}$ (altrimenti $a = b$ in ogni $R/m^{n+1} \implies a = b$)
$0 = f(a) = f(b + (a-b)) = f(b) + f'(b)(a-b) + (a-b)^2 g(a,b)$
$\implies -f'(b)(a-b) = (a-b)^2 g(a,b)$
$m \notin f'(a_1)$; $m^n \setminus m^{n+1}$; m^{2n}
Siccome $n \geq 1$, questo è impossibile. □

def Sia $\{G_n\}_{n\in\mathbb{N}}$ una sequenza di gruppi, muniti di omomorfismi $\phi_n: G_{n+1} \longrightarrow G_n$: questo si chiama sistema inverso di gruppi, se ϕ_n sono le mappe di transizione.
Il limite inverso (o limite proiettivo) è

$$\varprojlim G_n = \{ (g_n) \in \prod G_n \mid \phi_n(g_{n+1}) = g_n \ \forall n \}$$

proposizione Siano $(A_n), (B_n), (C_n)$ tre sistemi inversi di gruppi abeliani e

$$0 \longrightarrow A_\bullet \xrightarrow{\alpha_\bullet} B_\bullet \xrightarrow{\beta_\bullet} C_\bullet \longrightarrow 0$$

una successione esatta, cioè un insieme di diagrammi commutativi

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_n & \xrightarrow{\alpha_n} & B_n & \xrightarrow{\beta_n} & C_n & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle \phi^A_n} & \circlearrowleft & \uparrow{\scriptstyle \phi^B_n} & \circlearrowleft & \uparrow{\scriptstyle \phi^C_n} & & \\ 0 & \longrightarrow & A_{n+1} & \xrightarrow{\alpha_{n+1}} & B_{n+1} & \xrightarrow{\beta_{n+1}} & C_{n+1} & \longrightarrow & 0 \end{array} \qquad \text{esatta } \forall n$$

(i) C'è una successione esatta

$$0 \longrightarrow \varprojlim A_n \xrightarrow{\hat{\alpha}} \varprojlim B_n \xrightarrow{\hat{\beta}} \varprojlim C_n$$

(ii) Se inoltre ϕ^A_n è surgettiva, allora è esatta anche

$$0 \longrightarrow \varprojlim A_n \xrightarrow{\hat{\alpha}} \varprojlim B_n \xrightarrow{\hat{\beta}} \varprojlim C_n \longrightarrow 0$$

DIMOSTRAZIONE

(i) Iniettività di $\hat{\alpha}$: se $\hat{\alpha}((a_n)) = 0$, allora $(\alpha_n(a_n)) = 0$
$\Longrightarrow \forall n \ \alpha_n(a_n) = 0$, ma α_n è iniettiva $\Longrightarrow a_n = 0 \ \forall n \Longrightarrow (a_n) = 0$

Esattezza in $\varprojlim B_n$: $\ker\hat{\beta} = \operatorname{Im}\hat{\alpha}$
Sia $(b_n) \in \ker\hat{\beta}$. Allora $\beta_n(b_n) = 0 \ \forall n$, e quindi
$\forall n \ \exists a_n \in A_n$ con $b_n = \alpha_n(a_n)$. Vorrei dire $(b_n) = \hat{\alpha}((a_n))$:
(a_n) è compatibile, infatti $\phi^A_n(a_{n+1}) \overset{?}{=} a_n \ \forall n$

$$\overset{\alpha_n \text{ iniettiva}}{\Longleftrightarrow} \alpha_n \circ \phi^A_n(a_{n+1}) \overset{?}{=} \alpha_n(a_n) = b_n \Longleftrightarrow \phi^B_n \circ \alpha_{n+1}(a_{n+1}) \overset{?}{=} b_n$$
$$\Longleftrightarrow \phi^B_{n+1}(b_{n+1}) = b_n, \text{ vero poiché } (b_n) \text{ è compatibile}$$

(ii) Sia $(c_n) \in \varprojlim C_n$. Per ogni n, β_n è surgettiva
$\Longrightarrow \exists b_n \in B_n$ t.c. $c_n = \beta_n(b_n)$.
Non è detto che (b_n) sia compatibile, ma possiamo renderla tale.
$\phi^B_n(b_{n+1}) \overset{?}{=} b_n$
So che $\beta_n \circ \phi^B_n(b_{n+1}) = \phi^C_n \circ \beta_{n+1}(b_{n+1}) = \phi^C_n(c_{n+1}) = c_n = \beta_n(c_n)$
$\Longrightarrow \phi^B_n(b_{n+1}) - b_n \in \ker\beta_n = \operatorname{Im}\alpha_n \Longrightarrow \exists! \, a_n \in A_n$ t.c. $\phi^B_n(b_{n+1}) - \alpha_n(a_n) = b_n$
Per ipotesi, $\exists a_{n+1} \in A_{n+1}$ t.c. $a_n = \phi^A_n(a_{n+1})$, e allora

$$\alpha_n(a_n) = \alpha_n \circ \phi^A_n(a_{n+1}) = \phi^B_n \circ \alpha_{n+1}(a_{n+1})$$

Quindi $\phi^B_n(b_{n+1} - \alpha_{n+1}(a_{n+1})) = b_n$
Infine $\beta_{n+1}(b_{n+1} - \alpha_{n+1}(a_{n+1})) = c_{n+1} - \beta_{n+1} \circ \alpha_{n+1}(a_{n+1}) = c_{n+1}$
Iterativamente, posso rendere (b_n) compatibile
senza cambiare il fatto che $\hat{\beta}((b_n)) = (c_n) \Longrightarrow \hat{\beta}$ è surgettiva. □

Teorema A anello Noetheriano, I ideale di A. Se la successione

$$0 \longrightarrow M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \longrightarrow 0$$

è esatta e M_1, M_2, M_3 sono finitamente generati, allora

$$0 \longrightarrow \hat{M}_1 \xrightarrow{\hat{\alpha}} \hat{M}_2 \xrightarrow{\hat{\beta}} \hat{M}_3 \longrightarrow 0$$

è esatta.

Lemma di Artin-Rees A anello Noetheriano, $M_1 \subseteq M_2$ A-moduli fin. gen. La filtrazione $I^n M_2 \cap M_1$ induce la stessa topologia su M_1 della filtrazione $I^n M_1$.

DIMOSTRAZIONE (TEO)

$$0 \longrightarrow M_1 \longrightarrow M_2 \xrightarrow{\beta} M_3 \longrightarrow 0 \quad \text{esatta}$$

$$\Rightarrow \quad M_1/I^n M_1 \longrightarrow M_2/I^n M_2 \xrightarrow{\beta_n} M_3/I^n M_3 \longrightarrow 0$$

$$M_2 \twoheadrightarrow M_3 \twoheadrightarrow M_3/I^n M_3, \qquad M_2 \twoheadrightarrow M_2/I^n M_2 \twoheadrightarrow M_3/I^n M_3$$

Dico che $\ker\left(M_2/I^n M_2 \xrightarrow{\beta_n} M_3/I^n M_3\right)$ è $\dfrac{M_1 + I^n M_2}{I^n M_2}$

Se $m_2 + I^n M_2 \in \ker \beta_n$, allora $\beta(m_2) \in I^n M_3$

$\Rightarrow$ posso scrivere $\beta(m_2) = i_n m_3$ con $i_n \in I^n$, $m_3 \in M_3$

$= i_n \beta(m_2')$ $\quad m_2' \in M_2$

$\Rightarrow \beta(m_2 - i_n m_2') = 0$

$\Rightarrow m_2 - i_n m_2' \in M_1 \Rightarrow m_2 \in M_1 + I^n M_2$

Se ho $m_1 + i_n m_2$ e applico β, trovo

$\beta(m_1) + i_n \beta(m_2) = i_n \beta(m_2) \in I^n M_3$ e passando al quoziente trovo 0.

Ho quindi

$$0 \longrightarrow \frac{M_1 + I^n M_2}{I^n M_2} \longrightarrow M_2/I^n M_2 \longrightarrow M_3/I^n M_3 \longrightarrow 0 \quad \text{esatta } \forall n$$

$$\| 2$$

$$0 \longrightarrow \frac{M_1}{M_1 \cap I^n M_2} \longrightarrow M_2/I^n M_2 \longrightarrow M_3/I^n M_3 \longrightarrow 0$$

$$\uparrow \qquad\qquad \uparrow \qquad\qquad \uparrow$$

$$0 \longrightarrow \frac{M_1}{M_1 \cap I^{n+1} M_2} \longrightarrow M_2/I^{n+1} M_2 \longrightarrow M_3/I^{n+1} M_3 \longrightarrow 0$$

La proposizione fornisce

$$0 \longrightarrow \varprojlim \frac{M_1}{M_1 \cap I^n M_2} \longrightarrow \varprojlim M_2/I^n M_2 \longrightarrow \varprojlim M_3/I^n M_3 \longrightarrow 0$$

$$\| \text{ Artin-Rees}$$

$$0 \longrightarrow \hat{M}_1 \longrightarrow \hat{M}_2 \longrightarrow \hat{M}_3 \longrightarrow 0$$

□

Def. A anello, M modulo, $M = M^0 \supset M^1 \supset M^2 \supset \dots$ una filtrazione. Diciamo che $\{M^n\}$ è

- una I-filtrazione se $I M^n \subseteq M^{n+1}$ $\forall n \geq 0$
- una I-filtrazione stabile se inoltre $\exists n_0 \geq 0$ t.c. $\forall r \geq 0$

$$M^{n_0+r} = I^r M^{n_0}$$

Due filtrazioni M^n, N^n hanno differenze limitate se $\exists n_0$ t.c. $M^{n+n_0} \subseteq N^n$ $\forall n$ e $N^{n+n_0} \subseteq M^n$ $\forall n$

Lemma Se $M^{\bullet}, N^{\bullet}$ sono due filtrazioni I-stabili, allora hanno differenze limitate.

DIMOSTRAZIONE

$\exists n_0$ t.c. $\forall r \geq 0$ $M^{n_0+r} = I^r M^{n_0}$ e $N^{n_0+r} = I^r N^{n_0}$

$M^{n_0+r} = I^r M^{n_0} \subseteq I^r M^0 = I^r N^0 \subseteq N^r$

e viceversa. □

Lemma di Artin-Rees Sia A anello Noetheriano, I ideale di A, M A-modulo fin.gen, $M^{\bullet}$ una I-filtrazione stabile, $M' \subseteq M$ un sottomodulo.

(i) $M^n \cap M'$ è una I-filtrazione stabile di M'

(ii) $\exists k \geq 0$ t.c. $\forall n \geq k$ vale

$$I^n M \cap M' = I^{n-k}(I^k M \cap M')$$

(iii) $\{I^n M'\}$ e $\{I^n M \cap M'\}$ inducono la stessa topologia su M'.

Anelli graduati

Def Un anello graduato è un anello A munito di una decomposizione $A \simeq \bigoplus_{n \in \mathbb{N}} A_n$ come gruppo additivo, tale che $\forall a_m \in A_m$ $\forall a_n \in A_n$ $a_n a_m \in A_{n+m}$

esempio $A = K[x_1, \dots, x_n] = \bigoplus_{n \geq 0} A_n$, $A_n = \{\text{pol. omogenei di grado } n\}$

Oss $A_+ := \bigoplus_{n \geq 1} A_n$ è un ideale:

$$(b_0 + \underbrace{b_1 + \dots + b_m}_{\in A_+})(a_1 + a_2 + \dots + a_{n_0}) \in A_+$$

Def Un modulo graduato su $A \simeq \bigoplus A_n$ è un A-modulo M con una decomposizione $M \simeq \bigoplus_{n \geq 0} M_n$, in cui ogni M_n è un sotto-A_0-modulo, con la proprietà $\forall a \in A_d$, $\forall m \in M_n$ si ha $am \in M_{n+d}$

Gli elementi $m \in M_n$ si chiamano omogenei di grado n.

In generale, ogni $m \in M$ si scrive in modo unico come

$$m = \underbrace{m_{d_1}}_{\in M_{d_1}} + \dots + \underbrace{m_{d_k}}_{\in M_{d_k}}$$

e gli m_{d_i} si chiamano le componenti omogenee di m

proposizione A anello graduato. Sono equivalenti:
(i) A Noetheriano
(ii) A_0 Noetheriano, A fin. gen. come A_0-algebra

DIMOSTRAZIONE
(ii) $\Rightarrow$ (i): $\underbrace{A_0[x_1,\dots,x_n]}_{\text{Noetheriano per Teo. base di Hilbert}} \twoheadrightarrow A \Rightarrow A$ Noetheriano
(i) $\Rightarrow$ (ii): $A_0 \simeq A/A_+$ è Noetheriano
$A_+ \lhd A$ Noeth $\Rightarrow A_+ = (x_1,\dots,x_n)$ (come ideale di A)
Scrivo ogni $x_i = \sum y_{ij}$ con y_{ij} omogeneo di deg >0
$\longrightarrow A_+ = (y_{ij})$
Quindi wlog posso supporre x_i omogenei di grado d_i
Consideriamo $\varphi: A_0[t_1,\dots,t_n] \longrightarrow A$, $t_i \longmapsto x_i$: voglio dire che è surg.

Siccome $A \simeq \bigoplus_{d\geq 0} A_d$, basta mostrare $A_d \subseteq \mathrm{Im}\varphi \ \forall d \geq 0$.
Per induzione:
- $d=0$: $A_0 = \varphi$(polinomi costanti)
- $d \geq 1$: sia $a \in A_{d+1} \subseteq A_+ = (x_1,\dots,x_n)$.
  In A posso scrivere $a = \sum_{i=1}^{n} a_i x_i$
  $\Rightarrow [a]_{d+1} = \sum_{i=1}^{n} [a_i x_i]_{d+1} = \sum_{i=1}^{n} [a_i]_{d+1-d_i} x_i$
  $a_i = a_{i,0} + \dots + a_{i,k}$ comp. omog.
  $\Rightarrow a_i x_i = a_{i,0}x_i + a_{i,1}x_i + \dots + a_{i,k}x_i$ comp. omog.
  Per ipotesi induttiva, $[a_i]_{d+1-d_i} \in \mathrm{Im}\varphi$ ($d+1-d_i \leq d$)
  $\Rightarrow a = [a]_{d+1} \in \mathrm{Im}\varphi \Rightarrow A_{d+1} \subseteq \mathrm{Im}\varphi$

def Sia A anello, I ideale di A, M A-modulo con una I-filtrazione M^n
L'algebra di blow-up (o algebra di Rees) è
$$B_I A := \bigoplus_{n\geq 0} I^n = A \oplus I \oplus I^2 \oplus \dots \quad \left(= \bigoplus_{n\geq 0} t^n I^n\right)$$
e $B(M) = \bigoplus_{n\geq 0} M^n$

Oss
- $B_I A$ è un anello graduato e $B(M)$ è un modulo graduato su $B_I A$:
  $I^m \times M^n \longrightarrow M^{m+n}$ ha senso perché, per def. di I-filtrazione, $I^m M^n \subseteq M^{m+n}$
- A Noetheriano, allora $B_I A$ è Noetheriano:
  $(B_I A)_0 = A$ è Noetheriano e $B_I A$ è generato come A-algebra da $\{t\, i_j\}_{j=1,\dots,m}$ dove $(i_1,\dots,i_m) = I$.

esempio
- $A = K[x]$, $I = (x)$
  $B_I A = K[x] \oplus (x)t \oplus (x)^2 t^2 \oplus \dots \simeq K[x, tx] \simeq K[x,y]$
- $A = K[x,y]$, $I = (x,y)$
  $B_I A \cong K[x,y] \oplus (x,y)t \oplus (x,y)^2 t^2 \oplus \dots \simeq$
  Siano $w = xt$, $z = yt$: soddisfano $yw = xz$
  $\Rightarrow B_I A \simeq K[x,y,z,w]/(xz - yw)$

Hauptidealsatz per varietà

ES K campo, $A = K[x_1, \dots, x_n]$, $f \in A$ irriducibile
$L = \mathrm{Frac}(A/(f))$. Dimostrare che
$\mathrm{trdeg}_K L = n-1$

SOL Wlog $\deg_{x_n}(f) > 0$
Considero le classi di $x_1, \dots, x_{n-1}$ in L.
- Sono alg. indipendenti: per assurdo, siano dipendenti
  Allora $\exists p(t_1, \dots, t_{n-1}) \in K[t_1, \dots, t_{n-1}]$ t.c. $p(\bar{x}_1, \dots, \bar{x}_{n-1}) = 0$ in L,
  cioè $p(x_1, \dots, x_n) \in (f)$ ma i multipli non banali di
  f dipendono da x_n, assurdo
- $K \subseteq K(\bar{x}_1, \dots, \bar{x}_{n-1}) \subseteq L$
  ↑ algebrica: è generata da x_n, che è algebrico su $K(\bar{x}_1, \dots, \bar{x}_{n-1})$

$\Rightarrow \mathrm{trdeg}_K L = \mathrm{trdeg}_K K(\bar{x}_1, \dots, \bar{x}_{n-1}) = n-1$

ES $A = K[x_1, \dots, x_n]$, $f \neq 0$: $f = u p_1^{e_1} \cdots p_r^{e_r}$.
- I primi minimali sopra f sono $P_1 = (p_1), \dots, P_r = (p_r)$.
- $\mathrm{ht} P_i = 1 \quad \forall i = 1, \dots, r$

SOL Se P primo contiene f, contiene uno dei p_i e quindi $P \supseteq P_i$.
Siccome p_i irrid $\Rightarrow p_i$ primo (in UFD), i P_i sono i primi minimali.
$\mathrm{ht} P_i = \dim K[x_1, \dots, x_n] - \dim\left(\frac{K[x_1, \dots, x_n]}{P_i}\right) = n - \mathrm{trdeg}_K \mathrm{Frac}\left(\frac{K[x_1, \dots, x_n]}{P_i}\right) = n - (n-1) = 1$
($\mathrm{trdeg}_K \mathrm{Frac} B = \dim B$, $\mathrm{ht} P = \dim B_P = \dim B - \dim(B/P)$)

ES K campo, A K-alg. fin. gen dominio,
$B \cong K[x_1, \dots, x_n] \subseteq A$ finita, $f \in A \setminus \{0\}$.
- C'è un numero finito di primi minimali sopra f.
  Fissiamone uno P.
- Dimostrare che $\exists g \in A \setminus \{0\}$ t.c. PA_g è l'unico primo minimale sopra $(f)A_g$
  Questo succede $g \in P_2, \dots, P_r$ (altri primi minimali) e $g \notin P$
  $g_2 \in P_2 \setminus P$ (se non esistesse $P_2 \subseteq P$, assurdo per minimalità)
  $g_i \in P_i \setminus P$ e prendiamo $g = \prod_{i=2}^{r} g_i \notin P$
  [A_g = aperto $D(g)$ = "$g \neq 0$" non contiene $P_2, \dots, P_r$]
- Supponiamo che in A_g, $\mathrm{ht} PA_g = 1$. Allora $\mathrm{ht} P = 1$
  $A_P = (A_g)_{PA_g}$ perché $g \notin P$.
  $\Rightarrow \mathrm{ht} P = \dim A_P = \dim (A_g)_{PA_g} = \mathrm{ht} PA_g = 1$
- $(f) \subseteq P$ e P è l'unico primo minimale $\Rightarrow \sqrt{(f)} = P$
  perché $\sqrt{(f)} = \bigcap_{f \in Q \text{ primo min.}} Q = P$

- A — $\mathrm{Frac}A = L$ — $\mathfrak{p}$
  B — $\mathrm{Frac}B = F$ — $N_{L/F}(\mathfrak{p}) =: \mathfrak{p}_0$

  Dimostriamo che $\mathfrak{p}_0 \in B$.
  Polinomio minimo di $\mathfrak{p}$: c'è un polinomio monico a coeff. in B che annulla $\mathfrak{p}$, $\mathfrak{p}^n + \tilde{b}_{n-1}\mathfrak{p}^{n-1} + \dots + \tilde{b}_0 = 0$
  $q(t) = t^n + \tilde{b}_{n-1}t^{n-1} + \dots + \tilde{b}_0 \in B[t]$
  Poiché B è UFD, fattorizzo il polinomio $q(t) = q_1(t)\cdots q_h(t)$ con q_i monico. $0 = q(\mathfrak{p}) = q_1(\mathfrak{p})\cdots q_h(\mathfrak{p}) \Rightarrow$ c'è un polinomio monico in $B[t]$ irriducibile che si annulla in $\mathfrak{p}$
  $\mathfrak{p}_0 = N_{L/F}(\mathfrak{p}) = [(-1)^m b_0]^{[L:F(\mathfrak{p}_0)]} \in B$ $\quad t^m + b_{m-1}t^{m-1} + \dots + b_0$
- Chiamiamo $Q = P \cap B$ Dimostriamo che $Q = \sqrt{(\mathfrak{p}_0)}$
  * Mostriamo che $\mathfrak{p}_0 \in B$. Basta $b_0 \in Q$
  $B \ni b_0 = -\mathfrak{p}^m - b_{m-1}\mathfrak{p}^{m-1} - \dots - b_1\mathfrak{p} \in (\mathfrak{p}) \subseteq P \Rightarrow b_0 \in Q$
  $\Rightarrow \sqrt{(\mathfrak{p}_0)} \subseteq Q$
  * Viceversa, se $y \in Q \subseteq P = \sqrt{(\mathfrak{p})}$, posso scrivere $y^N = \mathfrak{p}\cdot h$ per qualche $N \geq 1$, $h \in A$
  $\Rightarrow N_{L/F}(y)^N = N_{L/F}(\mathfrak{p})\, N_{L/F}(h) \in (\mathfrak{p}_0)$
  ($y \in L$, $\mathfrak{p} \in F$, N; $\mathfrak{p}_0$; $h \in B$)
  $\Rightarrow y \in \sqrt{(\mathfrak{p}_0)} \Rightarrow Q \subseteq \sqrt{(\mathfrak{p}_0)}$
- $\dim A/\mathfrak{p} = \dim B/Q$ perché sono in un'est. intera $B \subseteq A$ intera
  "$\dim A$" n - $\mathrm{ht}\,\mathfrak{p}$
  "$\dim B$" $n-1$ - $\mathrm{ht}\,Q$

  Quindi $\mathrm{ht}\,\mathfrak{p} = 1$ □

Hensel e i p-adici

① $\sqrt{1+X} = \sum_{n=0}^{+\infty} \binom{1/2}{n} X^n = 1 + \frac{1}{2}X - \frac{1}{8}X^2 + \frac{1}{16}X^3 + \dots$

Hensel: $R = K[[X]]$ K campo, $\mathrm{char}K \neq 2$
completamento di $K[X]$ rispetto a $I = (X)$
Mi chiedo se in R c'è una radice di $p(t) = t^2 - (1+X)$
Hensel: se c'è $r_0 \in R$ t.c. $p(r_0) \in (X)$ e $p'(r_0) \notin (X)$,
allora $\exists r \in R$ t.c. $p(r) = 0$ e $r \equiv r_0 \bmod (X)$
Se prendo $r_0 = 1$, $p(r_0) = -X \in (X)$, $p'(r_0) = 2 \notin (X)$ (perché $2 \neq 0$)
$r_0 = 1$, $r_1 = r_0 - p(r_0)/p'(r_0) = 1 - (-X)/2 = 1 + \frac{X}{2}$
$r_2 = 1 + \frac{X}{2} - \frac{p(1+\frac{X}{2})}{p'(1+\frac{X}{2})} = 1 + \frac{X}{2} - \frac{1+X+\frac{X^2}{4} - (1+X)}{2(1+\frac{X}{2})} = 1 + \frac{X}{2} - \frac{X^2}{8}\cdot\frac{1}{1+\frac{X}{2}} =$
$= 1 + \frac{X}{2} - \frac{X^2}{8}\left(1 - \frac{X}{2} + O(X^2)\right) \equiv 1 + \frac{X}{2} - \frac{X^2}{8} + \frac{X^4}{16} \bmod (X)^4$

② Se $\mathrm{char}K = 2$, $1+X = \mathfrak{p}^2(X)$ non ha soluzione:
se $f(X) = \sum_{n\geq 0} c_n X^n$ ho $f(X)^2 = \sum_{n\geq 0} c_n^2 X^{2n}$ ha solo potenze pari di X

③ L'ipotesi $f'(x_0) \notin \mathfrak{M}$ è necessaria

- Unicità: $R = \mathbb{Z}_p$, $\mathfrak{M} = (p)$, $f(x) = x(x-p)$, $x_0 = 0$
  $f(x)$ ha due radici congrue fra loro mod p
  $f'(x) = 2x - p$, $f'(0) = -p \in \mathfrak{M}$
- Esistenza: $R = \mathbb{Z}_p$, $\mathfrak{M} = (p)$, $f(x) = x^2 - p$, $x_0 = 0$
  $f(x)$ non ha radici in $\mathbb{Z}_p$: $\forall y \in \mathbb{Z}_p$ $v(y^2) = 2v(y)$ è pari
  quindi $y \neq p$ perché $v(p) = 1$
  $f'(0) = 0 \in \mathfrak{M}$

④ Dimostreremo che $\binom{1/2}{n} \in \mathbb{Q}$ ha denominatore una potenza di 2
(formulaz. alternativa: $\forall p \neq 2$, $v_p\left(\binom{1/2}{n}\right) \geq 0$)
Consideriamo $\binom{x}{n} : \mathbb{Q}_p \longrightarrow \mathbb{Q}_p$, dove $\mathbb{Q}_p = \operatorname{Frac} \mathbb{Z}_p$, $\operatorname{char} \mathbb{Q}_p = 0$
Vediamo che i polinomi $\in \mathbb{Q}_p[x]$ danno funzioni continue
Gli intorni di 0 in $\mathbb{Z}_p$ sono $\{x \in \mathbb{Z}_p \mid v(x) \geq n\} = \{\ker : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p/(p^n)\}$
Dato $q \in \mathbb{Q}_p$, una base di intorni è $\{q + x \mid x \in \mathbb{Z}_p, v(x) \geq n\}$
Questa topologia è indotta da una metrica

$$d(q_1, q_2) := p^{-v(q_1 - q_2)}$$

$$B(0, r) = \{x \mid d(x,0) < r\} = \{x \mid p^{-v(x)} < r\} = \{x \mid -v(x) \log p < \log r\}$$
$$= \left\{x \mid v(x) > -\frac{\log r}{\log p}\right\} \qquad r < 1$$

Prendiamo una $h(x) = \dfrac{\sum_{i=0}^{N} a_i x^i}{p^k}$ con $a_i \in \mathbb{Z}_p$
$\mathbb{Z}_p$ è un DVR con id. mass. $(p) \longrightarrow \operatorname{Frac} \mathbb{Z}_p = \mathbb{Z}_p\left[\frac{1}{p}\right]$
Sia $x_0 \in \mathbb{Q}_p$, un intorno $V = \{y \mid v(y - h(x_0)) \geq N\}$ dell'immagine.
Devo costruire un intorno U di x_0 t.c. $h(U) \subseteq V$
Prendo $U = \{z \mid v(z - x_0) \geq N + k\}$: allora $\forall u \in U$

$$\sum_{i=0}^{N} a_i u^i \equiv \sum_{i=0}^{N} a_i x_0^i \mod p^{N+k}$$

$$\Longrightarrow p^k h(u) \equiv p^k h(x_0) \mod p^{N+k}$$
$$\iff v(p^k(h(u) - h(x_0))) \geq N + k \iff k + v(h(u) - h(x_0)) \geq N + k \iff h(u) \in V$$

Oss $\mathbb{Z} \subset \mathbb{Z}_p$ è denso, cioè $\forall x \in \mathbb{Z}_p$ $\forall N$ $\exists n \in \mathbb{Z}$ t.c.
$n \in \{y \mid v(x - y) \geq N\} \iff v(x - n) \geq N \iff x \equiv n \mod p^N$
Dato x, calcolo $\bar{x} \in \mathbb{Z}_p/p^N\mathbb{Z}_p \simeq \mathbb{Z}/p^N\mathbb{Z}$, allora c'è
un n con la stessa classe di resto.

Oss $v_p : \mathbb{Q}_p \setminus \{0\} \longrightarrow \mathbb{Z}$ è continua
$x \in \mathbb{Q}_p \setminus \{0\}$, $v_p(x) = n$ $\quad v(x + p^{n+1}\mathbb{Z}_p) = n$

Dim che $v_p\left(\binom{1/2}{n}\right) \geq 0$ $\forall p \neq 2$
$p \neq 2 \Longrightarrow \frac{1}{2} \in \mathbb{Z}_p$
Per densità, $\exists \{x_k\} \subset \mathbb{Z}$ t.c. $\lim_{k \to \infty} x_k = \frac{1}{2}$. Allora

$$v_p\left(\tfrac{1/2}{n}\right) = v_p\left(\lim_{k \to \infty} \binom{x_k}{n}\right) = \lim_{k \to \infty} \underbrace{v_p\left(\binom{x_k}{n}\right)}_{\geq 0} \geq 0$$

perché $v_k(\text{intero}) \geq 0$

Oss Se $q \in \mathbb{Q}$, $v_p(q) \geq 0 \Longrightarrow v_p\left(\binom{q}{n}\right) \geq 0$

⑤ Sollevamento di Teichmüller

$\mathbb{Z}_p \xrightarrow{\pi} \mathbb{Z}_p/(p) \simeq \mathbb{F}_p$

ES Esiste un unico omomorfismo $\omega: \mathbb{F}_p^\times \longrightarrow \mathbb{Z}_p^\times$ tale che $\pi \circ \omega = id_{\mathbb{F}_p}$

SOL Oss $\mathrm{Im}\omega = \{x \in \mathbb{Z}_p^\times \mid x^{p-1} = 1\}$

Sia $f(x) = x^{p-1} - 1$. Cerco delle radici in $\mathbb{Z}_p$ applicando Hensel.

Dato $\bar{a} \in \mathbb{F}_p^\times$ e $a \in \mathbb{Z}_p$ t.c. $\pi(a) = \bar{a}$

$a^{p-1} - 1 \in (p) \iff \bar{a}^{p-1} - 1 = 0$, che è sempre vero

Si ha $f'(a) = (p-1)a^{p-2} \notin (p)$

Per Hensel, $\exists!\ \omega(a) \in \mathbb{Z}_p$ t.c. $f(\omega(a)) = 0$, $\omega(a) \equiv \bar{a} \bmod p$

Questa costruzione non dipende dalla scelta di a che solleva $\bar{a}$

Oss $f(x)$ ha esattamente $p-1$ radici in $\mathbb{Z}_p$, a 2 a 2 distinte mod p

Siano ora $\bar{a}, \bar{b} \in \mathbb{F}_p^\times$

$$\begin{cases} \omega(ab) \equiv \bar{a}\bar{b} \bmod p \\ \omega(ab)^{p-1} = 1 \end{cases} \qquad \begin{cases} \omega(a)\omega(b) \equiv \bar{a}\bar{b} \bmod p \\ \omega(a)^{p-1}\omega(b)^{p-1} = 1 \end{cases}$$

$\Longrightarrow \omega(ab) = \omega(a)\omega(b)$

⑥ Un giochino

Sia $S_k = \sum_{n=1}^{k} 2^n/n$. Dimostrare che $v_2(S_k) \longrightarrow +\infty$

FATTO $-\log_p(1-x) := \sum_{n \geq 1} \frac{x^n}{n}$ converge $\forall x \in p\mathbb{Z}_p$

Inoltre $\log(ab) = \log(a) + \log(b)$

$\log_p((1-x)(1-y)) = \log_p(1-x) + \log_p(1-y)$ $\forall x, y \in p\mathbb{Z}_p$

Prendo $p=2$, $x=y=2$ e trovo

$0 = \log_2(1) = \log_2(-1) + \log_2(-1) \Longrightarrow \log_2(-1) = 0$

$-\log_2(-1) = \sum_{n \geq 1} 2^n/n = 0 \Longrightarrow$ somme parziali tendono a 0

$\Longrightarrow v_2(S_k) \longrightarrow +\infty$

Lemma A anello Noetheriano, M A-mod fin.gen, $I \lhd A$, M^n I-filtrazione. Sono equivalenti:
(i) $B(M)$ è fin. gen. come $B_I A$-mod
(ii) M^n è I-stabile.

DIMOSTRAZIONE

Oss
- M^n è fin.gen su A (A Noeth, M fin.gen.)
- Poniamo
$$M^*_n = M^0 \oplus M^1 \oplus \dots \oplus M^n \oplus IM^n \oplus I^2M^n \oplus \dots \subseteq B(M)$$
è un sotto-$B_I A$-mod:
$I^k(M^*_n)_d \subseteq (M^*_n)_{k+d}$
se $k+d \le n$, $(M^*_n)_{k+d} = M^{k+d}$
se $k+d > n$, $(M^*_n)_{k+d} = I^{k+d-n}M^n$
se $d > n$ $I^k((M^*_n)_d) = I^k(I^{d-n}M^n)$
se $d \le n$ $I^k M^d \subseteq I^{k+d-n}M^n$ segue dalla def. di I-filtrazione: $I^k M^d = I^{k+d-n} I^{n-d} M^d \subseteq I^{k+d-n}M^n = (M^*_n)_{k+d}$
Inoltre M^*_n è fin. gen. come $B_I A$-mod, prendendo come generatori quelli di $M^0, \_, M^n$ come A-mod.
($B_I A \cdot M^n \supseteq I^k M^n = M^{n+k}$)
Abbiamo anche $\bigcup_{n\ge 0} M^*_n = B(M)$
- La successione M^*_n stabilizza $\iff$ la filtrazione è I-stabile:
$M^*_{n_0+r} = M^*_{n_0}$ $\forall r \ge 0 \iff \forall i = 1, \_, r$ vale $M^{n_0+i} = I^i M^{n_0}$
$M^*_{n_0} = M^0 \oplus \dots \oplus M^{n_0} \oplus IM^{n_0} \oplus \dots \oplus I^r M^{n_0} \oplus \dots$
$M^*_{n_0+r} = M^0 \oplus \dots \oplus M^{n_0} \oplus M^{n_0+1} \oplus \dots \oplus M^{n_0+r} \oplus IM^{n_0+r} \oplus \dots$

(i) $\Rightarrow$ (ii) Se $B(M)$ è fin gen su $B_I A$, che è Noeth siccome A è Noeth, $B(M)$ è Noeth $\Rightarrow$ $\{M^*_n\}$ stabilizza $\Rightarrow$ la filtrazione è stabile

(ii) $\Rightarrow$ (i) Se la filtrazione è I-stabile, $\{M^*_n\}$ stabilizza e quindi $B(M) = \bigcup_{n\ge 0} M^*_n = M^*_{n_0}$ che è fingen come $B_I A$-mod. □

DIMOSTRAZIONE (A-R)

(i) $M' \cap M^n$ è una I-filtrazione:
$$I(M' \cap M^n) \subseteq IM' \cap IM^n \subseteq M' \cap M^{n+1}$$
Inoltre $B(M') = \bigoplus_{n\ge 0} (M' \cap M^n) \subseteq \oplus M^n = B(M)$ è un sotto-$B_I A$-mod:
siccome M^n è I-stabile, $B(M)$ è fin gen su $B_I A$ Noeth
$\Rightarrow B(M')$ è fin gen $\Rightarrow$ la filtrazione su M' è I-stabile

(ii) Prendiamo $M^n = I^n M$. Per (i), $I^n M \cap M'$ è I-stabile, cioè
$\exists n_0$ t.c. $I^r(I^{n_0} M \cap M') = I^{n_0+r} M \cap M'$ $\forall r \ge 0$

(iii) $I^n M \cap M'$ e $I^n M'$ sono I-stabili: quindi hanno differenza limitata e in particolare inducono la stessa topologia □

Teorema dell'intersezione di Krull

Sia (A,P) Noetheriano locale, $I \lhd A$, $I \neq (1)$, M A-mod fin. gen. Vale $\bigcap_{n\geq 0} I^n M = \{0\}$, e in particolare $M \longrightarrow \hat{M}$ è iniettiva.

DIMOSTRAZIONE

Sia $N := \bigcap_{n\geq 0} I^n M$: è un A-sottomod di M

Per Artin-Rees, $\exists n_0$ t.c. $I^{n_0+r} M \cap N = I^r (I^{n_0} M \cap N)$ $\forall r \geq 0$,

cioè $N = I^r N$: prendo $r=1$, osservo $I \subseteq P$ e applico Nakayama $\square$

Lunghezza

Def. A anello comm., M A-mod

- M è semplice se non ammette sottomoduli non banali $(M \neq \{0\})$
- M è di lunghezza finita se è Noetheriano e Artiniano.
  Equivalentemente, se esiste una filtrazione finita
  (*) $0 = M_0 \subsetneq M_1 \subsetneq \dots \subsetneq M_n = M$ t.c. M_i/M_{i-1} sia semplice
- In tal caso, (*) si dice serie di composizione per M e i quozienti semplici M_i/M_{i-1} si dicono fattori di composizione o costituenti di Jordan-Hölder.

Teorema di Jordan-Hölder

Date due serie di composizione

$0 = M_0 \subsetneq M_1 \subsetneq \dots \subsetneq M_m = M$

$0 = N_0 \subsetneq N_1 \subsetneq \dots \subsetneq N_n = M$

si ha $m=n$ e $\{M_i/M_{i-1}\} = \{N_j/N_{j-1}\}$ (insiemi con molteplicità)

Esempio

- $A = K$ campo: lunghezza = dimensione
- $A = \mathbb{Z}$, gruppi abeliani finiti. I moduli semplici sono $\mathbb{Z}/p\mathbb{Z}$ per p primo

$$0 \subsetneq \underbrace{3\mathbb{Z}/6\mathbb{Z}}_{\mathbb{Z}/2\mathbb{Z}} \subsetneq \underbrace{\mathbb{Z}/6\mathbb{Z}}_{\mathbb{Z}/3\mathbb{Z}} \qquad \text{o} \qquad 0 \subsetneq \underbrace{2\mathbb{Z}/6\mathbb{Z}}_{\mathbb{Z}/3\mathbb{Z}} \subsetneq \underbrace{\mathbb{Z}/6\mathbb{Z}}_{\mathbb{Z}/2\mathbb{Z}}$$

$|M| = p_1^{e_1} \cdots p_r^{e_r} \longrightarrow \ell(M) = e_1 + \dots + e_r$

- $A = K[x]$. Un A-mod M è un K-spazio vettoriale + un endomorfismo come K-S.V.
  $K[x] \longrightarrow \mathrm{End}(M)$
  $M = K^2$, x agisce tramite $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$
  $0 \subsetneq \langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rangle \subsetneq M$, entrambi i quozienti sono K con l'endom. identità
- Gruppi non abeliani: se G è un gpp finito, c'è
  $\{e\} \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \dots \trianglelefteq G_n = G$ con G_n/G_{n-1} semplici
  Vale JH: la lunghezza e i quozienti G_i/G_{i-1} non dipendono dalla serie di composizione.

DIMOSTRAZIONE

Per induzione sul minimo m t.c. M ammetta una serie di decomposizione di lungh. m

- $m=0$: $M=\{0\}$
- $m=1$: $0=M_0 \subsetneq M_1 = M$ con $M=M_1/M_0$ semplice
  Ogni serie deve essere $\{0\} \subsetneq M$
- $m \geq 2$: distingo due casi: $M_{m-1}=N_{n-1}$ o $M_{m-1} \neq N_{n-1}$

  Se $M_{m-1}=N_{n-1}$,
  $0=M_0 \subsetneq M_1 \subsetneq \dots \subsetneq M_{m-1}$ è una serie di comp. per M_{m-1} di lung $m-1$
  Allora per hp. ind.
  $0=N_0 \subsetneq N_1 \subsetneq \dots \subsetneq N_{n-1}=M_{m-1}$ deve valere $n-1=m-1 \Rightarrow n=m$
  e avere $\{N_j/N_{j-1}\}_{j=1,\dots,n} \cup \{M/N_{n-1}\} = \{M_i/M_{i-1}\}_{i=1,\dots,m-1} \cup \{M/M_{m-1}\}$

  Se $M_{m-1} \neq N_{n-1}$: sia M_{m-1} sia N_{n-1} sono sottomod massimali,
  quindi $M_{m-1}+N_{n-1}=M$. Sia $K=M_{m-1} \cap N_{n-1}$
  $M/M_{m-1} = M_{m-1}+N_{n-1}/M_{m-1} \simeq N_{n-1}/M_{m-1} \cap N_{n-1} = N_{n-1}/K$
  e similmente $M/N_{n-1} \simeq M_{m-1}/K$
  Inoltre N_{n-1}/K e M_{m-1}/K sono semplici
  Fissiamo una serie di composiz. per K
  $0=K_0 \subsetneq K_1 \subsetneq \dots \subsetneq K_r=K \subsetneq M_{m-1}$
  $0=K_0 \subsetneq K_1 \subsetneq \dots \subsetneq K_r=K \subsetneq N_{n-1}$
  Siccome M_{m-1} ammette una serie di compos. di lungh. $m-1$,
  tutte hanno lungh. $m-1 \Rightarrow r+1=m-1 \Rightarrow r=m-2$
  Guardando la seconda, è una serie di lungh. $r+1=m-1$
  Riapplicando l'ipotesi induttiva, $n-1=r+1=m-1 \Rightarrow m=n$
  Ogni serie di comp. per N_{n-1} ha gli stessi fattori semplici,
  che sono $K_1/K_0, K_2/K_1, \dots, K_r/K_{r-1}, N_{n-1}/K$.
  Allo stesso modo, quelli di M_{m-1} sono
  $K_1/K_0, K_2/K_1, \dots, K_r/K_{r-1}, M_{m-1}/K$
  Le due serie di comp. hanno fattori semplici
  $K_1/K_0, K_2/K_1, \dots, K_r/K_{r-1}, M_{m-1}/K_r, M/M_{m-1}$
  $K_1/K_0, K_2/K_1, \dots, K_r/K_{r-1}, N_{n-1}/K_r, M/N_{n-1}$ □

corollario

(1) Per ogni succ. esatta corta di moduli di lungh. finita
$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$
allora $\ell(M_2)=\ell(M_1)+\ell(M_3)$

(2) In particolare, $\ell(M_1 \oplus M_2)=\ell(M_1)+\ell(M_2)$

(3) Per ogni succ. esatta lunga
$$0 \longrightarrow M_1 \longrightarrow \dots \longrightarrow M_n \longrightarrow 0$$
vale $\sum_{i=1}^{n} (-1)^i \ell(M_i)=0$

DIMOSTRAZIONE

(1) Sia $0=M_{1,0} \subsetneq \dots \subsetneq M_{1,l_1}=M_1$ una serie di comp. per M_1

$0=M_{3,0} \subsetneq \dots \subsetneq M_{3,l_3}=M_3$ una serie di comp. per M_3

Allora $0=M_{1,0} \subsetneq \dots \subsetneq M_{1,l_1}=\pi^{-1}(M_{3,0}) \subsetneq \pi^{-1}(M_{3,1}) \subsetneq \dots \subsetneq \pi^{-1}(M_{3,l_3})$

è una serie di comp. per M_2 di lung. l_1+l_3

(2) $0 \longrightarrow M_1 \longrightarrow M_1 \oplus M_2 \longrightarrow M_2 \longrightarrow 0$ è esatta

(3) $0 \longrightarrow M_1 \xrightarrow{\alpha_1} M_2 \xrightarrow{\alpha_2} M_3 \xrightarrow{\alpha_3} M_4 \longrightarrow 0$

$$\begin{cases} 0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow \alpha_2(M_2) \longrightarrow 0 \\ 0 \longrightarrow \alpha_2(M_2) \longrightarrow M_3 \longrightarrow M_4 \longrightarrow 0 \end{cases} \Rightarrow \begin{array}{l} \ell(M_1)-\ell(M_2)+\ell(\alpha_2(M_2))=0 \\ -\ell(\alpha_2(M_2))+\ell(M_3)-\ell(M_4)=0 \end{array}$$

Per induzione su n □

Funzioni di Hilbert

$A=\bigoplus_{n\geq 0} A_n$ anello graduato Noetheriano, con A_0 artiniano

esempio
- $A=K[x_1,\dots,x_n]$ con la graduazione standard
- (B,m) locale Noetheriano, q ideale m-primario (cioè $\sqrt{q}=m$)

$\mathrm{Gr}_q B=\bigoplus_{n\geq 0} q^n/q^{n+1}$

$$q^a/q^{a+1} \times q^b/q^{b+1} \longrightarrow q^{a+b}/q^{a+b+1}$$

$$q^a \times q^b \longrightarrow q^{a+b} \longrightarrow q^{a+b}/q^{a+b+1}$$

$$\searrow\ q^a/q^{a+1} \times q^b/q^{b+1} \nearrow$$

$\mathrm{Gr}_q B$ è Noetheriano

e $(\mathrm{Gr}_q B)_0 = B/q$ è Artiniano perché è locale e m/q è nilpotente

$$\ell(B/q^n) = \ell(B/q)+\ell(q/q^2)+\dots+\ell(q^{n-1}/q^n)$$

def Sia $M=\bigoplus M_n$ un modulo fin.gen. su $A=\bigoplus A_n$

la serie di Poincaré di M è

$$P_M(t)=\sum_{n\geq 0} \ell_{A_0}(M_n)t^n \in \mathbb{Z}[[t]]$$

ex Ogni singolo M_n è un A_0-mod fin. gen.

ES Ideali massimali delle $\mathbb{Z}$-alg. fin.gen.

(i) Sia K un campo e una $\mathbb{Z}$-alg. fin.gen. Allora $\dim K > 0$

- Per assurdo, sia $\dim K = 0$ e $\varphi: \mathbb{Z}[t_1, \dots, t_n] \twoheadrightarrow K$
  Siccome $\operatorname{char} K = 0$, $\mathbb{Q} \subset K$ e quindi φ si estende a $\psi: \mathbb{Q}[t_1, \dots, t_n] \twoheadrightarrow K$
  Per Zariski, siccome K è $\mathbb{Q}$-alg. fin.gen, $K/\mathbb{Q}$ è un'est. finita.
  Siano $\alpha_i = \psi(t_i)$: generano $K/\mathbb{Q}$ e sono algebrici su $\mathbb{Q}$, quindi ci sono dei polinomi $p_i \in \mathbb{Q}[x]$ monici e irr. t.c. $p_i(\alpha_i) = 0$
  Ho un n° finito di polinomi con un n° finito di coefficienti
  $\Rightarrow \exists N > 1$ t.c. $N p_i \in \mathbb{Z}[x]$ $\forall i \Rightarrow p_i \in \mathbb{Z}[\frac{1}{N}][x]$
  Quindi $K = \mathbb{Z}[\alpha_1, \dots, \alpha_n]$, e ogni α_i è intero su $\mathbb{Z}[\frac{1}{N}] \subseteq \underbrace{\mathbb{Q} \subseteq K}_{\text{intera}}$

  $\Rightarrow 1 \leq \dim \mathbb{Z}[\frac{1}{N}] = \dim K = 0$ ↯

- $\underbrace{\mathbb{Z} \subset \mathbb{Q} \subset K}_{\text{fin.gen come algebra}}$ fingen come algebra ?

Lemma di Artin-Tate Siano $R \subset A \subset B$ con
- R Noetheriano
- B fin.gen. come R-algebra
- B fin gen come A-modulo.

Allora A è fin.gen come R-algebra.

DIMOSTRAZIONE

Fissiamo generatori $\{b_j\}_{j=1,\dots,m}$ di B come A-modulo
e generatori $\{c_i\}$ di B come R-algebra

Scriviamo $c_i = \sum_{j=1}^{m} a_{ij} b_j$ con $a_{ij} \in A$

$b_i b_j = \sum_{k=1}^{m} a_{ijk} b_k$ con $a_{ijk} \in A$ (incluso $i=j$)

Sia $A' := R[a_{ij}, a_{ijk}] \subseteq A$ è un R-alg. fin.gen.

Consideriamo poi $B' := \frac{A'[T_1, \dots, T_m]}{(T_i T_j - \sum a_{ijk} T_k \mid i,j)}$ $\ni 1, \overline{T}_1, \dots, \overline{T}_m$

$$\begin{array}{ccc} R & \hookrightarrow & A \hookrightarrow B \\ & & \uparrow \quad \uparrow \text{(da dim)} \\ & & A' \hookrightarrow B' \end{array}$$

B' è un'est. finita (da dim)

Per induzione sul grado del polinomio, si mostra che ogni elemento $p(\overline{T}_1, \dots, \overline{T}_m) \in B'$ si scrive come comb. lineare di $1, \overline{T}_1, \dots, \overline{T}_m$ a coeff. in A'
$\Rightarrow B'/A'$ est. finita

Posso definire $\psi: B' \to B$, $\overline{T}_i \mapsto b_i$, che è surgettiva perché

L'immagine di ψ è una A'-algebra ($\Rightarrow$ R-algebra) che contiene $b_1, \dots, b_m$
e quindi anche $c_i = \sum_{j=1}^{m} a_{ij} b_j$
$\Rightarrow \operatorname{Im}\psi \supseteq R[c_1, \dots, c_t] = B$

Segue che B è un A'-mod fin.gen e A' è Noetheriano (perché R-alg. fin.gen.)

$A' \subset A \subset B$ (B fin gen come modulo) $\Rightarrow A$ è fin.gen come A'-modulo

$\Rightarrow A$ è fin gen come A'-alg
$\Rightarrow A$ è fingen come R-alg. □

esempio $K \subset K[xy^n \mid n \geq 1] \subset K[x,y]$
$R \quad A \quad B$

A non è una R-alg. fin.gen.: se lo fosse, da certi polinomi
$p_1(x,y), \dots, p_r(x,y)$
$q_i(xy, xy^2, \dots, xy^{n_i})$ $\quad N = \max(n_1, \dots, n_r) \longrightarrow p_i = q_i(xy, \dots, xy^N)$
Allora i generatori sono $xy, xy^2, \dots, xy^N$
Però $xy^{N+1} \notin K[xy, xy^2, \dots, xy^{N+1}]$
Se fosse $xy^{N+1} = q(xy, \dots, xy^{N+1})$, almeno un monomio di q, valutato in $(xy, \dots, xy^{N+1})$ dovrebbe essere xy^{N+1}, ma nessun monomio funziona

Oss A non è neppur Noetheriano: ha la catena
$(xy) \subsetneq (xy, xy^2) \subsetneq \dots \subsetneq (xy, xy^2, \dots, xy^n) \subsetneq \dots$

(ii) Sia M un id. mass. di una $\mathbb{Z}$-alg. fin. gen. A.
Allora A/M è un campo finito

Per (i), $\operatorname{char} A/M = p > 0$
$M' = \ker(\mathbb{Z}[t_1, \dots, t_n] \twoheadrightarrow A \twoheadrightarrow A/M)$ è un id. mass. di $\mathbb{Z}[t_1, \dots, t_n]$ per corrisp.
Siccome $p = 0$ in $\mathbb{Z}[t_1, \dots, t_n]/M \cong A/M$, $p \in M'$
Gli ideali di $\mathbb{Z}[t_1, \dots, t_n]$ che contengono (p) sono in bigez. con quelli di $\mathbb{Z}[t_1, \dots, t_n]/(p) \cong \mathbb{F}_p[t_1, \dots, t_n]$
In particolare, A/M è un quoziente di $\mathbb{F}_p[t_1, \dots, t_n]$
$\Rightarrow$ A/M è una $\mathbb{F}_p$-alg fin.gen. e campo
Zariski $\Rightarrow$ A/M è un'est. finita di $\mathbb{F}_p \Rightarrow$ è un campo finito

Oss $B = \mathbb{Z}[t_1, \dots, t_n]$ è un anello regolare
- $\dim B = n+1$
- id. mass. sono l'immagine inversa in $\mathbb{Z}[x_1, \dots, x_n]$ di un id. mass. in $\mathbb{F}_p[x_1, \dots, x_n] \supset \overline{m} = (\overline{f}_1, \dots, \overline{f}_n)$ $\quad ht\, \overline{m} = n$
$\Longrightarrow m = (p, f_1, \dots, f_n)$ ha $n+1$ generatori $\quad ht\, m = n+1$
che è più forte che essere regolare

ES $A = \mathbb{R}[x,y]/(x^2+y^2+1)$ è PID ma non euclideo

SOL Per assurdo, sia Euclideo con grado d

- Gli el. di grado min. sono le unità $A^\times$
- Fra gli el. di grado > del minimo, questo "2° minimo" è realizzato da un el. irr. p
- Divisione euclidea per p: $\forall a \in A \ \exists q \in A, r \in A$ t.c. $a = pq + r$ con $r = 0$ o $d(r) < d(p)$

la condizione $d(r) < d(p)$ vuol dire $r \in A^\times$

$\Longrightarrow A/(p) =$ immagine di $A^\times$ tutti in $A/(p)$

- Abbiamo visto $p = ax + by + c$ con $(a,b) \neq (0,0)$ e che $A/(p) \simeq \mathbb{C}$
- Per concludere, basta mostrare che $A^\times = \mathbb{R}^\times$, perché $\mathbb{R}^\times$ tutti non si sorgetta su $\mathbb{C}$
- Prendiamo $u(x,y) \in A^\times$ $\quad u_0(x) + y u_1(x)$

$$\begin{array}{c} A \\ | \\ \mathbb{R}[x] \end{array}$$

Osservo che $\sigma : A \longrightarrow A$ ("generatore del gpp. Galois")

$x \longmapsto x$, $y \longmapsto -y$

è un automorfismo. Allora $\sigma(u) \in A^\times$

quindi $u \cdot \sigma(u) = N_{\mathbb{R}(x,y)/\mathbb{R}(x)}(u) \in A^\times$

$$(u_0 + y u_1)(u_0 - y u_1) = u_0^2 - y^2 u_1^2 = \underbrace{u_0^2 - (-x^2-1)u_1^2}_{v(x)} \in A^\times$$

$$v(x) \cdot [w_0(x) + y w_1(x)] = 1 \Longrightarrow \begin{cases} v(x) \cdot w_0(x) = 1 \\ v(x) \cdot y w_1(x) = 0 \end{cases}$$

$\Longrightarrow v(x) \in \mathbb{R}[x]^\times = \mathbb{R}^\times \Longrightarrow \deg u_0 = 0, \ u_1 = 0$

Quozienti di anelli graduati

$A = \oplus A_n$ graduato.

Un ideale $I \lhd A$ si dice omogeneo se $I = \bigoplus_{i\geq 0} (I \cap A_i)$

o equivalentemente se è generato da dei omogenei

In tal caso

$$A/I \simeq \oplus A_n/I \simeq \oplus \left(A_n/A_n \cap I\right) \text{ è graduato:}$$

se chiamo $\overline{A}_n = A_n/A_n \cap I$, ho $A/I \simeq \oplus \overline{A}_n$

e $\overline{A}_n \times \overline{A}_m \longrightarrow \overline{A}_{n+m}$ (si controlla risalendo in A)

Teorema Sia $A_+ = (x_1, \dots, x_s)$ l'ideale positivo, con gli x_i omogenei, $\deg x_i = k_i$.
Esiste $f(t) \in \mathbb{Z}[t]$ t.c.

$$p_M(t) = \frac{f(t)}{\prod_{i=1}^{s}(1-t^{k_i})} \in \mathbb{Z}[[t]]$$

DIMOSTRAZIONE

Per induzione su s

- $s=0$. $A_+ = (0)$, cioè $A = A_0$ è Artiniano

  $M = \oplus M_n$ è fin gen su $A = A_0$ da dei omogenei

  Se questi generatori sono tutti di grado $\leq N$, $M = \bigoplus_{n\leq N} M_n$

  $\Longrightarrow p_M(t) \in \mathbb{Z}[t]$ è una somma finita

- $s \geq 1$: consideriamo la mult. per x_s:

(*) $0 \longrightarrow K_n \longrightarrow M_n \xrightarrow{\cdot x_s} M_{n+k_s} \longrightarrow L_{n+k_s} \longrightarrow 0$ è esatta

con $K_n = \ker(\cdot x_s)$ e $L_{n+k_s} = \operatorname{coker}(\cdot x_s)$, che sono A_0-moduli

Sia $K := \bigoplus_{n\geq 0} K_n$ e $L := \bigoplus_{n\geq 0} L_n$, che sono A-moduli

Da (*), otteniamo $\forall n$

$$\ell(K_n)t^{n+k_s} + \ell(M_{n+k_s})t^{n+k_s} = \ell(M_n)t^{n+k_s} + \ell(L_{n+k_s})t^{n+k_s}$$

Sommando su $n \in \mathbb{Z}$ trovo:

$$t^{k_s}\left(\sum_{n\in\mathbb{Z}} \ell(K_n)t^n\right) + p_M(t) = t^{k_s} p_M(t) + p_L(t)$$

$$\Longrightarrow (1-t^{k_s})p_M(t) = p_L(t) - t^{k_s} p_K(t)$$

Oss chiave - x_s è 0 su K, è 0 su L perché

$$\underbrace{M_{n+k_s}/x_s M_n}_{L_{n+k_s}} \xrightarrow{\cdot x_s} \underbrace{M_{n+2k_s}/x_s M_{n+k_s}}_{L_{n+2k_s}} \quad \text{è zero}$$

Quindi K, L sono $A/(x_s)$-moduli, che è graduato con ideale positivo gen da $(\overline{x}_1, \dots, \overline{x}_{s-1})$.

Per induzione, $p_L(t) = \frac{f_L(t)}{\prod_{i=1}^{s-1}(1-t^{k_i})}$ e $p_K(t) = \frac{f_K(t)}{\prod_{i=1}^{s-1}(1-t^{k_i})}$ dove $f_L, f_K \in \mathbb{Z}[t]$

$$p_M(t) = \frac{p_L(t) - t^{k_s} p_K(t)}{(1-t^{k_s})} = \frac{f_M(t)}{\prod_{i=1}^{s}(1-t^{k_i})}$$

□

Def $d(M) = $ ordine di polo di $p_M(t)$ in $t=1$ $=$

$$= \inf\{k \geq 0 \mid \lim_{t\to 1} |(1-t)^k p_M(t)| < +\infty\}$$

Oss $d(M) \leq s$: infatti

$$\lim_{t\to 1} \left|(1-t)^s \frac{f(t)}{\prod_{i=1}^{s}(1-t^{k_i})}\right| < +\infty$$

Oss Se $x_s \in A_{k_s}$ è un el. omogeneo di grado k_s e se $\cdot x_s$ è iniettiva, allora

$$P_M(t) = P_{M/x_sM}(t)/(1-t^{k_s})$$

corollario A graduato Noetheriano, A_0 Artiniano, M A-mod graduato fin gen, $A_+ = (x_1, \dots, x_s)$, $\deg x_i = 1$. Allora la funzione $n \longmapsto \ell(M_n)$ coincide, per $n \gg 1$, con un polinomio di grado $d(M)-1$.

DIMOSTRAZIONE

$$\sum_{n\geq 0} \ell(M_n) t^n = \frac{f(t)}{(1-t)^s} = \frac{g(t)}{(1-t)^{d(M)}} \quad \text{dove } g(t) \in \mathbb{Z}[t],\ g(1) \neq 0$$

Scrivo $g(t) = a_0 + a_1 t + \dots + a_k t^k$

Sviluppiamo $(1-t)^{-d(M)} = \sum_{n\geq 0} \binom{-d}{n} (-t)^n$

$$\binom{-d}{n} = \frac{(-d)(-d-1)\cdots(-d-(n-1))}{n!} = (-1)^n \frac{(d+(n-1))\cdots(d)}{n!} = (-1)^n \binom{d+n-1}{n} = (-1)^n \binom{d+n-1}{d-1}$$

Quindi $\sum_{n\geq 0} \ell(M_n) t^n = (a_0 + \dots + a_k t^k) \sum_{n\geq 0} \binom{d+n-1}{d-1} t^n$

$$\ell(M_n) = \sum_{h=0}^{n} a_h \binom{d+(n-h-1)}{d-1} \underset{\text{se } n \geq k}{=} \sum_{h=0}^{k} a_h \binom{d+n-h-1}{d-1}$$

è un polinomio, di grado $\leq d-1$.

Per controllare che il grado sia $d-1$, calcolo il coeff. di n^{d-1}:

$$\sum_{h=0}^{k} a_h \cdot \frac{1}{(d-1)!} = \frac{1}{(d-1)!} g(1) \neq 0$$

□

Oss Il polinomio che dà $\ell(M_n)$ è a coefficienti razionali

def La funzione di Hilbert di M è la funzione $n \longmapsto \ell(M_n)$
Il polinomio di Hilbert è il polinomio che coincide con questa per n grande.

Oss $\mathrm{Int}(\mathbb{Z}) = \{ p(x) \in \mathbb{Q}[x] \mid p(\mathbb{Z}) \subset \mathbb{Z} \}$

I polinomi $\binom{x}{n}$ sono in $\mathrm{Int}(\mathbb{Z})$:

$\mathrm{Int}(\mathbb{Z})$ è uno $\mathbb{Z}$-modulo libero e $\{\binom{x}{n}\}_{n\in\mathbb{N}}$ ne è una base.

- Sia $\Delta : \mathrm{Int}(\mathbb{Z}) \longrightarrow \mathrm{Int}(\mathbb{Z})$ la derivata discreta
  $p(x) \longrightarrow p(x+1) - p(x)$
  che fa calare il grado di 1
  $\Delta\binom{x}{n} = \binom{x+1}{n} - \binom{x}{n} = \binom{x}{n-1}$ se $x \in \mathbb{N}$
- $\{\binom{x}{n}\}_{n\in\mathbb{N}}$ sono una base di $\mathbb{Q}[x]$, perché sono triangolari rispetto alle potenze di x
- $p(x) \in \mathrm{Int}(\mathbb{Z})$: $p(x) = \sum_{i=0}^{n} a_i \binom{x}{i}$, $a_i \in \mathbb{Q}$
  $a_0 = p(0) \in \mathbb{Z}$
  $\Delta p(x) = \sum_{i=0}^{n} a_i \Delta\binom{x}{i} = \sum_{i=1}^{n} a_i \binom{x}{i-1}$ $\quad a_1 = (\Delta p(x))(0) \in \mathbb{Z}$
  e in generale $a_i = (\Delta^i p(x))(0) \in \mathbb{Z}$
- Trovare formula per $\sum_{i=0}^{n} i^2 = q(n)$
  $q(n+1) - q(n) = (n+1)^2$
  $(\Delta q)(n) = (n+1)^2 = 2\binom{n}{2} + 3\binom{n}{1} + \binom{n}{0}$
  $\Longrightarrow q(n) = 2\binom{n}{3} + 3\binom{n}{2} + \binom{n}{1}$

Teoria della dimensione via funzioni di Hilbert

Sia $(A, \mathfrak{m})$ Noetheriano locale, q un ideale $\mathfrak{m}$-primario
(cioè $\sqrt{q} = \mathfrak{m}$, cioè $\exists r \geq 0$ t.c. $\mathfrak{m}^r \subseteq q$, cioè $\mathfrak{m}$ è minimale sopra q)
$\mathrm{Gr}_{\mathfrak{m}} A = \bigoplus_{n \geq 0} \mathfrak{m}^n / \mathfrak{m}^{n+1}$, $\mathrm{Gr}_q A = \bigoplus_{n \geq 0} q^n / q^{n+1}$

Ci interessa $\ell(A/\mathfrak{m}^n) = \ell(A/\mathfrak{m}) + \ell(\mathfrak{m}/\mathfrak{m}^2) + \dots + \ell(\mathfrak{m}^{n-1}/\mathfrak{m}^n)$

Oss $0 \longrightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1} \longrightarrow A/\mathfrak{m}^{n+1} \longrightarrow A/\mathfrak{m}^n \longrightarrow 0$ esatta
$\ell(A/\mathfrak{m}^{n+1}) = \ell(A/\mathfrak{m}^n) + \ell(\mathfrak{m}^n/\mathfrak{m}^{n+1})$

Come mai le lunghezze sono finite?
- $A/\mathfrak{m} = A$-mod su cui $\mathfrak{m}$ agisce banalmente
$= (A/\mathfrak{m})$-mod : come $(A/\mathfrak{m})$-mod è di lungh. finita
$\{\text{sotto-}A\text{-mod di } A/\mathfrak{m}\} = \{\text{sotto-}A/\mathfrak{m}\text{-mod di } A/\mathfrak{m}\}$
- $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ è un A-mod su cui $\mathfrak{m}$ agisce banalmente
$= A/\mathfrak{m}$-mod $= A/\mathfrak{m}$-sp. vett. di dim. finita
perché $\mathfrak{m}^n$ ha un n° finito di generatori

Teorema Sia M un A-mod fin.gen e $\{M^n\}$ una q-filtrazione stabile su M.
(i) M/M^n ha lunghezza finita $\forall n$
(ii) $\ell(M/M^n)$ coincide con un polinomio $g(n)$ per ogni $n \gg 0$
e $\deg g(n) \leq$ # generatori dell'ideale q.
(iii) Il grado e il termine di testa di g non dipendono dalla filtrazione.

DIMOSTRAZIONE
$\mathrm{Gr}(M) := \bigoplus_{n \geq 0} M^n/M^{n+1}$ è un mod graduato su $\mathrm{Gr}_q A$
(perché M^n è una q-filtrazione)
Vediamo che è fingen: siccome la filtrazione è stabile,
$\exists n_0$ t.c. $M^{n_0+r} = q^r M^{n_0}$ $\forall r \geq 0$ e in particolare
$q^r \times M^{n_0} \longrightarrow\!\!\!\rightarrow M^{n_0+r} \longrightarrow\!\!\!\rightarrow M^{n_0+r}/M^{n_0+r+1}$
ed inoltre $q^{r+1} \cdot M^{n_0} = M^{n_0+r+1}$ va in 0
$q^r \cdot M^{n_0+1} = M^{n_0+r+1}$ va in 0
$\longrightarrow$ ho $q^r/q^{r+1} \times M^{n_0}/M^{n_0+1} \longrightarrow\!\!\!\rightarrow M^{n_0+r}/M^{n_0+r+1}$

$\Longrightarrow \bigoplus_{n \leq n_0} M^n/M^{n+1}$ genera $\bigoplus_{n \geq 0} M^n/M^{n+1}$ su $\mathrm{Gr}_q A$

Ogni M^n è fingen (sottomod di M, fin gen su A noeth).
Le classi dei generatori di $M^0, M^1, \dots, M^{n_0}$ in $M^0/M^1, M^1/M^2, \dots, M^{n_0}/M^{n_0+1}$
sono una famiglia finita di generatori del modulo $\mathrm{Gr}(M)$
Inoltre M^n/M^{n+1} è fingen su A/q (ex),
quindi è fin gen su $\mathrm{Gr}_q A$

(i) $\ell(M/M^n) = \ell(M/M^1) + \ell(M^1/M^2) + \dots + \ell(M^{n-1}/M^n)$ è finita

(ii) $\ell(M/M^n) = \sum_{i=0}^{n-1} \ell(M^i/M^{i+1})$, e sappiamo che $\exists i_0$ e un polinomio $h(i) \in \mathbb{Q}[i]$ t.c. $\ell(M^i/M^{i+1}) = h(i)\ \forall i \geq i_0$

Allora $\ell(M/M^n) = \underbrace{\sum_{i=0}^{i_0} (\ell(M^i/M^{i+1}) - h(i))}_{\text{costante in } n} + \underbrace{\sum_{i=0}^{n-1} h(i)}_{\text{è un pol. in } n \text{ con deg} = \deg h + 1}$

$\deg h \leq$ (#generatori dell'ideale positivo di $\mathrm{Gr}_q A$) -1

$\mathrm{Gr}_q A = A/q \oplus \underbrace{q/q^2 \oplus q^2/q^3 \oplus \dots}_{(\mathrm{Gr}_q(A))_+}$, generato da q/q^2 : per generare q/q^2 bastano le classi dei generatori di q (di grado 1)

$\Rightarrow \ell(M/M^n)$ è un polinomio per $n \geq i_0$ di grado $\leq$ #generatori di q

(iii) Sia N^n un'altra filtrazione stabile : $\exists n_0$ t.c.

$$M^{n+2n_0} \subseteq N^{n+n_0} \subseteq M^n$$

$$\Rightarrow M/M^n \twoheadleftarrow M/N^{n+n_0} \twoheadleftarrow M/M^{n+2n_0}$$

$$\ell(M/M^n) \leq \ell(M/N^{n+n_0}) \leq \ell(M/M^{n+2n_0})$$

$$g_M(n) \leq g_N(n+n_0) \leq g_M(n+2n_0)$$

Dividendo per $n^{\deg g_M}$, passando al limite per $n \to +\infty$

coeff. dom di $g_M \leq$ coeff. dom. di $g_N \leq$ coeff. dom. di g_M □

Es A dominio Noetheriano, $p \in A$ primo.
Se $A[\frac{1}{p}] = B$ è un UFD, allora A è un UFD.

Sol Sia $x \in A$ irriducibile. Vediamo che $x \in B$ è un'unità o irr.

Se $\frac{x}{1} = \frac{a}{p^n} \cdot \frac{b}{p^m} \Rightarrow p^{n+m} x = ab \Rightarrow p \mid a : a = pa_1$

$\frac{x}{1} = \frac{a}{p^{n-1}} \cdot \frac{b}{p^m}$, ... iterando, trovo $x = a_n b_m$ con $a_n, b_m \in A$

$\Rightarrow a_n$ o b_m è un'unità in A

- Se $\frac{x}{1}$ è un'unità : $\exists \frac{a}{p^n}$ t.c. $x \frac{a}{p^n} = 1$ in $B \Rightarrow p^n = xa$
  Se $p \mid x$, allora p e x sono associati
  Se $p \nmid x$, $a = pa_1 \Rightarrow p^{n-1} = a_1 x \Rightarrow 1 = a_n x$ ↯
  $\Rightarrow x$ è associato a $p \Rightarrow x$ è primo
- Se $\frac{x}{1}$ è irrid $\Rightarrow \frac{x}{1}$ è primo : $ab = x \cdot c$ in A

$\overset{B \text{ UFD}}{\Rightarrow} \frac{x}{1} \mid \frac{a}{1}$ o $\frac{x}{1} \mid \frac{b}{1}$: $\frac{a}{1} = \frac{x}{1} \cdot \frac{b}{p^n}$ $\quad p^n a = xb$

$\Rightarrow a = b'x$ □

Es A K-alg fin gen dominio, $f \in A \setminus \{0\}$
$\dim A[\frac{1}{f}] = \dim A$

Sol ($\leq$): da localizzazione può solo far calare la dimensione

($\geq$): Sia m un ideale massimale di A, $(0) \subsetneq \dots \subsetneq P_{\dim A} = m$

Corrisponde a una catena in $A[\frac{1}{f}] \iff m \cap S = \emptyset \iff f \notin m$

$\bigcap_{m \in \mathrm{Spec}\max A} m = (0)$

Modo 2 $A[\frac{1}{f}] \simeq \frac{A[t]}{(tf-1)}$ è una k-alg fin gen.

$\dim\left(\frac{A[t]}{(tf-1)}\right) = \dim A[t] - \mathrm{ht}(tf-1) = \dim A + 1 - 1 = \dim A$ □

ES $A = \frac{\mathbb{Q}[x,y,z]}{(x^2+y^3-z^7)}$, $\mathfrak{m} = (x,y,z)$ $\quad A_\mathfrak{m}$

Mostrare che $A_\mathfrak{m}$ è dominio Noetheriano locale UFD, ma non è regolare

[In dim 1. UFD $\Rightarrow$ int. chiuso $\Rightarrow$ DVR $\Rightarrow$ regolare]

$\dim A = \dim \mathbb{Q}[x,y,z] - ht(x^2+y^3-z^7) = 3 - 1 = 2$

Oss $(x^2+y^3-z^7)$ è un ideale primo

$\quad \overset{\shortparallel}{p_1(x,y,z)p_2(x,y,z)}$ non è possibile

$\dim A_\mathfrak{m} = 2$: in A, una catena massimale da (0) a $\mathfrak{m}$ ha lung $= \dim A = 2$

$\frac{\mathfrak{m}A_\mathfrak{m}}{(\mathfrak{m}A_\mathfrak{m})^2} \simeq \frac{\mathfrak{m}}{\mathfrak{m}^2} \simeq \frac{(x,y,z)+(x^2+y^3-z^7)}{(x,y,z)^2+(x^2+y^3-z^7)} = \frac{(x,y,z)}{(x,y,z)^2}$ ha $\dim_\mathbb{Q} = 3$, con base $\bar{x}, \bar{y}, \bar{z}$

Quindi $A_\mathfrak{m}$ non è regolare

UFD: basta mostrare A UFD

Applico Nagata con elemento $p = z$

$A/(z) \simeq \mathbb{Q}[x,y,z]/(x^2+y^3-z^7, z) \simeq \mathbb{Q}[x,y]/(x^2+y^3)$ è un dominio

Nagata: basta dim che $A[\frac{1}{z}]$ è UFD

$a := \frac{x}{z^3}$, $b := y/z^2$ $\quad a^2+b^3 = \frac{x^2+y^3}{z^6} = z^7/z^6 = z$

$A = \mathbb{Q}[x,y,z] \subseteq \mathbb{Q}[a,b] \subseteq A[\frac{1}{z}]$

$\Rightarrow A[\frac{1}{z}] \subseteq \mathbb{Q}[a,b][\frac{1}{z}] \subseteq A[\frac{1}{z}] \Longrightarrow A[\frac{1}{z}] = \mathbb{Q}[a,b][\frac{1}{z}]$

Oss $\dim A[\frac{1}{z}] = \dim A = 2 = \dim \mathbb{Q}[a,b][\frac{1}{z}] = \dim \mathbb{Q}[a,b] = \text{trdeg}\, \mathbb{Q}(a,b)$

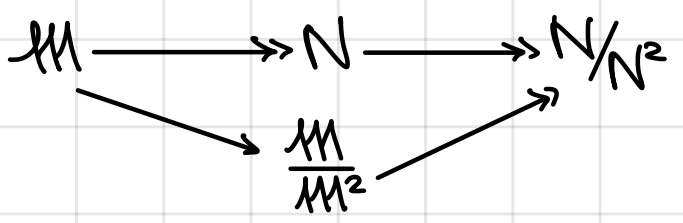
$\Rightarrow a, b$ sono alg. indipendenti $\Rightarrow \mathbb{Q}[a,b]$ è l'anello dei pol. in 2 variabili

$\Rightarrow A[\frac{1}{z}] \simeq \mathbb{Q}[a,b][\frac{1}{z}]$ è UFD

ES $(A,\mathfrak{m})$ locale, $I \trianglelefteq A$ ideale proprio, $k = A/\mathfrak{m}$, $N = \mathfrak{m}/I$

C'è una successione esatta di k-spazi vettoriali

$$0 \longrightarrow \frac{\mathfrak{m}^2+I}{\mathfrak{m}^2} \longrightarrow \frac{\mathfrak{m}}{\mathfrak{m}^2} \xrightarrow{\ \pi\ } \frac{N}{N^2} \longrightarrow 0$$



$x \in \mathfrak{m}$, $\bar{x} \in \mathfrak{m}/\mathfrak{m}^2$ $\quad \pi(\bar{x}) = 0 \iff \pi(x) \in N^2$, cioè $\exists i \in I, m \in \mathfrak{m}^2 : x = m + i$ $\quad \square$

$A = K[x_1, \dots, x_n]$ $\quad \mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n)$ $\quad a_i \in K$

$I = (F_1, \dots, F_r)$, $I \subset \mathfrak{m}$ $\quad \frac{\mathfrak{m}^2+I}{\mathfrak{m}^2}$ è il ssp di $\mathfrak{m}/\mathfrak{m}^2$ generato da $\left\{ \sum_{j=1}^n \frac{\partial F_i}{\partial x_j}(\underline{a})(x_j - a_j) \right\}_{i=1,\dots,r} =: G$

$f \in I$. Posso scrivere $f = \sum_{j=1}^n b_j (x_j - a_j)$ + qualcosa in $\mathfrak{m}^2$

$\frac{\partial f}{\partial x_i}(\underline{a}) = b_i + 0$

$f = g_1 F_1 + \dots + g_r F_r = \sum_{j=1}^n \frac{\partial f}{\partial x_j}(\underline{a})(x_j - a_j)$ + (cose in $\mathfrak{m}^2$) $\in$ Span G

$\frac{\partial}{\partial x_j}(g_1 F_1) = \frac{\partial g_1}{\partial x_j}(\underline{a}) \overset{0}{F_1(\underline{a})} + g_1(\underline{a}) \frac{\partial F_1}{\partial x_j}(\underline{a})$

Quindi: $\dim \left(\frac{\mathfrak{m}^2 + I}{\mathfrak{m}^2} \right) = rk \left(\frac{\partial F_i}{\partial x_j}(\underline{a}) \right)$

Criterio Jacobiano $A=k[x_1,\dots,x_n]$, $Q=(a_1,\dots,a_n)\in K^n$
$\mathfrak{m}=(x_1-a_1,\dots,x_n-a_n)\supseteq I$ ideale. Sia $B=(A/I)_{\mathfrak{m}}$
Scriviamo $I=(F_1,\dots,F_r)$, $J:=\left(\frac{\partial F_i}{\partial x_j}(Q)\right)$
$d=\dim B$, $r=\operatorname{rk} J$. Sono equivalenti:
(1) B regolare
(2) $r=n-d$
(3) $r\geq n-d$

DIMOSTRAZIONE
$(A/I)_{\mathfrak{m}}\simeq A_{\mathfrak{m}}/IA_{\mathfrak{m}}$ $\quad \mathfrak{m}A_{\mathfrak{m}}/(\mathfrak{m}A_{\mathfrak{m}})^2\simeq \mathfrak{m}/\mathfrak{m}^2$
Sia N l'ideale massimale di $(A/I)_{\mathfrak{m}}\simeq \mathfrak{m}A_{\mathfrak{m}}/IA_{\mathfrak{m}}$

$$0\longrightarrow \frac{IA_{\mathfrak{m}}+(\mathfrak{m}A_{\mathfrak{m}})^2}{(\mathfrak{m}A_{\mathfrak{m}})^2}\longrightarrow \frac{\mathfrak{m}}{\mathfrak{m}^2}\xrightarrow{\pi}\frac{N}{N^2}\longrightarrow 0$$

$$\frac{(I+\mathfrak{m}^2)A_{\mathfrak{m}}}{\mathfrak{m}^2A_{\mathfrak{m}}}\simeq S^{-1}\left(\frac{I+\mathfrak{m}^2}{\mathfrak{m}^2}\right)=\frac{I+\mathfrak{m}^2}{\mathfrak{m}^2}$$

$$0\longrightarrow \frac{\mathfrak{m}^2+I}{\mathfrak{m}^2}\longrightarrow \frac{\mathfrak{m}}{\mathfrak{m}^2}\longrightarrow \frac{N}{N^2}\longrightarrow 0$$

$$n=\dim\left(\mathfrak{m}/\mathfrak{m}^2\right)=\dim\frac{I+\mathfrak{m}^2}{\mathfrak{m}^2}+\dim\frac{N}{N^2}$$
$$=r+\text{min n° generatori di } N$$
$n-r=$ min n° generatori di $N\geq \operatorname{ht}N=\dim(A/I)_{\mathfrak{m}}=d$
Regolare $\iff$ e con $=$ $\iff n-r=d$
$r\leq n-d$ vale sempre $\square$

corollario $M=A$, q ideale $\mathfrak{m}$-primario, $\mathfrak{m}^n=q^n$.
Allora esiste un polinomio $\chi_q(n)$ t.c. $\ell(A/q^n)=\chi_q(n)$ $\forall n\gg 0$
e $\deg\chi_q(n)\leq$ # generatori di q.

Lemma Il grado di $\chi_q(n)$ non dipende dalla scelta dell'ideale $\mathfrak{m}$-primario q.

DIMOSTRAZIONE
Basta mostrare che $\deg\chi_q=\deg\chi_{\mathfrak{m}}$
Dato q, $\exists r\geq 1$ t.c. $\mathfrak{m}^r\subseteq q\subseteq\mathfrak{m}\implies \mathfrak{m}^{rn}\subseteq q^n\subseteq\mathfrak{m}^n$
$A/\mathfrak{m}^{rn}\twoheadrightarrow A/q^n\twoheadrightarrow A/\mathfrak{m}^n$
$\implies \ell(A/\mathfrak{m}^{rn})\geq\ell(A/q^n)\geq\ell(A/\mathfrak{m}^n)\quad\forall n\geq 1$
Quindi $\forall n\gg 0$ ho $\chi_{\mathfrak{m}}(rn)\geq\chi_q(n)\geq\chi_{\mathfrak{m}}(n)$
Siccome $\chi_{\mathfrak{m}}(n)$ e $\chi_{\mathfrak{m}}(rn)$ sono dello stesso grado, anche $\chi_q(n)$ ha lo stesso grado. $\square$

Quindi al momento per un anello locale Noetheriano $(A, \mathfrak{m})$ abbiamo 3 invarianti.

- $\dim A = \dim_{Krull} A$
- $\delta(A) = \min$. n° generatori di un ideale $\mathfrak{m}$-primario $q =$
  $= \min_{q\ \mathfrak{m}\text{-prim.}}$ (min n° generatori di q)
- $d(A) = \deg \chi_{\mathfrak{m}}$ $(= d(Gr_{\mathfrak{m}} A))$

Teorema fondamentale della dimensione $\quad \dim A = \delta(A) = d(A)$

Oss
- Il Teo dell'altezza dice $\dim A = ht\ \mathfrak{m} \leq \delta(A)$
- Il viceversa del Teo. dell'altezza dice $\delta(A) \leq \dim A$
- $d(A) \leq \delta(A)$: $\deg \chi_{\mathfrak{m}} = \deg \chi_q \leq$ # gen. di q $\forall q \implies d(A) \leq \delta(A)$
- Se dimostriamo che $\dim A \leq d(A)$, abbiamo finito

Lemma $(A, \mathfrak{m})$ locale Noetheriano, $x \in A$ non divisore di 0. Allora $d(A_{/(x)}) \leq d(A) - 1$

DIMOSTRAZIONE

Sia $B := A/(x)$. Come A-moduli, abbiamo:

$$0 \longrightarrow \frac{(x)+\mathfrak{m}^n}{\mathfrak{m}^n} \longrightarrow A/\mathfrak{m}^n \longrightarrow B/\mathfrak{m}_B^n \longrightarrow 0 \quad \text{esatta}$$

$$\frac{(x)+\mathfrak{m}^n}{\mathfrak{m}^n} \cong \frac{(x)}{(x)\cap \mathfrak{m}^n}$$

- $\ell_B(B/\mathfrak{m}_B^n) = \ell_A(B/\mathfrak{m}_B^n)$
- Come A-modulo, $(x) \simeq A \qquad 0 \to A \xrightarrow{\cdot x} (x) \to 0$
  perché x non è divisore di 0

Inoltre, per Artin-Rees la filtrazione $(x)\cap \mathfrak{m}^n$ è una filtrazione $\mathfrak{m}$-stabile
$\implies \ell((x)/(x)\cap\mathfrak{m}^n)$ per $n \gg 0$ è un polinomio, il cui grado e termine di testa coincidono con quelli del polinomio $\chi_{\mathfrak{m}}(n) = \ell(A/\mathfrak{m}^n)$

Dalla succ. esatta,

$\ell_B(B/\mathfrak{m}_B^n) = \ell_A(B/\mathfrak{m}_B^n) = \ell(A/\mathfrak{m}^n) - \ell((x)/(x)\cap\mathfrak{m}^n)$ è un pol. di grado strettamente minore di $\ell(A/\mathfrak{m}^n)$ perché i termini di testa si cancellano

$\implies d(B) \leq d(A) - 1$ □

Oss $(A, \mathfrak{m})$ locale Noetheriano, $\pi: A \to A'$ un quoziente, $\mathfrak{m}' = \pi(\mathfrak{m})$. e $d(A') \leq d(A)$

DIMOSTRAZIONE

$$A/\mathfrak{m}^n \longrightarrow A'/\mathfrak{m}'^n \longrightarrow 0$$

$\ell_{A'}(A'/\mathfrak{m}'^n) = \ell_A(A'/\mathfrak{m}'^n) \leq \ell_A(A/\mathfrak{m}^n)$

Per $n \gg 0$, questo dà $d(A') \leq d(A)$.

proposizione $\dim A \leq d(A)$

DIMOSTRAZIONE

Per induzione su $d(A)$

- $d(A)=0$: $\ell(A/\mathfrak{m}^n)$ è costante per $n \gg 0$

$$0 \longrightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1} \longrightarrow A/\mathfrak{m}^{n+1} \longrightarrow A/\mathfrak{m}^n \longrightarrow 0$$

$$\Rightarrow \ell(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = \ell(A/\mathfrak{m}^{n+1}) - \ell(A/\mathfrak{m}^n) = 0 \quad \text{per } n \gg 0$$

$$\Rightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1} = (0) \Rightarrow \mathfrak{m}\cdot\mathfrak{m}^n = \mathfrak{m}^n \overset{\text{Nak}}{\Rightarrow} \mathfrak{m}^n = (0)$$

per cui A è Artiniano e quindi di dim. 0

- $d(A) \geq 1$: Prendiamo $P_0 \subsetneq P_1 \subsetneq \dots \subsetneq P_r$ catena di primi in A con $r = \dim A$

Se $r=0$, ok $\dim A \leq d(A)$

Se $r \geq 1$, scelgo $x \in P_1 \setminus P_0$. Sia $A' = A/P_0$: è un dominio e $d(A') \leq d(A)$. La classe di x in A' non è un divisore di 0

$$\Rightarrow d(A'/(x)) \leq d(A') - 1 \leq d(A) - 1$$

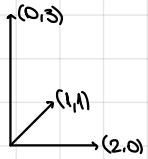
Per hp. induttiva, $\dim(A'/(x)) \leq d(A) - 1$

D'altra parte, la catena $P_1/(x) \subsetneq \dots \subsetneq P_r/(x)$ mostra che $\dim(A'/(x)) \geq r-1$

$$\Rightarrow r-1 \leq d(A)-1 \Rightarrow r \leq d(A)$$

□

esempio combinatorio



$v_1, v_2, v_3 \in \mathbb{R}^3$

Consideriamo le combinazioni $a_1v_1 + a_2v_2 + a_3v_3$, con $a_i \in \mathbb{N}$

"Quanti sono" questi punti? Specificamente, quanti ce ne sono con $x+y=n$, con $n \gg 0$?

$A = K[x^2, y^3, xy] \subseteq K[x,y]$

Contare i punti con somma delle coord $=n$ è come calcolare $\dim A_n$

$\varphi : K[u,v,w] \longrightarrow A$

$u \mapsto x^2$

$v \mapsto y^3$

$w \mapsto xy$

- $\ker\varphi \ni -u^3v^2 + w^6$
- $\ker\varphi$ è primo, perché φ è surj e A è un dominio
- $\dim A = \dim K[u,v,w] - \operatorname{ht}\ker\varphi$

$$2 = 3 - \operatorname{ht}\ker\varphi \Rightarrow \operatorname{ht}\ker\varphi = 1$$

$$\dim A = \operatorname{trdeg}\operatorname{Frac}A = \operatorname{trdeg} K(x,y) = 2$$

Ora $\ker\varphi \supseteq (w^6 - u^3v^2)$ primo

$$\Rightarrow A \simeq K[u,v,w]/(w^6 - u^3v^2) =: B \qquad \deg u = 2 \quad \deg v = 3 \quad \deg w = 2$$

$$p_B(t) = \sum_{n \geq 0} \ell(B_n) t^n$$

$$p_B(t) = \frac{1}{(1-t^{\deg u})} p_{B/uB}(t) \qquad \text{se } [u] \text{ è inattiva}$$

$$= \frac{1}{(1-t^2)} p_{K[v,w]/(w^6)}(t) = \frac{1}{(1-t^2)(1-t^3)} p_{K[w]/(w^6)}(t)$$

$$= \frac{1}{(1-t^2)(1-t^3)} (1 + t^2 + t^4 + t^6 + t^8 + t^{10}) = \frac{1-t^{12}}{(1-t^2)^2(1-t^3)}$$

$$= (1 + t^2 + \_ + t^{10}) \sum_{n \geq 0} r(n) t^n = \sum_{n \geq 0} s(n) t^n$$

$$\frac{1}{1-t^2} = 1 + t^2 + t^4 + \dots \qquad \frac{1}{1-t^3} = 1 + t^3 + t^6 + \dots$$

$$r(n) = \#\{(a,b) \in \mathbb{N}^2 \mid 2a + 3b = n\}$$

$$s(n) = r(n) + r(n-2) + \_ + r(n-10)$$

$\left| r(n) - \frac{n}{6} \right|$ è limitato $\Rightarrow s(n) = n +$ un termine limitato

Funzioni di Hilbert e varietà proiettive

def Sia I un ideale omogeneo di $A := K[x_0, \dots, x_N]$. Poniamo
$$h_I(d) = \dim_K (A/I)_d$$

Oss $(B, \mathfrak{M}) = K[x_0, \dots, x_N]_{(x_0, \dots, x_N)}$
$$Gr_{\mathfrak{M}} B = \bigoplus_{d \geq 0} \frac{(x_0, \dots, x_N)^d}{(x_0, \dots, x_N)^{d+1}} \cong K[x_0, \dots, x_N]$$
(hanno le stesse parti graduate in ogni grado)

Oss Sia $F \in K[x_0, \dots, x_N]$ un polinomio omogeneo
$$V_{\mathbb{P}}(F) = \{ [x_0 : \dots : x_N] \in \mathbb{P}^N(K) \mid F(x_0, \dots, x_N) = 0 \}$$
Più generalmente, se I è ideale omogeneo
$$V_{\mathbb{P}}(I) = \{ [x_0 : \dots : x_N] \in \mathbb{P}^N(K) \mid F(P) = 0 \ \forall F \in I \text{ omogeneo} \}$$
Viceversa, dato $V \subseteq \mathbb{P}^N(K)$, il corrispondente ideale è
$$I(V) = \{ F \in K[x_0, \dots, x_N] \mid F(\hat{P}) = 0 \ \forall \hat{P} \in K^{N+1} \text{ che rappresenta } P \in V \}$$
è un ideale omogeneo (K infinito)

esempio funzione di Hilbert di un punto
$$V = \{ [a_0 : \dots : a_N] \} \longrightarrow I(V) = (a_i x_j - a_j x_i \mid i, j)$$
A meno di una trasformazione proiettiva, posso portare
$$P \text{ in } [1 : \dots : 0] \longrightarrow I = (x_1, \dots, x_N)$$
Algebricamente: se A_{ij} è una matrice invertibile in $M_{m}(K)$
$$x_i \longmapsto \sum_j A_{ij} x_j \text{ è un automorfismo di } K[x_0, \dots, x_N]$$
$$\dim_K \left(K[x_0, \dots, x_N] / (a_i x_j - a_j x_i)_d \right) = \dim_K \left(\frac{K[x_0, \dots, x_N]}{(x_1, \dots, x_N)} \right)_d = 1 \quad \forall d$$

Oss (additività) I, J omogenei. Vale
$$h_{I+J} + h_{I \cap J} = h_I + h_J$$

$$h_L(d) = \dim K[x_0, \dots, x_N]_d - \dim L_d$$
Basta dim che $\dim (I+J)_d + \dim (I \cap J)_d = \dim I_d + \dim J_d$
che è Grassmann

Oss $\cdot V(I+J) = V(I) \cap V(J)$
$\cdot V_{\mathbb{P}}(I) = \emptyset \iff \exists m \geq 0$ t.c. $(x_0, \dots, x_N)^m \subseteq I$
(infatti $V_{\mathbb{P}}(I) = \emptyset \iff V(I) \subseteq \{(0, \dots, 0)\} \iff V(I) \subseteq V((x_0, \dots, x_N))$
$\iff \sqrt{I} \supseteq (x_0, \dots, x_N)$

Conseguenza: se $P_1, \dots, P_n$, $I = V(\{P_1, \dots, P_n\})$
$$h_I(d) = n \quad \forall d \gg 0$$
$h_{(x_0, \dots, x_N)^m}(d) = 0 \ \forall d \gg 0$:
$$\dim \frac{K[x_0, \dots, x_N]_d}{[(x_0, \dots, x_N)^m]_d} = 0 \text{ per } d > m$$

Per induzione dall'additività trovo $h_I(d) = n \ \forall d \gg 0$

Funzione di Hilbert di 3 o 6 punti

- Sia $V=\{P_1,P_2,P_3\}$, $I=I(V)$ nel piano

$$h_I(1)=\dim \frac{K[x_0,x_1,x_2]_1}{I_1}=\begin{cases}3 & \text{se } P_1,P_2,P_3 \text{ non allineati}\\ 2 & \text{se } P_1,P_2,P_3 \text{ allineati}\end{cases}$$

- Sia $V=\{P_1,\dots,P_6\}$, $P_1,\dots,P_6$ non allineati, $I=I(V)$

$$\dim \frac{K[x_0,x_1,x_2]_2}{I_2}=\begin{cases}6 & \text{se i punti non stanno su una conica}\\ 5 & \text{altrimenti}\end{cases}$$

esempio $h_{(0)}=?$ $\quad V=\mathbb{P}^N \longrightarrow I=(0)$

$$h_I(d)=\dim K[x_0,\dots,x_N]_d$$

$x_0^{e_0}\cdots x_N^{e_N}$ con $e_0+\dots+e_N=d$, $e_i\geq 0 \longrightarrow \binom{N+d}{N}$

$$h_I(d)=p_{K[x_0,\dots,x_N]}(d)=\frac{1}{1-d}p_{K[x_0,\dots,x_{N-1}]}(d)=\dots=\frac{1}{(1-d)^{N+1}}$$

Questo dimostra $\sum_{d\geq 0}\binom{N+d}{N}t^d=\frac{1}{(1-t)^{N+1}}$

$C:=K[x_0,\dots,x_N]$. I ideale primo omogeneo $\subseteq (x_0,\dots,x_N)$

$A=(C(I)_{(x_0,\dots,x_N)=m}$ $B=C/I$ dominio

$\dim A=d(A)=d(\mathrm{Gr}_m A)=ht_B(x_0,\dots,x_N)=\dim B$

$\dim V_p(I)=\dim V(I)-1=\dim B-1$

$h_I(d)=\dim_K \frac{K[x_0,\dots,x_N]_d}{I_d}$

$$m_A^d/m_A^{d+1}\simeq m_B^d/m_B^{d+1}\simeq \frac{(x_0,\dots,x_N)^d+I}{(x_0,\dots,x_N)^{d+1}+I}$$

$$(x_0,\dots,x_N)^d+I=I_0\oplus I_1\oplus\dots\oplus I_{d-1}\oplus C_d\oplus C_{d+1}\oplus\dots$$

Quozientando per $(x_0,\dots,x_N)^{d+1}+I$, ottengo

$$\frac{(x_0,\dots,x_N)^d+I}{(x_0,\dots,x_N)^{d+1}+I}\simeq C_d/I_d=\frac{K[x_0,\dots,x_N]_d}{I_d}$$

Per d grande, $\dim_K\left(m_A^d/m_A^{d+1}\right)=h_I(d)=$ pol. di grado $\dim A-1=\dim B-1=\dim V_p(I)$

ES(PG) Sia F un polinomio omogeneo, I un ideale omogeneo in $K[x_0,\dots,x_N]$
Supponiamo che $\exists d_0$ t.c. $\forall d\geq d_0$ $\forall G\in K[x_0,\dots,x_N]_d$ vale $FG\in I\Rightarrow G\in I$.
Allora $\forall d\gg 0$ $h_{I+(F)}(d)=h_I(d)-h_I(d-\deg F)$

FATTO $K=\bar{K}$, I t.c. $V_p(I)\neq\emptyset$. Allora $\exists F\in K[x_0,\dots,x_N]_d$ che soddisfa l'ipotesi dell'es. precedente.

esempio Partiamo con una varietà $V = V_p(I)$.
Usando i fatti sopra, trovo F lineare t.c.

$$h_{I+(F)}(d) = h_I(d) - h_I(d-1) \quad \text{per } d \gg 0$$

Se $h_I(d) \sim C\frac{d^{\dim V}}{(\dim V)!}$, $C \in \mathbb{N}_{>0}$

$$h_{I+(F)}(d) \sim C\,\frac{x^{\dim V - 1}}{(\dim V - 1)!}$$

$$\Delta\left(\frac{x^k}{k!}\right) = \frac{(x+1)^k - x^k}{k!} = \frac{kx^{k-1} + O(x^{k-2})}{k!} = \frac{x^{k-1}}{(k-1)!}$$

Ripetendo questo procedimento $(\dim V)$ volte, trovo

$$h_{I+(F_1,\dots,F_{\dim V})}(d) = C$$

def Questo C si chiama il grado di V ed è il numero* di punti che trovo intersecando con $(\dim V)$ iperpiani generici
*con molteplicità

ES K campo, m id. massimale di $K[x_1,\dots,x_n] = A$
Allora $\exists (\alpha_1,\dots,\alpha_n) \in \bar{K}^n$ t.c. $m = \{p \in A \mid p(\alpha_1,\dots,\alpha_n) = 0\}$

SOL Considero $B = \bar{K}[x_1,\dots,x_n]$ e $A \subseteq B$
Ci basterebbe sapere che ogni ideale massimale di A è l'intersezione tra A e un id. massimale di B.
Per lying over / going down, basta che $A \subseteq B$ sia un'est. intera
Perciò devo mostrare che ogni $p(x_1,\dots,x_n) \in B$ è intero su A
Osservo che $\bar{K}[x_1,\dots,x_n] = \bigcup_{\substack{F/K \text{ est. finita} \\ F \subseteq \bar{K}}} F[x_1,\dots,x_n]$

l'insieme $C := \{q \in F[x_1,\dots,x_n] \mid q \text{ è intero su } A\}$ è un sottoanello di $F[x_1,\dots,x_n]$
- $x_1,\dots,x_n \in C$ perché stanno in A
- $f \in F$: allora $f \in C$, perché f è radice di un polinomio monico a coeff in K e quindi a coeff in A

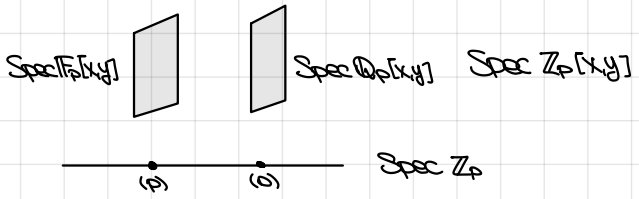
$\Rightarrow C = F[x_1,\dots,x_n] \Rightarrow B/A$ intera □

Oss $\prod_{\sigma \in \mathrm{Gal}(F/K)} (t - \sigma p(x_1,\dots,x_n)) \in A[t]$

ES p primo. L'anello $\mathbb{Z}_p[x,y]$ è regolare.

SOL Classifichiamo gli ideali massimali.
Sia m massimale. Considero $m \cap \mathbb{Z}_p$: è un primo di $\mathbb{Z}_p$, cioè (0) e (p)
- Se $m \cap \mathbb{Z}_p = (p)$, m corrisponde a un ideale di $\mathbb{Z}_{p/(p)}[x,y] = \mathbb{F}_p[x,y]$.
  $\overline{m}$ è generato da 2 elementi e che $ht\,\overline{m} = 2$
  $\Rightarrow m = (p, f_1, f_2)$, $ht\, m \leq 3$
  In effetti $ht\, m = 3$: prendo una catena $\overline{P}_0 \subsetneq \overline{P}_1 \subsetneq \overline{m}$ e per corrispondenza ho $(0) \subsetneq (p) \subsetneq (p, f_3) \subsetneq m$
- Se $m \cap \mathbb{Z}_p = (0)$: m non incontra $\{p^n : n \in \mathbb{N}\}$
  corrisponde a un ideale di $S^{-1}\mathbb{Z}_p[x,y] = \mathbb{Q}_p[x,y]$
  $m\mathbb{Q}_p[x,y] = (g_1, g_2)$ di altezza 2
  Una catena dentro m è in corrisp. con una catena contenuta in $m\mathbb{Q}_p[x,y]$
  La localizz. $\mathbb{Z}_p[x,y]_m = \mathbb{Q}_p[x,y]_m$ ha dim 2
  e il suo ideale è generato da 2 elementi

OSS Gli ideali del 2° tipo esistono : $(1-px, y)$
$\mathbb{Z}_p[x,y]/(1-px,y) \simeq \mathbb{Z}_p[x]/(1-px) \simeq \mathbb{Z}_p[\frac{1}{p}] = \mathbb{Q}_p$



ES A regolare, $x \in A$. Supponiamo che $\forall\, m$ id. massimale di A valga $x \notin m^2$.
Allora $A/(x)$ è regolare.

SOL Sia $\overline{m}$ un massimale di $A/(x)$; corrisponde ad un massimale m di A, $x \in m$.
Considero $m/m^2 \ni \overline{x} \neq 0$. Completo $\overline{x}$ ad una base di m/m^2 come A/m-spazio vett : $\overline{x} = \overline{x}_1, \dots, \overline{x}_r$, con $r = \dim_{A/m} m/m^2 = ht\, m$
Allora $m = (x, x_2, \dots, x_r)$ e questo è un sist. reg. di parametri
$A_m/(x)A_m$ è regolare
12
$(A/(x))_{\overline{m}}$
Questo vale $\forall\, \overline{m}$, quindi $A/(x)$ è regolare. □

Es $A = \mathbb{Z}_p[x,y]/(y^2 - x^5 - p)$ $\quad B = \mathbb{Z}_p[x,y]/(y^2 - x^5 - p^2)$

Mostriamo che B non è regolare, ma A sì

Cominciamo da B: basta esibire $\mathfrak{m} \subset B$ massimale con

$\dim_{B/\mathfrak{m}} (\mathfrak{m}/\mathfrak{m}^2) > ht\, \mathfrak{m}$

$\mathfrak{m} = (p, x, y)$ $\quad \mathfrak{m}/\mathfrak{m}^2 \simeq \dfrac{\mathfrak{m} + (y^2 - x^5 - p^2)}{\mathfrak{m}^2 + (y^2 - x^5 - p^2)} = \dfrac{(x,y,p)}{(x,y,p)^2}$ ha dim 3 su $B/\mathfrak{m} \simeq \mathbb{F}_p$

|| siccome $\mathbb{Z}_p[x,y]$ è regolare

$ht_{\mathbb{Z}_p[x,y]}(x,y,p) = 3$

D'altro canto $ht\, \mathfrak{m} \leq \dim B \leq 2$, perché le catene in B corrispondono a catene in $\mathbb{Z}_p[x,y]$ che non partono da 0.

Oss $d(A/(x)) \leq d(A) - 1$ per A dominio, $x \neq 0$

Ora prendiamo A. Per l'es precedente, basta mostrare che $f = y^2 - x^5 - p \notin \mathfrak{m}^2$ $\forall \mathfrak{m}$ massimale.

- Caso $\mathfrak{m} \not\ni p$, cioè $\mathfrak{m}$ corrisponde ad un massimale di $\mathbb{Q}_p[x,y]$

  Se $f \in \mathfrak{m}^2$ in $\mathbb{Z}_p[x,y] \Longrightarrow f \in (\mathfrak{m}\mathbb{Q}_p[x,y])^2$

  So che $\mathfrak{m}\overline{\mathbb{Q}}_p[x,y] = \{g \in \overline{\mathbb{Q}}_p[x,y] : g(\alpha,\beta) = 0\}$ per un certo $(\alpha,\beta) \in \overline{\mathbb{Q}}_p^2$

  $\Longrightarrow f \in (x - \alpha, y - \beta)^2$ in $\overline{\mathbb{Q}}_p[x,y]$

Oss $\mathfrak{m}\overline{\mathbb{Q}}_p[x,y]$ non è necess. massimale: ad es.

$p = 3$, $\mathfrak{m} = (x^2 + 1, y)$ $\rightsquigarrow$ $\mathfrak{m}\overline{\mathbb{Q}}_3[x,y] \subsetneq (x + i, y)$

Si avrebbe $f(\alpha,\beta) = 0 = \frac{\partial f}{\partial x}(\alpha,\beta) = \frac{\partial f}{\partial y}(\alpha,\beta)$

perché questa proprietà è vera per ogni pol. del tipo

$(x-\alpha)^2 g(x,y)$, $\quad (y-\beta)^2 g(x,y)$, $\quad (x-\alpha)(y-\beta) g(x,y)$.

Quindi (α,β) risolvono

$$\begin{cases} \beta^2 - \alpha^5 - p = 0 \\ -5\alpha^4 = 0 \\ 2\beta = 0 \end{cases} \qquad \begin{cases} \beta = 0 \\ \alpha = 0 \\ p = 0 \end{cases} \quad \text{assurdo}$$

- Caso $p \in \mathfrak{m}$: $\mathfrak{m} = (p, f_1, f_2) \longleftrightarrow \overline{\mathfrak{m}}$ mass. di $\mathbb{F}_p[x,y]$

  $f \in \mathfrak{m}^2 \longrightarrow f \bmod p \in \overline{\mathfrak{m}}^2$ $\qquad \overline{\mathfrak{m}} = \{g(x,y) \mid g(\alpha,\beta) = 0\}$ per $(\alpha,\beta) \in \overline{\mathbb{F}}_p^2$

  $\Longrightarrow f \in (x - \alpha, y - \beta)^2$ in $\overline{\mathbb{F}}_p[x,y]$

  Allora α, β soddisfa

$$\begin{cases} \beta^2 - \alpha^5 - p = 0 \\ -5\alpha^4 = 0 \\ 2\beta = 0 \end{cases} \quad \text{in } \overline{\mathbb{F}}_p$$

Se $p \neq 2,5 \longrightarrow \begin{cases} \beta^2 - \alpha^5 = 0 \\ \alpha = 0 \\ \beta = 0 \end{cases}$

$p=2 \longrightarrow \begin{cases} \alpha^4 = 0 \longrightarrow \alpha = 0 \\ \beta^2 = 0 \longrightarrow \beta = 0 \end{cases}$ $\qquad$ $p=5 \longrightarrow \begin{cases} \alpha^5 = 0 \longrightarrow \alpha = 0 \\ 2\beta = 0 \longrightarrow \beta = 0 \end{cases}$

SE $f \in \mathfrak{M}^2$, allora $\mathfrak{M} \ni p$ e $\overline{\mathfrak{M}} = (x,y) \Longrightarrow \mathfrak{M} = (x,y,p)$
Basta chiedersi se $f = y^2 - x^5 - p \in \mathfrak{M}^2$, cioè $p \in \mathfrak{M}^2$ impossibile

ES Completamenti e regolarità
Sia $(A, \mathfrak{M})$ locale Noeth. $\hat{A}$ il completamento $\mathfrak{M}$-adico.
(1) $\dim \hat{A} = \dim A$
(2) A regolare $\Longrightarrow \hat{A}$ regolare

SOL $\hat{A}$ Noetheriano, locale, con id. massimale $\mathfrak{M}\hat{A}$
$\hat{A}/\hat{\mathfrak{m}} \simeq \widehat{A/\mathfrak{M}} = A/\mathfrak{M}$ campo e $\hat{\mathfrak{m}} = \mathfrak{M}\hat{A}$
$d(A)$ = grado del pol. che coincide con $n \longmapsto \ell_A(A/\mathfrak{M}^n)$ per $n \gg 0$
$d(A)-1$ = grado del pol. che coincide con $n \longmapsto \ell_A(\mathfrak{M}^n/\mathfrak{M}^{n+1})$ per $n \gg 0$
$d(\hat{A})-1$ = $\quad$ // $\quad$ $n \longmapsto \ell_{\hat{A}}(\hat{\mathfrak{m}}^n/\hat{\mathfrak{m}}^{n+1})$
$\ell_{\hat{A}/\hat{\mathfrak{m}}}(\hat{\mathfrak{m}}^n/\hat{\mathfrak{m}}^{n+1})$ $\qquad$ $\ell_{A/\mathfrak{M}}(\mathfrak{M}^n/\mathfrak{M}^{n+1})$

Osserviamo che $\hat{\mathfrak{m}}^n/\hat{\mathfrak{m}}^{n+1} \simeq \widehat{\mathfrak{M}^n/\mathfrak{M}^{n+1}} = \mathfrak{M}^n/\mathfrak{M}^{n+1}$

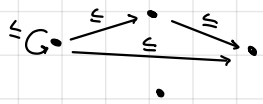
(2) A regolare $\Longleftrightarrow \dim_{A/\mathfrak{M}} \mathfrak{M}/\mathfrak{M}^2 = \dim A \Longleftrightarrow \dim_{\hat{A}/\hat{\mathfrak{m}}} \hat{\mathfrak{m}}/\hat{\mathfrak{m}}^2 = \dim \hat{A} \Longleftrightarrow \hat{A}$ regolare

TEORIA DELLE CATEGORIE

def. Una categoria $\mathcal{C}$ consiste dei dati seguenti:
- una classe $Ob(\mathcal{C})$ o $|\mathcal{C}|$ di "oggetti"
- una classe $Mor(\mathcal{C})$ di "frecce"
- due funzioni "classe" dominio e codominio (source e target)
  $s: Mor(\mathcal{C}) \longrightarrow Ob(\mathcal{C})$ $\quad t: Mor(\mathcal{C}) \longrightarrow Ob(\mathcal{C})$
- per ogni 3 oggetti $A,B,C \in Ob(\mathcal{C})$, posto
  $Hom_{\mathcal{C}}(A,B) = \{f \in Mor(\mathcal{C}) \mid s(f)=A, t(f)=B\}$,
  un' operazione binaria
  $$Hom_{\mathcal{C}}(A,B) \times Hom_{\mathcal{C}}(B,C) \longrightarrow Hom_{\mathcal{C}}(A,C)$$
  $$f \quad , \quad g \longmapsto g \circ f$$

che soddisfano
(i) associatività: $\forall A,B,C,D \in Ob(\mathcal{C})$, $\forall f: A \to B, \forall g: B \to C, \forall h: C \to D$ vale $h \circ (g \circ f) = (h \circ g) \circ f$
(ii) identità: $\forall A \in Ob(\mathcal{C})$, $\exists id_A \in Hom_{\mathcal{C}}(A,A)$ che è l'identità bilatera per la composizione

esempio
- (Set): Ob = insiemi, Mor = funzioni
- Ab: Ob = gruppi abeliani, Mor = omomorfismi di gruppi abeliani
- Vect$_K$
- Mod$_R$
- Top*: Ob = coppie (X,p), X sp. top. e $p \in X$
  Mor: $f: (X,p) \longrightarrow (Y,q)$ continua t.c. $f(p)=q$
- Categorie con $|Ob(\mathcal{C})| = 1$ (e localmente piccole) $\quad \leadsto$ monoide $Hom_{\mathcal{C}}(A,A)$
- Poset: $(X, \leq)$ un insieme parz. ordinato
  "Categoria poset" se $|Hom_{\mathcal{C}}(A,B)| \leq 1$



- Grafi diretti



- Categoria opposta: $\mathcal{C} = (|\mathcal{C}|, Mor(\mathcal{C}) \longrightarrow \mathcal{C}^{op} = (|\mathcal{C}|, Mor(\mathcal{C})^{op})$
  $Hom_{\mathcal{C}^{op}}(A,B) = Hom_{\mathcal{C}}(B,A)$

def. Siano $\mathcal{C}, \mathcal{D}$ due categorie.
Un funtore (covariante) $F: \mathcal{C} \longrightarrow \mathcal{D}$ è il dato di:
- una funzione classe $F: |\mathcal{C}| \longrightarrow |\mathcal{D}|$
- $\forall A,B \in |\mathcal{C}|$, $F: Hom_{\mathcal{C}}(A,B) \longrightarrow Hom_{\mathcal{D}}(F(A), F(B))$
  tale che
(i) $\forall A \quad F(id_A) = id_{F(A)}$
(ii) $\forall A,B,C \in |\mathcal{C}| \quad \forall f: A \to B, \forall g: B \to C$ vale
$F(g \circ f) = F(g) \circ F(f)$

esempio • $\pi_1 : \mathrm{Top}^* \longrightarrow \mathrm{Grp}$

$(X,p) \longmapsto \pi_1(X,p)$

$f : (X,p) \longrightarrow (Y,q) \longmapsto \pi_1(f) : \pi_1(X,p) \longrightarrow \pi_1(Y,q)$

$[\gamma] \longmapsto [f \circ \gamma]$

- Funtori dimenticanti
- localizzazione : R anello, S parte moltiplicativa

$S^{-1} : \mathrm{Mod}_R \longrightarrow \mathrm{Mod}_{S^{-1}R}$

$M \longmapsto S^{-1}M$

$f : M \to N \longmapsto S^{-1}f : S^{-1}M \longrightarrow S^{-1}N$

$\frac{m}{s} \longmapsto \frac{f(m)}{s}$

- Dualità : $\mathrm{Vect}_K \longrightarrow \mathrm{Vect}_K$

$V \longmapsto V^* = \mathrm{Hom}(V,K)$

$f : V \to W \longmapsto f^* : W^* \longrightarrow V^*$

$\psi \longmapsto \psi \circ f$

$(f \circ g)^* = g^* \circ f^*$

diventa un funtore $\mathrm{Vect}_K \longrightarrow \mathrm{Vect}_K^{op}$

def. Un funtore controvariante $F : \mathcal{C} \longrightarrow \mathcal{D}$ è un funtore $\mathcal{C} \longrightarrow \mathcal{D}^{op}$

esempio $\mathrm{Spec} : \mathrm{Ring} \longrightarrow \mathrm{Top}$ è un funtore controvariante

I nostri funtori preferiti

R anello, Mod_R. Fissiamo $M \in |\mathrm{Mod}_R|$

- $- \otimes M : \mathrm{Mod}_R \longrightarrow \mathrm{Mod}_R$

$N \longmapsto N \otimes_R M$

$f : N_1 \to N_2 \longmapsto f \otimes \mathrm{id} : N_1 \otimes M \longrightarrow N_2 \otimes M$

- $\mathrm{Hom}_R(-,M) : \mathrm{Mod}_R \longrightarrow \mathrm{Mod}_R^{op}$

$N \longmapsto \mathrm{Hom}_R(N,M)$

$f : N_1 \to N_2 \longmapsto \mathrm{Hom}(N_2,M) \longrightarrow \mathrm{Hom}(N_1,M)$

$\phi \longmapsto \phi \circ f$

- $\mathrm{Hom}_R(M,-) : \mathrm{Mod}_R \longrightarrow \mathrm{Mod}_R$

$N \longmapsto \mathrm{Hom}_R(M,N)$

$f : N_1 \to N_2 \longmapsto \mathrm{Hom}(M,N_1) \xrightarrow{f_*} \mathrm{Hom}(M,N_2)$

$\phi \longmapsto f \circ \phi$

Diagrammi

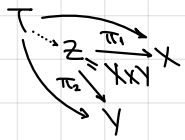
Un diagramma in una categoria $\mathcal{C}$ è un funtore
$F: J \longrightarrow \mathcal{C}$ (è detto di "forma" J)
Il diagramma è commutativo se J è una categoria poset.

Coni Un cono sul diagramma $F: J \longrightarrow \mathcal{C}$ è un oggetto $X \in |\mathcal{C}|$ con mappe $f_j: X \longrightarrow F(j)$ $\forall j \in |J|$ e tale che
$F(f) \circ f_{j_1} = f_{j_2}$ $\forall f \in \mathrm{Hom}_J(j_1, j_2)$

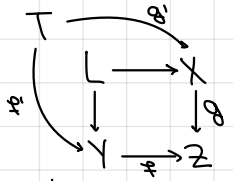
Un cono è detto un (il) limite di un diagramma se
$\forall (T, g_i)$ cono sullo stesso diagramma $\exists! h: T \longrightarrow X$ che fa commutare tutto: $g_i = f_i \circ h$
Tale limite è unico.

esempio

- In Set



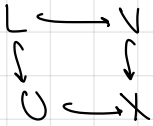
- In Set



$g \circ g' = f \circ f'$

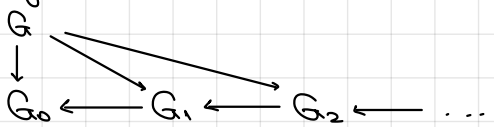
$L = X \times_Z Y = \{(x,y) \in X \times Y \mid g(x) = f(y)\}$

- X sp. top, Open_X = categoria degli aperti
$|\mathrm{Open}_X|$ = aperti di X, $\mathrm{Hom}_{\mathrm{Open}_X}(U,V) = \begin{cases} i: U \hookrightarrow V & \text{se } U \subseteq V \\ \emptyset & \text{altrimenti} \end{cases}$



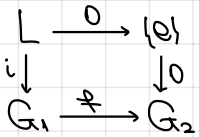
$L = U \cap V$

- In Ab, prendiamo un sistema inverso di gruppi
(= diagramma di forma $\bullet \longleftarrow \bullet \longleftarrow \bullet \longleftarrow \dots$)



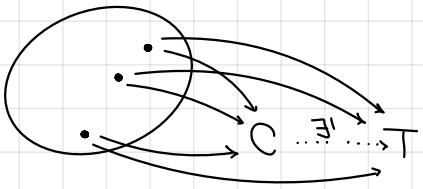
$G = \varprojlim G_i$

- In Ab

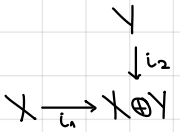


$L = \ker f$

Colimiti



esempio - In Ab



Oss $\mathrm{Hom}(A, \prod X_i) = \prod \mathrm{Hom}(A, X_i)$
$\mathrm{Hom}(\oplus X_i, A) = \prod \mathrm{Hom}(X_i, A)$

Aggiunti

$\mathcal{C}, \mathcal{D}$ categorie, $F: \mathcal{C} \longrightarrow \mathcal{D}$, $G: \mathcal{D} \longrightarrow \mathcal{C}$

Diciamo che F e G sono aggiunti l'uno all'altro se vale

$\mathrm{Hom}_{\mathcal{D}}(F(A), B) = \mathrm{Hom}_{\mathcal{C}}(A, G(B)) \quad \forall A \in \mathrm{ob}(\mathcal{C}) \ \forall B \in \mathrm{ob}(\mathcal{D})$

F si dice aggiunto sinistro, G è l'aggiunto destro.

teorema Gli aggiunti sinistri commutano con i colimiti.
Gli aggiunti destri commutano con i limiti.

esempio $\mathrm{Hom}_R(M_1 \otimes N, M_2) = \mathrm{Hom}_R(M_1, \mathrm{Hom}(N, M_2))$

I funtori $F = - \otimes N$ e $G = \mathrm{Hom}(N, -)$ sono aggiunti

Caso speciale del Teo: $- \otimes N$ commuta con i Coker

$M_1/M_2 \otimes N = M_1 \otimes N / M_2 \otimes N$ [$\otimes N$ è esatto a dx]

$\mathrm{Hom}(N, -)$ è aggiunto dx $\Longrightarrow$ commuta con i Ker $\Longrightarrow$ è esatto a sx.

ALGEBRA OMOLOGICA

Def. R, S due anelli, $F: \mathrm{Mod}_R \to \mathrm{Mod}_S$ funtore. Si dice che F è

- additivo se $\forall A, B \in |\mathrm{Mod}_R|$ la mappa
$$\mathrm{Hom}_R(A,B) \longrightarrow \mathrm{Hom}_S(F(A), F(B))$$
è un omomorfismo di gruppi abeliani
(Tutti i nostri funtori saranno additivi)
- esatto a SX se per ogni successione esatta $0 \to M_1 \to M_2 \to M_3 \to 0$ la successione $0 \to F(M_1) \to F(M_2) \to F(M_3)$ è esatta

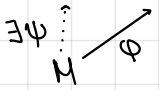
Oss $0 \to M_1 \to M_2 \rightsquigarrow 0 \to M_1 \to M_2 \to M_2/M_1 \to 0$
$0 \to F(M_1) \to F(M_2) \rightsquigarrow 0 \to F(M_1) \to F(M_2) \to F(M_2/M_1)$

- esatto a dx se per ogni $M_1 \to M_2 \to 0$ esatta la successione $F(M_1) \to F(M_2) \to 0$ è esatta
- esatto se è esatto sia a dx sia a SX

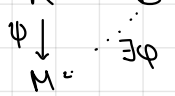
Def. Un modulo $M \in |\mathrm{Mod}_R|$ è

- piatto se $- \otimes M$ è esatto [a SX]
- proiettivo se $\mathrm{Hom}_R(M, -)$ è esatto [a dx]
- iniettivo se $\mathrm{Hom}_R(-, M)$ è esatto [a dx]
- libero se è isomorfo a $\bigoplus_{i \in I} R$ per un qualche insieme di indici I.

Concretamente

- Piatto: per ogni $0 \to A \xrightarrow{f} B$ iniettiva, anche
$$0 \to A \otimes M \xrightarrow{f \otimes \mathrm{id}} B \otimes M \text{ è iniettiva}$$
- Proiettivo:
$$A \xrightarrow{f} B \to 0 \quad \longrightarrow \quad \mathrm{Hom}_R(M,A) \to \mathrm{Hom}_R(M,B) \to 0, \quad \psi \mapsto f \circ \psi$$


$$\forall \varphi: M \to B \quad \exists \psi: M \to A \text{ t.c. } \varphi = f \circ \psi$$

- Iniettivo:
$$0 \to A \xrightarrow{f} B \rightsquigarrow 0 \leftarrow \mathrm{Hom}(A,M) \leftarrow \mathrm{Hom}(B,M), \quad \varphi \circ f \longleftarrow \varphi$$


$$\forall \psi: A \to M \quad \exists \varphi: B \to M \text{ t.c. } \psi = \varphi \circ f$$

Piatti R anello

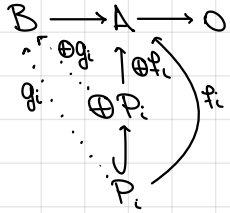
- R è piatto, perché $\_ \otimes_R R = id$ è esatto
- $\otimes$ commutano con $\oplus$ (aggiunzione), e quindi se $\{M_i\}$ sono piatti, anche $\oplus M_i$ è piatto

$$0 \longrightarrow A \longrightarrow B \xrightarrow{\otimes(\oplus M_i)} 0 \longrightarrow A\otimes(\oplus M_i) \longrightarrow B\otimes(\oplus M_i)$$
$$0 \longrightarrow \oplus(A\otimes M_i) \longrightarrow \oplus(B\otimes M_i)$$
che è iniettiva

- In particolare, ogni modulo libero è piatto.
- S parte moltiplicativa, $S^{-1}R$ è un R-modulo piatto poiché $M\otimes_R S^{-1}R = S^{-1}M$, il funtore $\otimes_R S^{-1}R$ coincide con S^{-1}, che è esatto (la distinzione fra R-mod e $S^{-1}R$-mod non è importante)

Proiettivi

- R è proiettivo: $\mathrm{Hom}_R(R,\_) = id$ è esatto
- $\oplus$ di proiettivi è proiettiva:



- In particolare, ogni modulo libero è proiettivo.

Costruzione $F(M) = \bigoplus_{m\in M} R \longrightarrow M \longrightarrow 0$

basta dare una mappa $R \longrightarrow M$ $\forall m\in M$

sulla componente m prendo $1 \longmapsto m$

Se M è fin gen da $m_1,\dots,m_n$. posso prendere

$$F_{fg}(M) = \bigoplus_{i=1}^{n} R \longrightarrow M$$
$$e_i \longmapsto m_i$$

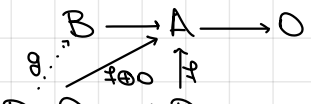
> **proposizione** La categoria Mod$_R$ ha abbastanza proiettivi, cioè per ogni $M\in$Mod$_R$ $\exists\ P \longrightarrow M \longrightarrow 0$ con P proiettivo.

Risoluzioni proiettive

$$\dots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

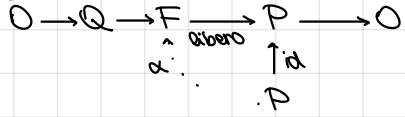
Lemma P proiettivo $\iff \exists Q$ t.c. $P \oplus Q$ libero

DIMOSTRAZIONE

($\Leftarrow$)


$g \circ (P \hookrightarrow P \oplus Q)$ solleva f

$P \oplus Q$ libero $\Rightarrow$ proiettivo $\Rightarrow$ $f \circ \alpha$ si solleva

($\Rightarrow$)


$\iff F \simeq P \oplus Q$

□

corollario Proiettivo $\Rightarrow$ piatto.

DIMOSTRAZIONE

Sia P proiettivo, Q t.c. $P \oplus Q = F$ libero

$0 \to A \to B \xrightarrow{\otimes F} 0 \to A \otimes F \to B \otimes F$ esatta

$0 \to A \otimes P \oplus A \otimes Q \to B \otimes P \oplus B \otimes Q$

In particolare, $A \otimes P \to B \otimes P$ è iniettiva

□

Lemma (R, M) locale (non necess. Noetheriano), P R-mod fin gen. proiettivo. Allora P è libero.

DIMOSTRAZIONE

$P \otimes R/M = P/MP$ è uno S.V. su R/M di dim finita

Diciamo che $\overline{m}_1, \dots, \overline{m}_n$ sia una base: la solleva a $m_1, \dots, m_n$ di M

Per Nak, $\langle m_1, \dots, m_n \rangle = M$

$0 \to Q \to R^n \to P \to 0$, $e_i \mapsto m_i$

Per proiettività, la successione spezza: $R^n = P \oplus Q$

Quozientando per M: $(R/M)^n \simeq P/MP \oplus Q/MQ$

dim n dim n $\Rightarrow$ dim 0

$\Rightarrow Q = MQ$ Siccome $Q = R^n/P$ è un quoziente di R^n, è fingen.

Posso applicare Nak: $Q = 0$.

Allora $P \simeq R^n$

□

Oss Kaplansky: su (A, M) locale, tutti i proiettivi sono liberi

proposizione R anello Noetheriano, M R-modulo fin gen.
M è proiettivo $\iff$ $M_\mathfrak{p} := M \otimes_R R_\mathfrak{p}$ è libero $\forall \mathfrak{p} \in \operatorname{Spec} R$
$\iff$ $M_\mathfrak{p} := M \otimes_R R_\mathfrak{p}$ è libero $\forall \mathfrak{p} \in \operatorname{Spec}_{\max} R$

def. Un R-modulo M si dice finitamente presentato se esiste una successione esatta $R^m \longrightarrow R^n \longrightarrow M \longrightarrow 0$
(nel caso Noetheriano vuol dire solo fin gen)

Lemma A R-mod fin. presentato. Allora $\forall \mathfrak{p} \in \operatorname{Spec} R$
$\operatorname{Hom}_R(A,B) \otimes_R R_\mathfrak{p} \simeq \operatorname{Hom}_{R_\mathfrak{p}}(A_\mathfrak{p}, B_\mathfrak{p})$
$\varphi \otimes \frac{r}{s} \longmapsto \left(\frac{a}{s'} \longmapsto \varphi(a) \otimes \frac{r}{ss'}\right)$

DIMOSTRAZIONE
- Se A è libero, $A \simeq R^n$:
$\operatorname{Hom}_R(R^n, B) \otimes_R R_\mathfrak{p} \overset{?}{\simeq} \operatorname{Hom}_{R_\mathfrak{p}}(R_\mathfrak{p}^n, B_\mathfrak{p})$
$B^n \otimes_R R_\mathfrak{p} = (B \otimes_R R_\mathfrak{p})^n$
perché $\otimes$ commuta con $\oplus$
- Se A è fin. pres: fissiamo $R^m \longrightarrow R^n \longrightarrow A \longrightarrow 0$
Applico prima $\operatorname{Hom}(-,B)$ e poi $\otimes R_\mathfrak{p}$: trovo

$$\begin{array}{ccccccc} \operatorname{Hom}(R^m,B)\otimes R_\mathfrak{p} & \longleftarrow & \operatorname{Hom}(R^n,B)\otimes R_\mathfrak{p} & \longleftarrow & \operatorname{Hom}(A,B)\otimes R_\mathfrak{p} & \longleftarrow & 0 \\ \wr & & \wr & & \downarrow & & \wr \\ \operatorname{Hom}(R_\mathfrak{p}^m, B_\mathfrak{p}) & \longleftarrow & \operatorname{Hom}(R_\mathfrak{p}^n, B_\mathfrak{p}) & \longleftarrow & \operatorname{Hom}(A_\mathfrak{p}, B_\mathfrak{p}) & \longleftarrow & 0 \end{array}$$

esatta (prima $\otimes R_\mathfrak{p}$ poi $\operatorname{Hom}(-,B_\mathfrak{p})$)
Il lemma dei 5 dice che la freccia centrale è un isomorfismo. □

DIMOSTRAZIONE
($\Longrightarrow$) Supponiamo M proiettivo f.g.
Scelgo $M \oplus Q \cong R^n$
localizzando: $M_\mathfrak{p} \oplus Q_\mathfrak{p} \simeq R_\mathfrak{p}^n \Longrightarrow M_\mathfrak{p}$ proiettivo e fin gen perché $M_\mathfrak{p} \subseteq R_\mathfrak{p}^n$ e $R_\mathfrak{p}$ Noeth.
$\Longrightarrow M_\mathfrak{p}$ libero
($\Longleftarrow$) $B \longrightarrow A \longrightarrow 0$ devo mostrare che $\operatorname{Hom}(M,B) \longrightarrow \operatorname{Hom}(M,A)$ è surgettiva

$$\iff \operatorname{Hom}(M,B)_\mathfrak{p} \longrightarrow \operatorname{Hom}(M,A)_\mathfrak{p} \text{ è surg } \forall \mathfrak{p}$$
$$\overset{\text{lemma}}{\iff} \operatorname{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, B_\mathfrak{p}) \longrightarrow \operatorname{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, A_\mathfrak{p}) \text{ è surg. } \forall \mathfrak{p}$$

che è vero perché $B_\mathfrak{p} \longrightarrow A_\mathfrak{p} \longrightarrow 0$ e $M_\mathfrak{p}$ è libero. □

Iniettivi

- Prodotti diretti di iniettivi sono iniettivi

Lemma: criterio di Baer — R anello, M R-modulo
M è iniettivo $\iff$ per ogni ideale $I \lhd R$ e ogni $f: I \to M$
$\exists g: R \to M$ t.c. $g|_I = f$.

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \hookrightarrow & R \\ & & {\scriptstyle f}\downarrow & \swarrow_{\exists g} & \\ & & M & & \end{array}$$

DIMOSTRAZIONE

($\Longrightarrow$) OVVIO

($\Longleftarrow$) Prendiamo $0 \to A \to B$ con $f: A \to M$

$\mathcal{Y} = \{(A', f') \mid A \subseteq A' \subseteq B,\ f': A' \to M,\ f'|_A = f\}$

$\mathcal{Y}$ soddisfa le ipotesi di Zorn

Sia $(\tilde{A}, \tilde{f})$ massimale

Se $\tilde{A} = B$ ho finito. Altrimenti prendo $b \in B \setminus \tilde{A}$.

Sia $I = \{r \in R \mid rb \in \tilde{A}\}$ è un ideale di R.

Considero

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \xrightarrow{\cdot r} & R \\ & & \downarrow & \swarrow_{\exists g} & \\ & & M & & \end{array} \qquad I \xrightarrow{\cdot r} M \text{ via } \tilde{f}(rb)$$

$g: R \to M$ t.c.
se $r \in I$, $g(r) = \tilde{f}(rb)$

$\tilde{A} + \langle b \rangle \longrightarrow M$

$\tilde{a} + rb \longmapsto \tilde{f}(\tilde{a}) + g(r)$

Verifichiamo la buona def:

$\tilde{a}_1 + r_1 b = \tilde{a}_2 + r_2 b \longrightarrow \tilde{A} \ni \tilde{a}_1 - \tilde{a}_2 = (r_2 - r_1)b \implies r_2 - r_1 \in I$

Quindi $g(r_2 - r_1) = \tilde{f}((r_2 - r_1)b)$

La proprietà da verificare è

$\tilde{f}(\tilde{a}_1) + g(r_1) \stackrel{?}{=} \tilde{f}(\tilde{a}_2) + g(r_2)$

$\iff \tilde{f}(\tilde{a}_1 - \tilde{a}_2) \stackrel{?}{=} g(r_2 - r_1) = \tilde{f}((r_2 - r_1)b) = \tilde{f}(\tilde{a}_1 - \tilde{a}_2)$ □

Lemma — In $\mathrm{Mod}_{\mathbb{Z}} = \mathrm{Ab}$, M è iniettivo $\iff$ M è divisibile, cioè
$\forall n \neq 0$ la funzione $[n]: M \to M$ è suriettiva.

DIMOSTRAZIONE

M iniettivo $\iff \forall I \lhd \mathbb{Z}$

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \longrightarrow & \mathbb{Z} \\ & & {\scriptstyle f}\downarrow & \swarrow_{\exists g} & \\ & & M & & \end{array}$$

1° caso: $I = (0)$, $f = 0$ e prendo $g = 0$

2° caso: $I = (n)$

$$\begin{array}{ccccc} 0 & \longrightarrow & n\mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & & {\scriptstyle n}\downarrow \ {\scriptstyle f}\downarrow & \swarrow_{g} & \\ & & m \quad M & & \end{array}$$

Se $f(n) = m$, $g(1)$ deve essere un el. di M t.c. $ng(1) = g(n) = f(n) = m$

Da questo segue l'equivalenza. □

esempio $\mathbb{Q}, \mathbb{Q}/\mathbb{Z}$ sono $\mathbb{Z}$-mod iniettivi

Lemma A R-mod, $T \in |Ab|$.
$\mathrm{Hom}_{\mathbb{Z}}(A,T) \simeq \mathrm{Hom}_R(A, \mathrm{Hom}_{\mathbb{Z}}(R,T))$
dove $\mathrm{Hom}_{\mathbb{Z}}(R,T)$ è un R-mod con moltiplicazione
$(r \cdot \varphi)(r') := \varphi(rr')$
Inoltre $\forall A \longrightarrow B$ omomorfismo di R-moduli

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbb{Z}}(A,T) & \longleftarrow & \mathrm{Hom}_{\mathbb{Z}}(B,T) \\ \| & & \| \\ \mathrm{Hom}_R(A, \mathrm{Hom}_{\mathbb{Z}}(R,T)) & \longleftarrow & \mathrm{Hom}_R(B, \mathrm{Hom}_{\mathbb{Z}}(R,T)) \end{array}$$

DIMOSTRAZIONE

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbb{Z}}(A,T) & \longleftrightarrow & \mathrm{Hom}_R(A, \mathrm{Hom}_{\mathbb{Z}}(R,T)) \\ \varphi & \longmapsto & (a \longmapsto (r \longmapsto \varphi(ra))) \\ (a \longmapsto (\psi(a))(1)) & \longleftarrow & \psi \end{array}$$

□

corollario Se $Q \in |Ab|$ iniettivo, $\mathrm{Hom}_{\mathbb{Z}}(R,Q)$ è un R-mod iniettivo.

DIMOSTRAZIONE

$Q' := \mathrm{Hom}_{\mathbb{Z}}(R,Q)$

$$0 \longrightarrow A \longrightarrow B$$
$$\downarrow$$
$$Q$$

$$\begin{array}{ccc} \mathrm{Hom}_R(B,Q') & \longrightarrow & \mathrm{Hom}_R(A,Q') \text{ surg?} \\ \| & \hookrightarrow & \| \\ \mathrm{Hom}_{\mathbb{Z}}(B,Q) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(A,Q) \end{array}$$

□

proposizione Mod_R ha abbastanza iniettivi, cioè
$\forall M \in |\mathrm{Mod}_R|$ $\exists I$ iniettivo con $\psi : M \longrightarrow I$ iniettiva.

DIMOSTRAZIONE

$I := \prod_{\varphi \in \mathrm{Hom}_R(M,Q)} Q$, dove $Q := \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$, è iniettivo

Costruiamo $\psi : M \longrightarrow I$, cioè costruiamo una $M \longrightarrow Q$ per ogni fattore: se fattore ϕ uso ϕ.
Vediamo che ψ è iniettiva: $\ker \psi = \{0\} \iff \forall m \in M$ $\exists \phi$ t.c. $\phi(m) \neq 0$

$$\begin{array}{ccccc} 0 & \longrightarrow & \langle m \rangle & \longrightarrow & M \\ & & \varphi \downarrow & \swarrow \tilde{\varphi} & \\ & & \mathbb{Q}/\mathbb{Z} & & \end{array}$$

Costruire $M \longrightarrow Q \in \mathrm{Hom}_R(M,Q)$
$\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$
$\langle m \rangle = \mathbb{Z}$ o $\mathbb{Z}/n\mathbb{Z}$

quindi posso costruire φ non banale
In Ab, $\mathbb{Q}/\mathbb{Z}$ è iniettivo

□

Obiettivo Sia $F: \mathrm{Mod}_R \longrightarrow \mathrm{Mod}_S$ un funtore esatto a sx (R, S non necess comm)

$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ succ. esatta corta

$0 \longrightarrow F(A) \longrightarrow F(B) \longrightarrow F(C) \longrightarrow (R^1F)(A) \longrightarrow (R^1F)(B) \longrightarrow (R^1F)(C) \longrightarrow$

$\longrightarrow (R^2F)(A) \longrightarrow \dots$

Se F è esatto a dx:

$\dots \longrightarrow (L^1F)(A) \longrightarrow (L^1F)(B) \longrightarrow (L^1F)(C) \longrightarrow F(A) \longrightarrow F(B) \longrightarrow F(C) \longrightarrow 0$

Def. Un complesso (di catene) coomologico di R-moduli è una successione

$$\dots \longrightarrow A^{i-1} \longrightarrow A^i \xrightarrow{d_A^i} A^{i+1} \xrightarrow{d_A^{i+1}} A^{i+2} \longrightarrow \dots$$

tali che $d_A^{i+1} \circ d_A^i = 0 \ \forall i$

Numerazione omologica: $A_{\cdot i} = A^i$

La coomologia del complesso $(A^\bullet, d_A^\bullet)$ si ottiene come segue.

- gli i-cocicli $Z^i(A^\bullet) = \ker d_A^i \subseteq A^i$
- gli i-cobordi $B^i(A^\bullet) = \mathrm{Im}\, d_A^{i-1} \subseteq Z^i(A) \subseteq A^i$
- l'i-esimo gruppo di coomologia è

$$H^i(A^\bullet) = Z^i(A^\bullet)/B^i(A^\bullet)$$

Diciamo che il complesso è aciclico o esatto se $H^i(A^\bullet) = 0 \ \forall i$.

Un morfismo di complessi $\phi^\bullet : A^\bullet \longrightarrow B^\bullet$ è è una collezione di mappe $\phi^i : A^i \longrightarrow B^i$

$$\begin{array}{ccccccc} \dots \longrightarrow & A^i & \xrightarrow{d_A^i} & A^{i+1} & \longrightarrow & A^{i+2} & \longrightarrow \dots \\ & \downarrow{\scriptstyle \phi^i} & \circlearrowright & \downarrow{\scriptstyle \phi^{i+1}} & \circlearrowright & \downarrow{\scriptstyle \phi^{i+2}} & \\ \dots \longrightarrow & B^i & \xrightarrow{d_B^i} & B^{i+1} & \longrightarrow & B^{i+2} & \longrightarrow \dots \end{array}$$

t.c. $\phi^{i+1} \circ d_A^i = d_B^i \circ \phi^i \ \forall i$

Oss Sia $\phi^\bullet : A^\bullet \longrightarrow B^\bullet$ un morfismo di complessi.

Ci sono mappe indotte $H^i(\phi^\bullet) : H^i(A^\bullet) \longrightarrow H^i(B^\bullet) \quad \forall i$

$$a_i \in Z^i(A^\bullet) \qquad [a_i] \longmapsto [\phi^i(a_i)]$$

1) $\phi^i(a_i) \in Z^i(B^\bullet)$: $d_B^i \phi^i(a_i) = \phi^{i+1} \circ \underbrace{d_A^i(a_i)}_{=0}$

2) passa al quoziente: $\phi^i(d_A^{i-1}(a_{i-1})) = d_B^{i-1} \circ \phi^{i-1}(a_{i-1})$ quindi ϕ^i manda $B^i(A^\bullet)$ in $B^i(B^\bullet)$

Oss $H^i(A^\bullet \oplus B^\bullet) = H^i(A^\bullet) \oplus H^i(B^\bullet)$. Ogni H^i è un funtore additivo $\mathrm{Ch}_R \longrightarrow \mathrm{Mod}_R$

Def. Siano $A^\bullet, B^\bullet$ due complessi.

Un morfismo di complessi $\phi^\bullet : A^\bullet \longrightarrow B^\bullet$ è un quasi-isomorfismo se $H^i(\phi^\bullet)$ è un isomorfismo $\forall i$

Due morfismi $\phi^\bullet, \psi^\bullet : A^\bullet \longrightarrow B^\bullet$ sono omotopi (chain homotopic)

$$\begin{array}{ccccccc} \dots \longrightarrow & A^i & \longrightarrow & A^{i+1} & \longrightarrow & A^{i+2} & \longrightarrow \dots \\ & \swarrow{\scriptstyle k_i} \downarrow{\scriptstyle \phi^i - \psi^i} & \swarrow & \downarrow{\scriptstyle \phi^{i+1} - \psi^{i+1}} & \swarrow & \downarrow{\scriptstyle \phi^{i+2} - \psi^{i+2}} & \\ \dots \longrightarrow & B^i & \longrightarrow & B^{i+1} & \longrightarrow & B^{i+2} & \longrightarrow \dots \end{array}$$

se $\exists\, k_i : A^i \longrightarrow B^{i-1}$ t.c. $\phi^i - \psi^i = d_B^{i-1} \circ k_i + k_{i+1} \circ d_A^i \ \forall i$.

Oss Se $\phi^\bullet$ e $\psi^\bullet$ sono omotope, $H^i(\phi^\bullet) = H^i(\psi^\bullet)\ \forall i$.

$[a_i] \in H^i(A),\ a_i \in Z^i(A^\bullet)$ $\quad \phi^i(a_i) - \psi^i(a_i) = d_B^{i-1} \circ k^i(a_i) + k^{i+1} \circ d_A^i(a_i) = d_B^{i-1} \circ k^i(a_i)$ è un coborso

$\Rightarrow [\phi^i(a_i)] = [\psi^i(a_i)] \in H^i(B^\bullet)$

Def. Diciamo che $\phi^\bullet : A^\bullet \longrightarrow B^\bullet$, $\psi^\bullet : B^\bullet \longrightarrow A^\bullet$ sono equivalenze omotopiche se $\phi^\bullet \circ \psi^\bullet$ e $\psi^\bullet \circ \phi^\bullet$ sono omotope all'identità.

In particolare, $\phi^\bullet$ e $\psi^\bullet$ sono quasi-isomorfismi:

$\phi^\bullet \circ \psi^\bullet \sim id^\bullet \implies H^i(\phi^\bullet \circ \psi^\bullet) = H^i(id^\bullet)$

$H^i(\phi^\bullet) \circ H^i(\psi^\bullet) \quad id$

Def. Una successione esatta di complessi è

$0 \longrightarrow A^\bullet \longrightarrow B^\bullet \longrightarrow C^\bullet \longrightarrow 0$

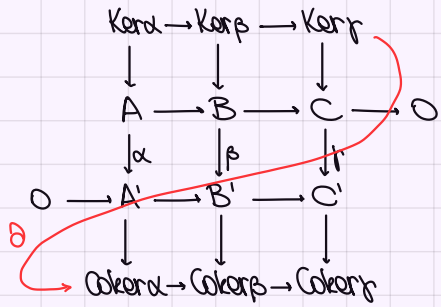
t.c. $\forall i$ $0 \longrightarrow A^i \longrightarrow B^i \longrightarrow C^i \longrightarrow 0$ è esatta.

Proposizione Sia $0 \longrightarrow A^\bullet \longrightarrow B^\bullet \longrightarrow C^\bullet \longrightarrow 0$ esatta corta di complessi.

C'è una successione esatta lunga

$$\dots \longrightarrow H^{i-1}(C^\bullet) \xrightarrow{\partial} H^i(A^\bullet) \longrightarrow H^i(B^\bullet) \longrightarrow H^i(C) \xrightarrow{\partial} H^{i+1}(A^\bullet) \longrightarrow \dots$$

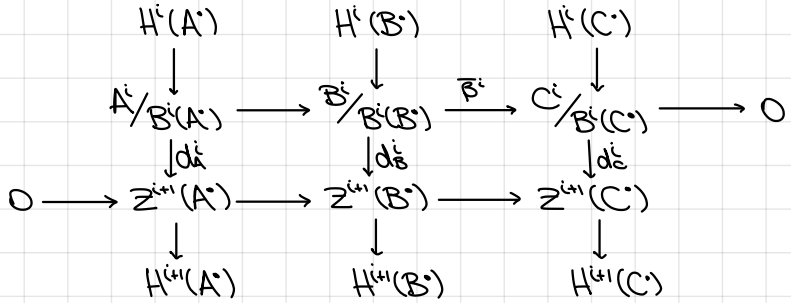
Lemma del serpente



la successione

$\mathrm{Ker}\,\alpha \longrightarrow \mathrm{Ker}\,\beta \longrightarrow \mathrm{Ker}\,\gamma \longrightarrow \mathrm{Coker}\,\alpha \longrightarrow \mathrm{Coker}\,\beta \longrightarrow \mathrm{Coker}\,\gamma$ è esatta.

DIMOSTRAZIONE



le successioni orizzontali sono esatte:

- iniettività di $Z^{i+1}(A^\bullet) \xrightarrow{\alpha^{i+1}} Z^{i+1}(B^\bullet)$: α^{i+1} è iniettiva
- analogamente, $B^i/B^i(B^\bullet) \longrightarrow C^i/B^i(C^\bullet)$ è surgettiva
- esattezza in $B^i/B^i(B^\bullet)$: se $\bar{b} \in B^i/B^i(B^\bullet)$ t.c. $\bar{\beta}^i(\bar{b}) = 0$,

allora $\beta^i(b) \in B^i(C^\bullet)$: $\beta^i(b) = d_C^{i-1}(c_{i-1}) = d_C^{i-1}(\beta^{i-1}(b_{i-1})) = \beta^i \circ d_B^{i-1}(b_{i-1})$

$\Rightarrow \beta^i(b - d_B^{i-1}(b_{i-1})) = 0$

$\Rightarrow b - d_B^{i-1}(b_{i-1}) = \alpha^i(a_i)$

$\Rightarrow \bar{b} = \bar{\alpha}^i(\bar{a}_i)$

$\bar{\beta}^i \circ \bar{\alpha}^i = 0$ è facile.

□

Lemma

$$\begin{array}{ccccccc} 0 & \longrightarrow & A^\cdot & \longrightarrow & B^\cdot & \longrightarrow & C^\cdot \longrightarrow 0 \quad \text{esatta} \\ & & \downarrow f^\cdot & & \downarrow g^\cdot & & \downarrow h^\cdot \\ 0 & \longrightarrow & D^\cdot & \longrightarrow & E^\cdot & \longrightarrow & F^\cdot \longrightarrow 0 \quad \text{esatta} \end{array}$$

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & H^i(A^\cdot) & \longrightarrow & H^i(B^\cdot) & \longrightarrow & H^i(C^\cdot) & \xrightarrow{\partial} & H^{i+1}(A^\cdot) \longrightarrow \cdots \\ & & H^i(f^\cdot)\downarrow & \curvearrowright & H^i(g^\cdot)\downarrow & \curvearrowright & H^i(h^\cdot)\downarrow & \curvearrowright & \downarrow \\ \cdots & \longrightarrow & H^i(D^\cdot) & \longrightarrow & H^i(E^\cdot) & \longrightarrow & H^i(F^\cdot) & \xrightarrow{\partial} & H^{i+1}(D^\cdot) \longrightarrow \cdots \end{array}$$

Strategia Partire con $0 \to A^\cdot \to B^\cdot \to C^\cdot \to 0$, F esatto a dx

- Costruire $0 \to P^A_\cdot \to P^B_\cdot \to P^C_\cdot \to 0$
- Applicare F: $0 \to F(P^A_\cdot) \to F(P^B_\cdot) \to F(P^C_\cdot) \to 0$ esatta
- Dalla prop:

$$H_{i+1}(F(P^C_\cdot)) \to H_i(F(P^A_\cdot)) \to H_i(F(P^B_\cdot)) \to H_i(F(P^C_\cdot)) \to H_{i-1}(F(P^A_\cdot)) \to \dots$$

- Serve che $H_0(F(P^A_\cdot)) = F(A)$ e poi in generale definiremo $(L_iF)(A) = H_i(F(P^A_\cdot))$

Risoluzioni proiettive

Def. Dato $A \in Mod_R$, una risoluzione proiettiva di A è una sequenza esatta

$$\dots \to P^A_2 \to P^A_1 \to P^A_0 \to A \to 0$$

in cui i P^A_i sono moduli proiettivi

Una risoluzione iniettiva è

$$0 \to A \to I^0_A \to I^1_A \to I^2_A \to \dots$$

proposizione Esistono sempre:

$$\dots \to P^A_1 \xrightarrow{\pi_1} \ker\pi_0 \subseteq P^A_0 \xrightarrow{\pi_0} A \to 0$$

Lemma

$$\begin{array}{ccccccccc} \cdots & \xrightarrow{\pi_2} & P_1 & \xrightarrow{\pi_1} & P_0 & \xrightarrow{\pi_0} & A & \longrightarrow & 0 \\ & & & & & & \downarrow{\scriptstyle \alpha_{-1}} & & \\ \cdots & \xrightarrow{\beta_2} & B_1 & \xrightarrow{\beta_1} & B_0 & \xrightarrow{\beta_0} & B & \longrightarrow & 0 \end{array}$$

risoluzione proiettiva

complesso aciclico

(i) Esistono $\alpha_i : P_i \longrightarrow B_i$ $\forall i \geq 0$ che fanno commutare tutto, cioè $\alpha_i \circ \pi_{i+1} = \beta_{i+1} \circ \alpha_{i+1}$

(ii) Se $\{\alpha_i\}$ e $\{\beta_i\}$ hanno questa proprietà, allora $\alpha_\bullet$ e $\beta_\bullet$ sono omotope.

corollario

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & A \longrightarrow 0 \\ & & \downarrow{\scriptstyle \alpha_2} & \overset{id}{\searrow} & \downarrow{\scriptstyle \alpha_1} & \overset{id}{\searrow} & \downarrow{\scriptstyle \alpha_0} & \overset{id}{\searrow} & \| \\ \cdots & \longrightarrow & Q_2 & \longrightarrow & Q_1 & \longrightarrow & Q_0 & \longrightarrow & A \longrightarrow 0 \\ & & \downarrow{\scriptstyle \beta_2} & \swarrow & \downarrow{\scriptstyle \beta_1} & \swarrow & \downarrow{\scriptstyle \beta_0} & \swarrow & \| \\ \cdots & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & A \longrightarrow 0 \end{array}$$

Per il lemma, $\beta_\bullet \circ \alpha_\bullet$ è omotopa ad id. e viceversa.

DIMOSTRAZIONE

(i)
$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & P_2 & \longrightarrow & P_1 & \xrightarrow{\pi_1} & P_0 & \xrightarrow{\pi_0} & A & \longrightarrow & 0 \\ & & & & & \searrow^{\alpha_0} & \downarrow & \searrow & \downarrow{\scriptstyle \alpha_{-1}} & & \\ \cdots & \longrightarrow & B_2 & \longrightarrow & B_1 & \longrightarrow & B_0 & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

α_0 esiste per proprietà dei proiettivi.

Per usare la proiettività per sollevare $\alpha_0 \circ \pi_1$ a P_1, mi basta sapere che $B_1 \longrightarrow 0 \geq \mathrm{Im}(\alpha_0 \circ \pi_1)$

Ora $\mathrm{Im}(B_1 \longrightarrow B_0) = \ker \beta_0$, quindi basta verificare che

$$\mathrm{Im}(\alpha_0 \circ \pi_1) \subseteq \ker \beta_0 \iff \beta_0 \circ \alpha_0 \circ \pi_1 = 0 \iff \alpha_{-1} \circ \underbrace{\pi_0 \circ \pi_1}_{=0} = 0$$

Poi si procede per induzione.

(ii)
$$\begin{array}{ccccccccc} P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & A & \longrightarrow & 0 \\ \| & & \downarrow{\scriptstyle \alpha_1} \| \downarrow{\scriptstyle \beta_1} & \swarrow{\scriptstyle k_0} & \downarrow{\scriptstyle \alpha_0} \| \downarrow{\scriptstyle \beta_0} & \swarrow{\scriptstyle k_{-1}} & \downarrow{\scriptstyle \alpha_{-1}} & & \\ B_2 & \longrightarrow & B_1 & \longrightarrow & B_0 & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

Tesi: $\exists k_i : P_i \longrightarrow B_{i+1}$ t.c. $\alpha_i - \beta_i = \beta_{i+1} \circ k_i + k_{i-1} \circ \pi_i$ $\forall i$

$i=-1$: $0 = \alpha_{-1} - \beta_{-1} = \beta_0 \circ k_{-1} + k_{-2} \circ \pi_{-1}$: prendo $k_{-1} = 0$

$i=0$: $\alpha_0 - \beta_0 = \beta_1 \circ k_0$

Ho $\alpha_0 - \beta_0 : P_0 \longrightarrow B$ con $\mathrm{Im}(\alpha_0 - \beta_0) \subseteq \mathrm{Im}(B_1 \longrightarrow B_0)$

Per proiettività, ho il sollevamento da P_0 a B_1

Per il contenimento: $\mathrm{Im}(\alpha_0 - \beta_0) \subseteq \ker \beta_0 \iff \beta_0 \circ (\alpha_0 - \beta_0) = 0$

$$\iff \alpha_{-1} \circ \pi_0 - \beta_{-1} \circ \pi_0 = 0$$

Poi si procede per induzione. □

Gruppo di Picard

ES Sia R un anello Noetheriano, M R-mod proiettivo fin.gen
Consideriamo la funzione $r: \operatorname{Spec} R \longrightarrow \mathbb{N}$. Come varia r?
$P \longmapsto \operatorname{rk}_{R_P}(M_P)$

Oss Il rango è ben definito: se $M_P \simeq R_P^r$, allora
$r = \dim_{R_P/PR_P}(M_P/PM_P)$ $\quad M_P/PM_P \simeq R_P^r/PR_P^r \simeq (R_P/PR_P)^n$

SOL Siano $P \subset Q$ due primi
$$(M_Q)_{PR_Q} \simeq (R_Q^{r(Q)})_{PR_Q} \simeq (R_P)^{r(Q)}$$
$$M_P \simeq R_P^{r(P)}$$
$\Longrightarrow r(P) = r(Q)$
Se P è primo minimale, r è costante su $V(P) = \{Q \in \operatorname{Spec} R \mid Q \supset P\}$,
e quindi sulle componenti connesse. □

In particolare, se R è un dominio, abbiamo un ben definito "rango"
per i moduli proiettivi.

ES R dominio Noetheriano, M R-mod proiettivo di rango 1 fin.gen.
Definiamo $M^* := \operatorname{Hom}(M, R)$
Allora $M \otimes M^* \simeq R$ come R-mod.

SOL Ho $\varphi: M \otimes M^* \longrightarrow R$ è la stessa cosa
che descrivere $\Phi: M \times M^* \longrightarrow R$
$(m, f) \longmapsto f(m)$ è bilineare
Per dimostrare che φ è isomorfismo, basta farlo in ogni localizzazione
$\varphi_P: (M \otimes M^*)_P \longrightarrow R_P$
$M_P \otimes M_P^* = M_P \otimes \operatorname{Hom}_{R_P}(M_P, R_P) \simeq R_P \otimes \operatorname{Hom}_{R_P}(R_P, R_P) \simeq R_P$
$\operatorname{Hom}_R(M, R) \otimes R_P \simeq \operatorname{Hom}_{R_P}(M_P, R_P) \simeq \operatorname{Hom}_{R_P}(R_P, R_P) \simeq R_P$
Quindi M^* è loc. libero $\Longrightarrow$ proiettivo

Def. R dominio Noetheriano.
$\operatorname{Pic}(R) = (\{M$ R-moduli proiettivi fin.gen di rango $1\}/_{\simeq}, \otimes)$
$(M_1 \otimes M_2)_P \simeq (M_1)_P \otimes_{R_P} (M_2)_P \simeq R_P \otimes_{R_P} R_P \simeq R_P$
è associativo, l'el. neutro è R e l'inverso è M^*

ES Se R è un PID, $\operatorname{Pic}(R)$ è banale.

SOL Sia P un proiettivo: $\exists Q$ t.c. $P \oplus Q$ sia libero
$\Longrightarrow P$ sottomodulo di un libero $\overset{\text{PID}}{\Longrightarrow} P$ è libero

ES $R = \mathbb{Z}[\sqrt{-5}] = \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$. $\mathrm{Pic}(R) \neq \{1\}$

SOL $I = (2, 1+\sqrt{-5})$ non è principale $\Rightarrow$ non è libero

I è proiettivo: vediamo che è loc. libero

I_P è libero se R_P

Per $P=(0)$: I_P è libero se $\mathrm{Frac}(R)$ (sp. vett.)

Per P massimale: R_P è un DVR $\Rightarrow$ PID

I_P è principale e quindi libero

I non è principale:

$R/I = \frac{\mathbb{Z}[\sqrt{-5}]}{(2, 1+\sqrt{-5})} \simeq \frac{\mathbb{Z}[X]}{(X^2+5, 2, 1+X)} \simeq \mathbb{F}_2$

Supponiamo $I = (a+b\sqrt{-5})$

$R \longrightarrow I \subseteq R$

$r \longmapsto r(a+b\sqrt{-5})$ ha immagine I

Scrivo $R = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\sqrt{-5} \simeq \mathbb{Z}^2$ come $\mathbb{Z}$-mod

$\Phi : \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2$

$(1,0) \longmapsto (a,b)$

$(0,1) \longmapsto (-5b, a)$

Φ ha matrice $\begin{pmatrix} a & -5b \\ b & a \end{pmatrix}$

Voglio dire che $|\mathrm{Coker}\,\Phi| = \det M = a^2+5b^2 \neq 2$

Applico l'algoritmo di Euclide

es $\begin{pmatrix} 3 & -35 \\ 7 & 3 \end{pmatrix} \xrightarrow{[2]+12[1]} \begin{pmatrix} 3 & 1 \\ 7 & 87 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 3 \\ 87 & 7 \end{pmatrix} \xrightarrow{[2]-3[1]} \begin{pmatrix} 1 & 0 \\ 87 & 7-3\cdot 87 \end{pmatrix}$ □

ES R dominio di Dedekind, M R-mod proiettivo di rango 1 fin. gen.
Allora esiste $I \lhd R$ con $I \simeq M$ come R-mod.

SOL $K = \mathrm{Frac}(R)$

$\otimes M$ applicato a $0 \longrightarrow R \longrightarrow K$ dà $0 \longrightarrow R \otimes_R M \longrightarrow K \otimes_R M$ esatta

M proiettivo $\Rightarrow$ piatto $\quad 0 \longrightarrow M \longrightarrow K \xrightarrow{\simeq}$

$\langle \frac{\alpha_1}{s}, -, \frac{\alpha_t}{s} \rangle = \langle \frac{a_1}{s_1}, -, \frac{a_t}{s_t} \rangle$

$\Rightarrow M \subseteq \frac{1}{s}\cdot R \simeq R \quad \Rightarrow sM \subseteq R$ è un sottomod, cioè un ideale

(Un tale M si dice ideale frazionario). □

ES $I, J \lhd R$ dominio di Dedekind ($\Rightarrow$ automaticamente mod. proiettivi)
Allora $I \cdot J \simeq I \otimes J$

SOL $0 \longrightarrow J \longrightarrow R$ applicato a $\otimes I$ dà $0 \longrightarrow J \otimes I \xrightarrow{\text{ind\`oid}} R \otimes I \simeq I \hookrightarrow R$

$j \otimes i \longmapsto ji \longmapsto ji$

$0 \longrightarrow J \otimes I \longrightarrow IJ$ ed è surgettiva □

Conseguenza: $\mathrm{Pic}(\mathcal{O}_K) \simeq Cl(K)$

> Teorema $\quad \#Cl(K) < +\infty$

esempio $\mathrm{Pic}(\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}) = \mathrm{Pic}(\mathbb{Z}[\sqrt{-5}]) \simeq \mathbb{Z}/2\mathbb{Z}$

ES $\mathbb{Z}^{\mathbb{N}}$ non è libero

Lemma $f: \mathbb{Z}^{\mathbb{N}} \longrightarrow \mathbb{Z}$ omomorfismo t.c. $f|_{\mathbb{Z}^{(\mathbb{N})}} \equiv 0$.
Allora $f \equiv 0$ (dove $\mathbb{Z}^{(\mathbb{N})} = \bigoplus_{n\in\mathbb{N}} \mathbb{Z}$)

DIMOSTRAZIONE
Sia $x \in \mathbb{Z}^{\mathbb{N}}$ della forma $x=(x_n)=(p^n y_n)$ dove p è un primo e $y_n \in \mathbb{Z}$.
$f(x) = f((y_0, py_1, \underbrace{p^2}_{A}, p^3 y_3, 0, \_) + (0, \_, \underbrace{0, p^{n+1} y_{n+1}}_{B = p^{n+1}C}, \_)) = f(A) + f(B) = 0 + f(B) =$
$= p^{n+1} f(C)$
$\Longrightarrow f(x)$ è multiplo di p^{n+1} $\forall n \Longrightarrow f(x) = 0$
Se $x=(x_n)$ è qualsiasi $x = (2^n a_n + 3^n b_n)_n$
$\Longrightarrow f(x) = f((2^n a_n)_n) + f((3^n b_n)) = 0$ □

Lemma $f: \mathbb{Z}^{\mathbb{N}} \longrightarrow \mathbb{Z}$ omomorfismo di $\mathbb{Z}$-mod.
Sia $e_i = (0, \_, 0, \overset{i}{1}, 0, \_)$.
Allora $f(e_i) = 0$ $\forall i$ tranne un numero finito.

DIMOSTRAZIONE
Per assurdo, supponiamo di no
Considero $x=(2^{k_n})$ (k_n da scegliere, crescente) e calcolo
$f(x) = f(\sum_{i=1}^{j} 2^{k_i} e_i + 2^{k_{j+1}} \cdot b_j)$
$\Longrightarrow f(x) - \sum_{i=1}^{j} 2^{k_i} f(e_i) = 2^{k_{j+1}} f(b_j)$

$\frac{3}{4} > \left| \frac{f(x) - \sum_{i=0}^{j} 2^{k_i} f(e_i)}{2^{k_{j+1}}} \right| = |f(b_j)|$
Scelgo k_{j+1} t.c. $\left| \frac{\sum_{i=0}^{j} 2^{k_i} f(e_i)}{2^{k_{j+1}}} \right| < \frac{1}{2}$
Per j abbastanza grande, $|f(b_j)| < 1 \Rightarrow f(b_j) = 0$
Per j grande $b_j - b_{j+1} = c_j e_{j+1}$, con $c_j \in \mathbb{Z} \Longrightarrow 0 = f(b_j - b_{j+1}) = c_j f(e_{j+1})$ □

corollario $\mathrm{Hom}(\mathbb{Z}^{\mathbb{N}}, \mathbb{Z}) = \bigoplus_{n=0}^{+\infty} \mathbb{Z}\, pr_n$, dove $pr_n : \mathbb{Z}^{\mathbb{N}} \longrightarrow \mathbb{Z}$, $(x_m) \longmapsto x_n$

DIMOSTRAZIONE
($\supseteq$) è chiaro
($\subseteq$) $f \in \mathrm{Hom}(\mathbb{Z}^{\mathbb{N}}, \mathbb{Z})$, pongo $g := \sum_{i=0}^{+\infty} f(e_i)\, pr_i$
e osservo che f e g coincidono su $\mathbb{Z}^{(\mathbb{N})}$
$\Longrightarrow f - g|_{\mathbb{Z}^{(\mathbb{N})}} \equiv 0 \Longrightarrow f - g \equiv 0 \Longrightarrow f = g$ □

Teorema $\mathbb{Z}^{\mathbb{N}}$ non è libero.

DIMOSTRAZIONE
Per assurdo, $\mathbb{Z}^{\mathbb{N}} \simeq \bigoplus_{i\in I} \mathbb{Z}$
- $|I|$ finito: $|\mathbb{Z}^{\mathbb{N}}| = \mathfrak{c}$, $|\bigoplus_{i\in I} \mathbb{Z}| = \aleph_0$.
- $|I|$ infinito: $\mathrm{Hom}(\mathbb{Z}^{\mathbb{N}}, \mathbb{Z}) \simeq \bigoplus_{n=0}^{+\infty} \mathbb{Z}$ numerabile
$\mathrm{Hom}(\bigoplus_{i\in I} \mathbb{Z}, \mathbb{Z}) \simeq \prod_{i\in I} \mathbb{Z}$ più che numerabile ↯ □

Funtori derivati

$F: \mathrm{Mod}_R \longrightarrow \mathrm{Mod}_S$ funtore additivo esatto a dx

I funtori derivati sinistri $L_iF: \mathrm{Mod}_R \longrightarrow \mathrm{Mod}_S$ sono definiti come segue:

(i) dato $A \in |\mathrm{Mod}_R|$, scelgo una risoluzione proiettiva $P^A_\bullet \longrightarrow A \longrightarrow 0$, considero il complesso $F(P^A_\bullet)$, cioè

$$\ldots \longrightarrow F(P^A_2) \longrightarrow F(P^A_1) \longrightarrow F(P^A_0) \longrightarrow 0$$

e definisco $(L_iF)(A) := H_i(F(P^A_\bullet))$

(ii) dato $f: A \longrightarrow B$ omomorfismo di R-moduli, scelgo $P^A_\bullet \longrightarrow A \longrightarrow 0$ e $P^B_\bullet \longrightarrow B \longrightarrow 0$ risoluzioni proiettive

$$\begin{array}{ccccc} P^A_\bullet & \longrightarrow & A & \longrightarrow & 0 \\ \downarrow f_\bullet & & \downarrow f & & \\ P^B_\bullet & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

Applico F e trovo $F(P^A_\bullet) \xrightarrow{F(f_\bullet)} F(P^B_\bullet)$

$(L_iF)(f) := H_i(F(f_\bullet)) : H_i(F(P^A_\bullet)) \longrightarrow H_i(F(P^B_\bullet))$

Buona definizione

Se prendo $P^A_\bullet \longrightarrow A \longrightarrow 0$, $Q^A_\bullet \longrightarrow A \longrightarrow 0$ risoluzioni proiettive

$\alpha_\bullet, \beta_\bullet$ è un'equivalenza omotopica

$$\beta_\bullet \left(\begin{array}{ccccc} P^A_\bullet & \longrightarrow & A & \longrightarrow & 0 \\ \downarrow \alpha_\bullet & & \| & & \\ Q^A_\bullet & \longrightarrow & A & \longrightarrow & 0 \end{array} \right.$$

Oss $f_\bullet, g_\bullet$ omotope vuol dire

$$f_i - g_i = d_{i-1} \circ k + k \circ d_i$$

$$F(f_i) - F(g_i) = F(d_{i-1}) \circ F(k) + F(k) \circ F(d_i)$$

$\Longrightarrow$ l'omotopia si preserva applicando F

Applicando F, trovo che $F(\alpha_\bullet)$ e $F(\beta_\bullet)$ sono equivalenze omotopiche fra $F(P^A_\bullet) \underset{F(\beta_\bullet)}{\overset{F(\alpha_\bullet)}{\rightleftarrows}} F(Q^A_\bullet)$

Prendendo l'omologia in grado i

$$H_i(F(P^A_\bullet)) \underset{\sim}{\overset{\sim}{\rightleftarrows}} H_i(F(Q^A_\bullet))$$

La stessa verifica mostra la buona definizione di $(L_iF)(f)$

$L_0F = F$

$$\ldots \longrightarrow P^A_2 \longrightarrow P^A_1 \longrightarrow P^A_0 \longrightarrow A \longrightarrow 0$$

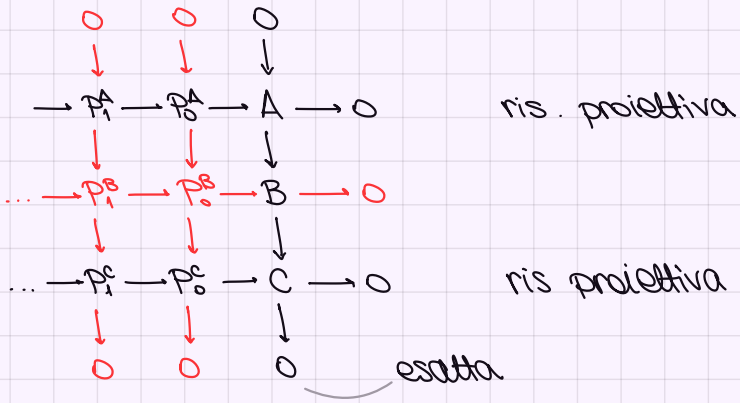
$$\Big) F$$

$$F(P^A_1) \xrightarrow{\partial_1} F(P^A_0) \xrightarrow{\partial_0} F(A) \longrightarrow 0 \quad \text{esatta}$$

$$F(P^A_\bullet) = \ldots \longrightarrow F(P^A_1) \xrightarrow{\partial_1} F(P^A_0) \xrightarrow{\tilde{\partial}_0} 0$$

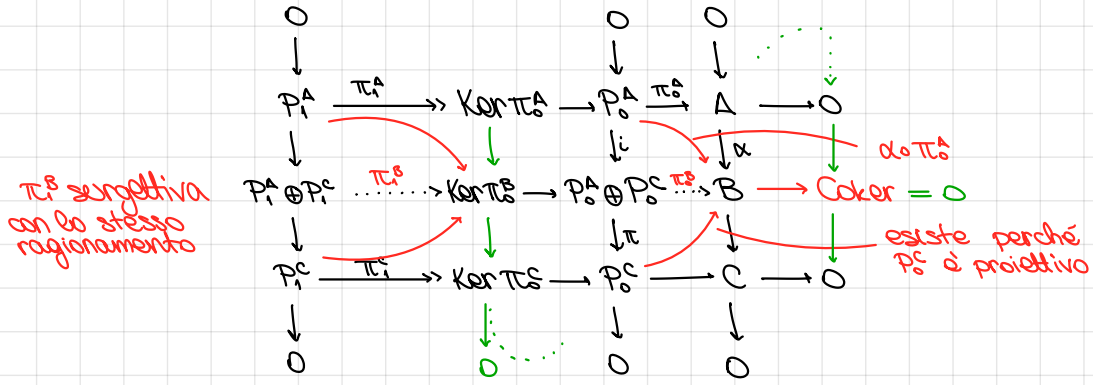
$$L_0F(A) = H_0(F(P^A_\bullet)) = \frac{Z^0(F(P^A_\bullet))}{B^0(F(P^A_\bullet))} = \frac{F(P^A_0)}{\mathrm{Im}\,\partial_1} = \mathrm{Im}\,\partial_0 = F(A)$$

Lemma del ferro di cavallo



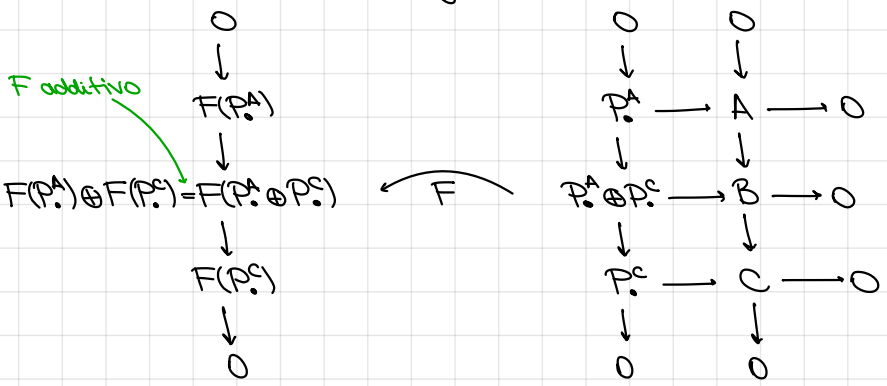
Oss le succ. esatte corte verticali splittano, quindi dobbiamo prendere $P^B_i := P^A_i \oplus P^C_i$

DIMOSTRAZIONE



□

Successione esatta lunga



è rimasta una succ. esatta corta di complessi

La succ. esatta lunga in omologia allora ci dà

$$\dots \to H_i(F(P^B_\bullet)) \to H_i(F(P^B_\bullet)) \to H_i(F(P^C_\bullet)) \xrightarrow{\partial} H_{i-1}(F(P^A_\bullet)) \to \dots$$

$$\dots \to L_iF(C) \to L_iF(B) \to L_iF(C) \to L_{i-1}F(A) \to \dots$$

$$\dots \to \underset{A}{L_0F(A)} \to \underset{B}{L_0F(B)} \to \underset{C}{L_0F(C)} \to 0$$

Commenti

1) Se P è proiettivo, $L_iF(P) = (0)$ per $i > 0$

Posso prendere la risoluz. proiettiva $\quad \cdots \to 0 \to P \xrightarrow{\sim} P \to 0$

$\cdots \to 0 \to F(P) \xrightarrow{\sim} F(P) \to 0$

L'omologia in grado $i > 0$ è banale

"Dimension shifting": $0 \to B \to P \to A \to 0$ con P proiettivo

$$L_1F(B) \to 0 \to L_1F(A) \to F(B) \to F(P) \to F(A) \to 0$$

$$L_2F(A) \leftarrow 0 \leftarrow L_2F(B) \leftarrow L_3F(A) \leftarrow 0 \leftarrow \dots$$

$\Rightarrow L_{n+1}F(A) = L_nF(B)$ per ogni $n \geq 1$.

2) $\quad 0 \to A_\bullet \to B_\bullet \to C_\bullet \to 0$

$\quad\quad\quad\quad \downarrow \quad \downarrow \quad \downarrow$

$\quad 0 \to D_\bullet \to E_\bullet \to F_\bullet \to 0$

$H_i(A_\bullet) \to H_i(B_\bullet) \to H_i(C_\bullet) \to H_{i-1}(A_\bullet)$

$H_i(D_\bullet) \to H_i(E_\bullet) \to H_i(F_\bullet) \to H_{i-1}(D_\bullet)$

Questo implica

$$\begin{array}{ccccccc} 0 & \to & A & \to & B & \to & C \to 0 \\ & & \downarrow & \circlearrowright & \downarrow & \circlearrowright & \downarrow \\ 0 & \to & D & \to & E & \to & F \to 0 \end{array} \qquad \begin{array}{ccccccc} 0 & \to & P^A_\bullet & \to & P^B_\bullet & \to & P^C_\bullet \to 0 \\ & & \downarrow & \circlearrowright & \downarrow & \circlearrowright & \downarrow \\ 0 & \to & P^D_\bullet & \to & P^E_\bullet & \to & P^F_\bullet \to 0 \end{array}$$

$$\begin{array}{ccccccc} L_iF(A) & \to & L_iF(B) & \to & L_iF(C) & \to & L_{i-1}F(A) \\ \downarrow & \circlearrowright & \downarrow & \circlearrowright & \downarrow & \circlearrowright & \downarrow \\ L_iF(D) & \to & L_iF(E) & \to & L_iF(F) & \to & L_{i-1}F(D) \end{array}$$

3) L_iF sono funtori additivi

Se voglio calcolare $L_iF(A \oplus B)$, posso prendere

$$\begin{array}{ccc} L_iF(A \oplus B) & & P^A_\bullet \to A \\ \| & \xleftarrow{F} & \oplus \quad \oplus \\ H_i(F(P^A_\bullet) \oplus F(P^B_\bullet)) & & P^B_\bullet \to B \end{array}$$

$$H_i(F(P^A_\bullet)) \oplus H_i(F(P^B_\bullet)) = L_iF(A) \oplus L_iF(B)$$

4) Se F è esatto a sx covariante:

$0 \to A \to I^\bullet_A \quad \rightsquigarrow \quad R^iF(A) := H^i(F(I^\bullet_A))$

$0 \to A \to B \to C \to 0 \quad \rightsquigarrow \quad 0 \to F(A) \to F(B) \to F(C) \to R^1F(A) \to R^1F(B) \to$

$\to R^1F(C) \to R^2F(A) \to \dots$

Se I è iniettivo, $R^iF(I) = 0 \ \forall i \geq 1$

Se F è controvariante esatto a sx posso calcolare R^iF usando $P^A_\bullet \to A \to 0 \quad \rightsquigarrow R^iF(A) := H^i(F(P^\bullet))$

Ext e Tor

(1) Dato B R-mod, considero $F: \text{Mod}_R \to \text{Mod}_R$, $A \mapsto A \otimes B$

è esatto a dx: ammette funtori derivati sx $L_iF(A)$ t.c.
$\forall$ succ. esatta corta $0 \to M_1 \to M_2 \to M_3 \to 0$ ottengo

$$\dots \to L_1F(M_2) \to L_1F(M_3) \to M_1 \otimes B \to M_2 \otimes B \to M_3 \otimes B \to 0$$

Si denota $L_iF(A) =: \text{Tor}_i^R(A,B)$

D'altro canto posso considerare $G: \text{Mod}_R \to \text{Mod}_R$, $B \mapsto A \otimes B$

anche questo ammette funtori derivati sx

$$(L_iG)(B) \underset{\text{da vedere}}{=} (L_iF)(A)$$

(2) Fissato $A \in \text{Mod}_R$, considero $F: \text{Mod}_R \to \text{Mod}_R$, $B \mapsto \text{Hom}_R(A,B)$

e $G: \text{Mod}_R \to \text{Mod}_R$, $A \mapsto \text{Hom}_R(A,B)$

Questi sono esatti a sx; i loro funtori derivati dx soddisfano

$$(R^iF)(B) = (R^iG)(A)$$

e si denotano $\text{Ext}^i_R(A,B)$

esempio (1) $R = \mathbb{Z}$. Calcoliamo $\text{Tor}_i(M, \mathbb{Z}/n\mathbb{Z})$

$$\dots \to 0 \to \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0 \quad \text{ris. proiettiva}$$

$$\downarrow M \otimes -$$

$$\dots \to 0 \to M \otimes \mathbb{Z} \xrightarrow[id \otimes \cdot n]{\cdot n} M \otimes \mathbb{Z} \to M \otimes \mathbb{Z}/n\mathbb{Z} \to 0$$

Elimino l'ultimo termine e prendo l'omologia:

$$0 \to M \xrightarrow{\cdot n} M \xrightarrow{d_0} 0$$

$$\text{Tor}_0(M, \mathbb{Z}/n\mathbb{Z}) = \frac{\ker d_0}{\text{Im} d_1} = \frac{M}{nM} = M \otimes \mathbb{Z}/n\mathbb{Z}$$

$$\text{Tor}_i(M, \mathbb{Z}/n\mathbb{Z}) = 0 \quad \text{per } i \geq 2$$

$$\text{Tor}_1(M, \mathbb{Z}/n\mathbb{Z}) = \frac{\ker d_1}{\text{Im} d_2} = \frac{M[n]}{0} = M[n] \quad n\text{-torsione}$$

Oss Sia R un PID. $\text{Tor}_i(A,B) = 0$ per $i \geq 2$

$$P^\bullet \to B \to 0 \longrightarrow 0 \to R^{\oplus J} \otimes A \to R^{\oplus I} \otimes A \to 0$$

$$R^{\oplus J} \to R^{\oplus I} \to B \to 0 \quad \text{(sottomod di un libero è libero)}$$

Dal grado 2 in poi, l'omologia è nulla.

(2) $R = K[x]/(x^2)$, $M = R/(x)$ come R-modulo

R non ammette una ris. proiettiva finita.

Intanto troviamo una ris. proiettiva:

$$\dots \longrightarrow R \xrightarrow{\cdot x} R \xrightarrow{\cdot x} R \xrightarrow{\pi} R/(x) \longrightarrow 0$$

$$1 \longmapsto x \quad x \longmapsto 0 \qquad 1 \longmapsto 1 \quad x \longmapsto 0$$

Calcoliamo $\mathrm{Tor}_i^R(M,M)$: è l'omologia del complesso

$$\dots \longrightarrow R\otimes M \xrightarrow{\cdot x \otimes \mathrm{id}} R\otimes M \longrightarrow R\otimes M \longrightarrow 0$$

$$\dots \longrightarrow M^2 \xrightarrow{\cdot x = 0} M^2 \xrightarrow{\cdot x = 0} M^2 \longrightarrow 0$$

$\mathrm{Tor}_i^R(M,M) = \frac{\ker 0}{\mathrm{Im}\, 0} = M \quad \forall i \geq 0$

In particolare, M non ha ris. proiettive finite, altrimenti Tor_i dovrebbe essere definitivamente nullo.

OSS Se F è un funtore esatto, applicandolo a una succ. esatta lunga trovo una succ. esatta lunga.

proposizione Le seguenti sono equivalenti (per colonne):

(i) P proiettivo	(i) I iniettivo	(i) F piatto
(ii) $\mathrm{Ext}^i(P,B)=0 \ \forall i\geq 1 \ \forall B$	(ii) $\mathrm{Ext}^i(A,I)=0 \ \forall i\geq 1 \ \forall A$	(ii) $\mathrm{Tor}_i(F,B)=0 \ \forall i\geq 1 \ \forall B$
(iii) $\mathrm{Ext}^1(P,B)=0 \ \forall i$	(iii) $\mathrm{Ext}^1(A,I)=0 \ \forall A$	(iii) $\mathrm{Tor}_1(F,B)=0 \ \forall B$
	(iv) $\mathrm{Ext}^1(R/J,I)=0 \ \forall J\lhd R$	(iv) $\mathrm{Tor}_1(F,R/J)=0 \ \forall J\lhd R$

DIMOSTRAZIONE (iniettivi)

(ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) ovvio

(i) $\Rightarrow$ (ii) "i funtori derivati di un esatto sono 0"

$\mathrm{Ext}^i(A,I) = (R^i \mathrm{Hom}(-,I))(A)$

$P_\bullet \longrightarrow A \longrightarrow 0 \longrightarrow \dots \to \mathrm{Hom}(P_1,I) \to \mathrm{Hom}(P_0,I) \to \mathrm{Hom}(A,I) \to 0$ esatta

$\mathrm{Ext}^i(A,I)$ = omologia di un complesso che è esatto in ogni grado ≥ 1 $= (0)$

(iv) $\Rightarrow$ (i) Applico il criterio di Baer:

I è iniettivo $\iff$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J & \longrightarrow & R & \longrightarrow & R/J & \longrightarrow & 0 \\ & & \forall\varphi \downarrow & \swarrow \exists\psi & & & & & \\ & & I & & & & & & \end{array}$$

$\mathrm{Hom}(-,I)$

$$0 \longrightarrow \mathrm{Hom}(R/J,I) \longrightarrow \mathrm{Hom}(R,I) \longrightarrow \mathrm{Hom}(J,I) \longrightarrow \mathrm{Ext}^1(R/J,I) = 0$$

$$\psi \xmapsto{\text{surgettiva}} \psi\circ i = \varphi|_J$$

□

complessi doppi

Def. Un complesso doppio (bigrado) è una collezione $A_{\cdot,\cdot}$ di moduli indicizzati da $\mathbb{N}\times\mathbb{N}$ con mappe

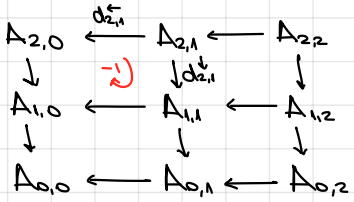
$d^{\leftarrow}_{i,j} : A_{i,j} \longrightarrow A_{i,j-1}$

$d^{\downarrow}_{i,j} : A_{i,j} \longrightarrow A_{i-1,j}$

tali che

$d^{\leftarrow}_{i,j-1} \circ d^{\leftarrow}_{i,j} = 0$, $d^{\downarrow}_{i-1,j} \circ d^{\downarrow}_{i,j} = 0$

e ogni quadrato anti-commuta: $d^{\downarrow}_{i,j-1} \circ d^{\leftarrow}_{i,j} = -\, d^{\leftarrow}_{i-1,j} \circ d^{\downarrow}_{i,j}$



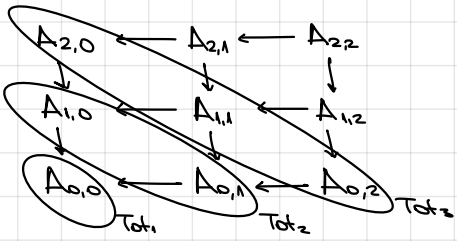
Un morfismo di complessi doppi $\varphi_{\cdot,\cdot} : A_{\cdot,\cdot} \longrightarrow B_{\cdot,\cdot}$ è una collezione di mappe che commutano con i differenziali.

Def. Il complesso totale di un complesso doppio $A_{\cdot,\cdot}$ è $\mathrm{Tot}(A_{\cdot,\cdot})$

$$\mathrm{Tot}(A_{\cdot,\cdot})_n = \bigoplus_{i+j=n} A_{i,j}$$

con $d_n : \bigoplus_{i+j=n} A_{i,j} \longrightarrow \bigoplus_{i+j=n-1} A_{i,j}$

$$A_{i,j} \xrightarrow{d^{\downarrow}_{i,j} \oplus d^{\leftarrow}_{i,j}} A_{i-1,j} \oplus A_{i,j-1}$$

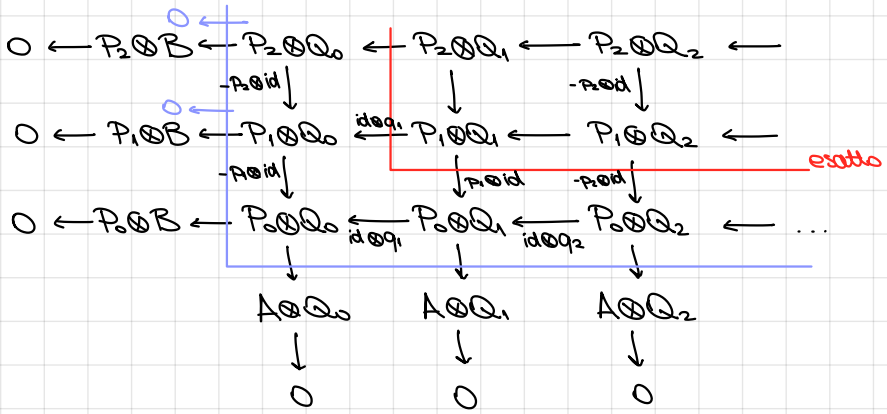


Oss $\mathrm{Tot} : \{\text{complessi doppi}\} \longrightarrow \mathrm{Ch}_R$ è un funtore esatto

Lemma Sia $\varphi_{\cdot,\cdot} : A_{\cdot,\cdot} \longrightarrow B_{\cdot,\cdot}$ morfismo di complessi doppi bigradati t.c. $\forall i$ $\varphi_{i,\cdot} : A_{i,\cdot} \longrightarrow B_{i,\cdot}$ è un quasi-isomorfismo.
Allora $\mathrm{Tot}(\varphi_{\cdot,\cdot}) : \mathrm{Tot}(A_{\cdot,\cdot}) \longrightarrow \mathrm{Tot}(B_{\cdot,\cdot})$ è un quasi-isomorfismo.

Da questo deduciamo la simmetria di Tor

Prendiamo $P_\cdot \longrightarrow A \longrightarrow 0$ e $Q_\cdot \longrightarrow B \longrightarrow 0$ ris. proiettive



Considero il complesso doppio $(P_i \otimes Q_j)_{(i,j)\in\mathbb{N}\times\mathbb{N}} = X_{\cdot,\cdot}$

e il complesso doppio $Y_{\cdot,\cdot} = \left(\begin{smallmatrix} 0 & 0 & 0 \\ \downarrow & \downarrow & \downarrow \\ A\otimes Q_0 & \leftarrow A\otimes Q_1 & \leftarrow A\otimes Q_2 \leftarrow \dots \end{smallmatrix} \right)$

C'è un morfismo $\varphi_{\cdot,\cdot}: X_{\cdot,\cdot} \longrightarrow Y_{\cdot,\cdot}$ che è 0 quasi ovunque, tranne $P_0 \otimes Q_i \xrightarrow{p_0 \otimes id} A \otimes Q_i$, dove p_0 è la mappa $\cdots \to P_1 \xrightarrow{p_1} P_0 \xrightarrow{p_0} A \to 0$

Questa mappa $\varphi_{\cdot,\cdot}$ soddisfa le ipotesi del lemma per le colonne.

$\Longrightarrow$ $Tot(\varphi_{\cdot,\cdot})$ è un isomorfismo fra l'omologia di $Tot(X_{\cdot,\cdot})$ e l'omologia di $Tot(Y_{\cdot,\cdot}) = (A \otimes Q_\cdot)$

$\Longrightarrow H_i(Tot(Y_{\cdot,\cdot})) = H_i(A \otimes Q_\cdot) = (L_i(A \otimes -))(B)$

Se ora pongo $Z_{\cdot,\cdot} = \begin{pmatrix} P_2 \otimes B \leftarrow 0 \leftarrow \cdots \\ \downarrow \\ P_1 \otimes B \leftarrow 0 \leftarrow \cdots \\ \downarrow \\ P_0 \otimes B \leftarrow 0 \leftarrow \cdots \end{pmatrix}$

con lo stesso ragionamento trovo

$$H_i(Tot(X_{\cdot,\cdot})) = H_i(Tot(Z_{\cdot,\cdot})) = H_i(P_\cdot \otimes B) = (L_i(- \otimes B))(A)$$

Lemma $0 \to A_\cdot \to B_\cdot \to C_\cdot \to 0$ (con $\alpha_\cdot \downarrow$, $\beta_\cdot \downarrow$, $\gamma_\cdot \downarrow$)

$0 \to E_\cdot \to F_\cdot \to G_\cdot \to 0$ esatte corte di complessi.

Se $\alpha_\cdot, \gamma_\cdot$ sono quasi-isomorfismi, allora $\beta_\cdot$ è quasi-isomorfismo.

DIMOSTRAZIONE

S.E.L. in omologia:

$$\begin{array}{ccccccccc} H_i(A_\cdot) & \to & H_i(B_\cdot) & \to & H_i(C_\cdot) & \to & H_{i-1}(A_\cdot) & \to & H_{i-1}(B_\cdot) \\ \downarrow H_i(\alpha_\cdot) & & \downarrow H_i(\beta_\cdot) & & \downarrow H_i(\gamma_\cdot) & & \downarrow H_{i-1}(\alpha_\cdot) & & \downarrow H_{i-1}(\beta_\cdot) \\ H_i(E_\cdot) & \to & H_i(F_\cdot) & \to & H_i(G_\cdot) & \to & H_{i-1}(E_\cdot) & \to & H_{i-1}(F_\cdot) \end{array}$$

Applico il lemma dei 5. □

DIMOSTRAZIONE

Per induzione

$$H_n(Tot(A_{\cdot,\cdot})) \xrightarrow[\sim]{H_n(\varphi_{\cdot,\cdot})} H_n(Tot(B_{\cdot,\cdot}))$$

Questa affermazione dipende da una quantità finita di informazioni (cioè solo da $A_{i,j}$ e $B_{i,j}$ con $0 \le i,j \le N$)

$$\begin{array}{ccc} \begin{matrix} 0 & 0 \\ \downarrow & \downarrow \end{matrix} & & \begin{matrix} 0 & 0 \\ \downarrow & \downarrow \end{matrix} \\ r \left\{ \begin{matrix} A_{i,j} \end{matrix} \right. & \xrightarrow{\varphi_{\cdot,\cdot}} & r \left\{ \begin{matrix} B_{i,j} \end{matrix} \right. \end{array}$$

- Se $r=1$: $Tot(A_{\cdot,\cdot}) = A_{0,\cdot}$, $Tot(B_{\cdot,\cdot}) = B_{0,\cdot}$, $Tot(\varphi_{\cdot,\cdot}) = \varphi_{0,\cdot}$ quasi-isomorfismo
- $r \to r+1$:

$$\begin{array}{ccccccccc} 0 & \to & A^{\le r} & \to & A & \to & A_{r+1,\cdot} & \to & 0 \\ & & \downarrow \varphi^{\le r}_{\cdot,\cdot} & & \downarrow \varphi_{\cdot,\cdot} & & \downarrow \varphi_{r+1,\cdot} & & \\ 0 & \to & B^{\le r} & \to & B & \to & B_{r+1,\cdot} & \to & 0 \end{array}$$

per ind., $Tot(\varphi^{\le r}_{\cdot,\cdot})$ è quasi-isom. $\quad$ $Tot(\varphi_{r+1,\cdot}) = \varphi_{r+1,\cdot}$ è quasi-isom.

$\Longrightarrow Tot(\varphi_{\cdot,\cdot})$ è quasi-isomorfismo □

ES Se $\mathrm{Tor}_1(R/I, M) = (0) \ \ \forall I \lhd R$, allora M è piatto.

SOL Per assurdo, sia
$0 \to A \to B$ t.c. $A \otimes M \to B \otimes M$ non iniettiva
Se $a_1 \otimes m_1 + \dots + a_r \otimes m_r \in \ker$, posso sostituire A con $\langle a_1, \dots, a_r \rangle =: A'$
$0 \to A' \to A$: se $A' \otimes M \to A \otimes M$ non iniettiva ok,
altrimenti $0 \to A' \to B$ è un esempio
$\Rightarrow$ wlog A fin.gen.
Similmente posso supporre B fin.gen.
$B = A + \langle b_1, \dots, b_r \rangle$
$0 \to A \to A + \langle b_1 \rangle \to A + \langle b_1, b_2 \rangle \to \dots \to A + \langle b_1, \dots, b_r \rangle$
Quindi wlog basta il caso $0 \to A \to A + \langle t \rangle \to \frac{A + \langle t \rangle}{A} \to 0$

$$\frac{A + \langle t \rangle}{A} \cong \frac{\langle t \rangle}{A \cap \langle t \rangle}$$

$$0 \to I \to R \xrightarrow{1 \mapsto \bar{t}} \frac{\langle t \rangle}{A \cap \langle t \rangle} \cong R/I$$

Ho $0 \to A \to A + \langle t \rangle \to R/I \to 0$
$\otimes M$
$\mathrm{Tor}_1(R/I, M) \to A \otimes M \to (A + \langle t \rangle) \otimes M \to R/I \otimes M \to 0$
$\mathrm{Tor}_1(R/I, M) = 0$

corollario Se R è PID, $\mathrm{Tor}_1(R/(r), M) = (0) \iff M[r] = 0 \ \ \forall r \in R$.

DIMOSTRAZIONE
$0 \to R \xrightarrow{\cdot r} R \to R/(r) \to 0$
$0 \to M \xrightarrow{\cdot r} M \to 0$ $\otimes M$
$\Rightarrow \mathrm{Tor}_1(R/(r), M) = M[r]$ □

Oss
- $\mathbb{Q}$ è $\mathbb{Z}$-piatto
- $0 \to A \to B \to \mathbb{Q} \to 0$, $M \in |Ab|$ qualsiasi
$\Rightarrow 0 \to \underbrace{\mathrm{Tor}_1(\mathbb{Q}, M)}_{=0} \to A \otimes M \to B \otimes M \to \mathbb{Q} \otimes M \to 0$ esatta
- $\mathbb{Q}$ proiettivo? No, altrimenti
$\mathbb{Q} \oplus T \cong \mathbb{Z}^{\oplus I} \Rightarrow \mathbb{Q}$ libero $\cong \mathbb{Z}^{\oplus J}$ assurdo

ES (R, P) locale noetheriano, $k = R/P$, M mod fin.gen. piatto (o $\mathrm{Tor}_1(k, M) = 0$).
Allora M è libero.

SOL $M \otimes k = \langle \overline{m}_1, \dots, \overline{m}_n \rangle$
$0 \to Q \to R^n \xrightarrow{e_i \mapsto m_i} M \to 0$
$\otimes k$
$0 \to Q \otimes k \to R^n \otimes k \xrightarrow{\sim} M \otimes k \to 0$
$R^n \otimes k \cong k^n$
$\Rightarrow Q \otimes k = 0 \overset{\text{Nak}}{\Rightarrow} Q = 0$
$\Rightarrow M \cong R^n$

Teorema di struttura per moduli finitamente generati su R Dedekind

M R-mod fin.gen.
$M = M_{tors} \oplus M/M_{tors}$ dove $M_{tors} = \{m \in M \mid \exists r \in R\setminus\{0\} \text{ t.c. } rm = 0\}$

$$0 \longrightarrow M_{tors} \longrightarrow M \longrightarrow \underbrace{M/M_{tors}}_{\text{proiettivo?}} \longrightarrow 0$$

Sia M fin.gen. e libero da torsione. Allora M è proiettivo.
1) Proiettivo $\iff$ Succ. libero
2) P primo di R; lavoro con $M \otimes R_P$, libero da torsione
3) Se $\dim P = 1$, R_P è un DVR
$\Longrightarrow M \otimes R_P$ è piatto $\Longrightarrow$ libero

$$0 \longrightarrow R \longrightarrow Frac(R) \xrightarrow{\otimes M} 0 \longrightarrow M \longrightarrow \underbrace{M \otimes_R Frac(R)}_{k^n} \overset{\simeq}{=} k$$

Fissiamo una base $m_1, \dots, m_n$ di $M \otimes k$
$I = \{x \in K \mid x \cdot m_1 \in M\}$ è un ideale frazionario di R
$$0 \longrightarrow \underset{x \mapsto xm_1}{I} \longrightarrow M \longrightarrow M' \longrightarrow 0 \quad \Longrightarrow I \text{ fin.gen.}$$

M' è fin.gen. e libero da torsione: se $x \cdot \overline{m} = 0$, dove $\overline{m} \in M/Im_1$, $x \neq 0$
$\iff xm \in m_1 I \cdot xm = im_1 \iff m = \frac{i}{x} m_1$
$\Longrightarrow \frac{i}{x} \in I \Longrightarrow m \in Im_1 \Longrightarrow \overline{m} = 0$

$\Longrightarrow M \simeq I \oplus M'$
Per induzione, $M \simeq I_1 \oplus \dots \oplus I_n$
$\simeq R^{n-1} \oplus I$ dove $I = I_1 \cdots I_n$

Sia ora M un modulo di torsione fin.gen.
$M = \langle m_1, \dots, m_n \rangle$ $\quad Ann(m_i) \ni x_i \neq 0 \Longrightarrow a := \prod m_i$ annulla $x_i \ \forall i \Longrightarrow aM = (0)$
M è $R/(a)$ − modulo
$(a) = \prod P_i^{e_i}$ con P_i primi
$A/(a) \simeq \prod A/P_i^{e_i}$
$M = M \otimes_A A/(a) = M \otimes \left(\oplus A/P_i^{e_i}\right) = \oplus \left(M/P_i^{e_i} M\right)$
Fisso i: $A/P^e \simeq A_P/(PA_P)^e \Longrightarrow M/P^e M$ è un A_P - modulo
2) $\quad \hookrightarrow$ DVR $\Rightarrow$ PID
$\oplus A_P/(PA_P)^{e_i} \simeq \oplus A/P^e$

oppure $\quad 0 \longrightarrow \underset{x \mapsto xm}{A/P^e} \longrightarrow M$ è iniettiva
e si mostra che A/P^e è iniettivo su se stesso.

coomologia di gruppo

def. G gruppo finito
Un G-modulo è un gruppo abeliano A munito di un omomorfismo $G \longrightarrow Aut A$

esempio L/k est. con gruppo G
Sia $(L,+)$ sia $(L^\times,\cdot)$ sono G-moduli.

def. L'anello di gruppo è
$\mathbb{Z}[G] = \{ \sum_{g \in G} a_g \cdot g \mid a_g \in \mathbb{Z} \}$

esempio Se $G = \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}[G] = \frac{\mathbb{Z}[t]}{(t^3-1)}$
$a_0[0] + a_1\underbrace{[1]}_{t} + a_2\underbrace{[2]}_{t^2}$

$\mathbb{Z}[\mathbb{Z}] = \mathbb{Z}[t, \frac{1}{t}]$

G-modulo $=$ $\mathbb{Z}[G]$-modulo
A M grp abeliano
$\varphi : G \longrightarrow Aut A$ $\psi : \mathbb{Z}[G] \longrightarrow End_{\mathbb{Z}} M$
$G \subseteq \mathbb{Z}[G]^\times$

$(\Sigma a_g g)(\Sigma b_h h) = \sum_{s \in G} (\sum_{gh=s} a_g b_h)\, s$ (convoluzione)

def. $A \longmapsto A^G = \{ a \in A \mid ga = a \ \forall g \in G \} \subset A$
$\mathbb{Z}[G]\text{-mod} \longrightarrow Ab = \mathbb{Z}\text{-mod}$

Oss Sia $\mathbb{Z}$ il G-mod banale
$Hom_{\mathbb{Z}[G]}(\mathbb{Z}, A) = \{ \varphi_a : \mathbb{Z} \longrightarrow A : \varphi_a(1) = a, a \in A^G \} = A^G$
$\varphi : \mathbb{Z} \longrightarrow A$, $1 \longmapsto a$
$\varphi(n) = g\varphi(n)$ $\forall n$
$n\varphi(1) \quad ng\varphi(1) \iff \varphi(1) = g\varphi(1)$ $\forall g$

def. $H^i(G,A) = Ext^i_{\mathbb{Z}[G]}(\mathbb{Z}, A)$

$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$
$g \cdot \alpha(a) = \alpha(ga)$, $g\beta(b) = \beta(gb)$
$\rightsquigarrow \quad 0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \longrightarrow H^1(G,A) \longrightarrow H^1(G,B) \longrightarrow \dots$

Risoluzione proiettiva di $\mathbb{Z}$ come $\mathbb{Z}[G]$-modulo

$$\dots \longrightarrow \mathbb{Z}[G^3] \xrightarrow{\delta_1} \mathbb{Z}[G^2] \longrightarrow \mathbb{Z}[G] \xrightarrow{\delta_0} \mathbb{Z} \longrightarrow 0$$
$$g \longmapsto 1$$

$(\sigma_0, \dots, \sigma_i) \in G^{i+1}$

$$\delta_i(\sigma_0, \dots, \sigma_i) = \sum_{j=0}^{i} (-1)^j (\sigma_0, \dots, \hat{\sigma}_j, \dots, \sigma_i)$$

- δ_i sono omomorfismi di G-moduli
- $\mathbb{Z}[G^i]$ è uno $\mathbb{Z}[G]$-mod libero
- $\delta_i \circ \delta_{i+1} = 0$
- esattezza

- $\mathbb{Z}[G^i]$ è G-mod con $g \cdot (g_0, \dots, g_{i-1}) = (gg_0, \dots, gg_{i-1})$
  $\mathbb{Z}[G^i]$ è libero su $\mathbb{Z}[G]$: una base è
  $$(id, \sigma_1, \dots, \sigma_{i-1})$$
  $$\oplus\, \mathbb{Z}[G] \cdot (id, \sigma_1, \dots, \sigma_{i-1}) = \mathbb{Z}[G^i]$$

- $\varphi((\Sigma a_g g)x) \stackrel{?}{=} \Sigma a_g g \varphi(x)$
  δ_i è omomorfismo di G-moduli.
  $$g \cdot \delta_i(\sigma_0, \dots, \sigma_i) = \sum_{j=0}^{i} (-1)^j (g\sigma_0, \dots, \widehat{g\sigma_j}, \dots, g\sigma_i) = \delta_i(g\sigma_0, \dots, g\sigma_i) = \delta_i(g \cdot (\sigma_0, \dots, \sigma_i))$$
- $\delta_i \circ \delta_{i+1} = 0$
  $$\delta_i(\delta_{i+1}(\sigma_0, \dots, \sigma_{i+1})) = \delta_i\Big(\sum_{j=0}^{i+1} (-1)^j (\sigma_0, \dots, \hat{\sigma}_j, \dots, \sigma_{i+1})\Big) = \sum_{j=0}^{i+1} (-1)^j \Big(\sum_{k=0}^{j-1} (-1)^k (\sigma_0, \dots, \hat{\sigma}_k, \dots, \hat{\sigma}_j, \dots, \sigma_{i+1}) +$$
  $$+ \sum_{k=j+1}^{i} (-1)^{k+1} (\sigma_0, \dots, \hat{\sigma}_j, \dots, \hat{\sigma}_k, \dots, \sigma_{i+1})\Big) = 0$$

- $$\dots \longrightarrow \mathbb{Z}[G^3] \longrightarrow \mathbb{Z}[G^2] \longrightarrow \mathbb{Z}[G] \xrightarrow{\delta_0} \mathbb{Z} \longrightarrow 0$$
  $$\dots \longrightarrow \mathbb{Z}[G^3] \longrightarrow \mathbb{Z}[G^2] \longrightarrow \mathbb{Z}[G] \xrightarrow{\delta_0} \mathbb{Z} \longrightarrow 0$$
  (con k_1, k_0, k_{-1})
  t.c. $k_{i-1} \circ \delta_i + \delta_{i+1} \circ k_i = id - 0$

1° costruzione: $k_i((\sigma_0, \dots, \sigma_i)) = (g, \sigma_0, \dots, \sigma_i)$ (non è una mappa di G-moduli)
$$k_{i-1}(\delta_i(\sigma_0, \dots, \sigma_i)) = k_{i-1}\Big(\sum_{j=0}^{i} (-1)^j (\sigma_0, \dots, \hat{\sigma}_j, \dots, \sigma_i)\Big) = \sum_{j=0}^{i} (-1)^j (g, \sigma_0, \dots, \hat{\sigma}_j, \dots, \sigma_i)$$
$$\delta_{i+1}(k_i(\sigma_0, \dots, \sigma_i)) = (\sigma_0, \dots, \sigma_i) + \sum_{j=1}^{i+1} (-1)^j (g, \sigma_0, \dots, \hat{\sigma}_{j-1}, \dots, \sigma_i) =$$
$$= (\sigma_0, \dots, \sigma_i) + \sum_{j=0}^{i} (-1)^{j+1} (g, \sigma_0, \dots, \hat{\sigma}_j, \dots, \sigma_i)$$
$$\Longrightarrow id \underset{omot.}{\sim} 0 \Longrightarrow H^i(\mathbb{Z}[G^\bullet]) = (0)$$

2° costruzione: $k_i((\sigma_0, \dots, \sigma_i)) = \sum_{g \in G} (g, \sigma_0, \dots, \sigma_i)$
è omotopia tra 0 e $|G| \cdot id$
Ora è una mappa di G-moduli:
$$k_i(h \cdot (\sigma_0, \dots, \sigma_i)) = \sum_{g \in G} (g, h\sigma_0, \dots, h\sigma_i) = \sum_{g \in G} (hg, h\sigma_0, \dots, h\sigma_i) = h \cdot k_i((\sigma_0, \dots, \sigma_i))$$

Per calcolare $Ext^i_{\mathbb{Z}[G]}(\mathbb{Z}, M)$, possiamo prendere l'omologia di
$$0 \longrightarrow Hom(\mathbb{Z}[G], M) \xrightarrow{\delta_1^*} Hom(\mathbb{Z}[G^2], M) \xrightarrow{\delta_2^*} \dots$$
$$0 \longrightarrow Hom(\mathbb{Z}[G], M) \xrightarrow{\delta_1^*} Hom(\mathbb{Z}[G^2], M) \xrightarrow{\delta_2^*} \dots$$
$(Hom(-, M))(k_i)$

omotopia tra 0 e $|G| \cdot id$

Se $Ext^i_{\mathbb{Z}[G]}(\mathbb{Z}, M)$, le mappe 0 e $|G| \cdot id$ coincidono (per $i \geq 1$)

teorema $\forall i \geq 1$ $H^i(G,M)$ è un gruppo abeliano di $|G|$-torsione.

corollario Se $(|G|,|M|)=1$, allora $H^i(G,M)=(0)$ $\forall i \geq 1$.

DIMOSTRAZIONE

Considero la moltiplicazione per $|G|$ da $H^i(G,M)$ in sè
È zero per il Teo. D'altra parte, $\cdot|G| : M \longrightarrow M$ è isomorfismo:
$\ker(\cdot|G|) \subseteq \{\text{el. di ord } |\#G|\} \cap \{\text{el. di ord } |\#M|\} = \{e\}$
$a\#G + b\#M = 1 \implies [a]\,[\#G] = id_M$
$[a] \cdot M \longrightarrow M$ induce $H^i(G,[a]) : H^i(G,M) \longrightarrow H^i(G,M)$

$$\begin{array}{ccccccc} \ldots \leftarrow & I^1_M & \leftarrow & I^0_M & \leftarrow & M & \leftarrow 0 \\ & \downarrow [a] & & \downarrow [a] & & \downarrow [a] & \\ \ldots \leftarrow & I^1_M & \leftarrow & I^0_M & \leftarrow & M & \leftarrow 0 \end{array}$$

$\implies$ la mappa indotta da $[a]$ su $H^i(G,M)$ è $[a]$.
$[a]\,[\#G] = id \overset{\text{su } H^i(G,M)}{\Longrightarrow} [a] \circ [\#G] = id$
$\implies [\#G]$ è biiettiva su $H^i(G,M)$ $\implies H^i(G,M)=(0)$. □

Calcolo di H^1 e H^2

$$\begin{array}{ccccccccc} 0 \longrightarrow & \mathrm{Hom}(\mathbb{Z}[G],M) & \xrightarrow{\delta_1^*} & \mathrm{Hom}(\mathbb{Z}[G^2],M) & \xrightarrow{\delta_2^*} & \mathrm{Hom}(\mathbb{Z}[G^3],M) & \longrightarrow \ldots \\ & \wr\downarrow & & \wr\downarrow & & \wr\downarrow & \\ & M & \xrightarrow{\delta_1^*} & M^G & \xrightarrow{\delta_2^*} & M^{G^2} & \\ & f(1) & & G \to M & & & \\ & & & g \mapsto f(1,g) = c_g & & & \end{array}$$

(sopra: $(1,\sigma)_*$ e $(1,\sigma_1,\sigma_2)$)

Oss La base "standard" che si prende è $(1, \sigma_1, \sigma_1\sigma_2, \sigma_1\sigma_2\sigma_3, \ldots)$

$\delta_1^*(m)$ $(f_m \circ \delta_1)(1,g) = f_m(g) - f_m(1) = g\cdot m - m$ dove $f_m(1)=m$
$\delta_1^*(f_m) = f_m \circ \delta_1$
$\delta_2^*(g)=0 \longleftrightarrow f\circ\delta_2(1,\sigma_1,\sigma_1\sigma_2)=0 \ \forall \sigma_1,\sigma_2 \in G \longleftrightarrow f(\sigma_1,\sigma_1\sigma_2) - f(1,\sigma_1\sigma_2) + f(1,\sigma_1) = 0$
$\longleftrightarrow \sigma_1 f(1,\sigma_2) - f(1,\sigma_1\sigma_2) + f(1,\sigma_1) = 0 \longleftrightarrow c_{\sigma_1} + \sigma_1 \cdot c_{\sigma_2} = c_{\sigma_1\sigma_2}$

Conclusione:
$$H^1(G,M) = \frac{\{c \in M^G \mid c(\sigma_1,\sigma_2) = c(\sigma_1) + \sigma_1 c_{\sigma_2}\}}{\{g \mapsto gm - m \mid m \in M\}}$$

Oss Se M è un G-mod banale, $H^1(G,M) = \mathrm{Hom}(G,M)$

$c : \mathbb{Z}[G^3] \longrightarrow M \longleftrightarrow G^2 \longrightarrow M$, $f_c : (\sigma_1,\sigma_2) \mapsto c(1,\sigma_1,\sigma_1\sigma_2)$

$\sigma_1 \cdot f_c(\sigma_2,\sigma_3) - f_c(\sigma_1\sigma_2,\sigma_3) + f_c(\sigma_1,\sigma_2\sigma_3) - f_c(\sigma_1,\sigma_2) = 0$ (2-cociclo)
$\sigma_1 \cdot f_c(\sigma_2) - f_c(\sigma_1\sigma_2) + f_c(\sigma_1)$ (2-coborde)

Def. Un 2-cociclo si dice normalizzato se
$c(id,\tau) = c(\sigma,id) = 0 \quad \forall \sigma,\tau \in G$

Ex (1) Se c è un 2-cociclo e $c(id,id)=0$, allora è normalizzato.
(2) Ogni 2-cociclo sta nella stessa classe di omologia di un 2-cociclo normalizzato

Estensioni di gruppi

Def. G gruppo, A gruppo abeliano
Un'estensione di G tramite A è una successione esatta

$$1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$$

Due estensioni
$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & \| & & \| & & \| \\ 1 & \longrightarrow & A & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 1 \end{array}$$
sono isomorfe se $\exists \varphi : E \longrightarrow E'$ omomorfismo di gruppi che fa commutare.

Oss φ è automaticamente isomorfismo.

Obiettivo (i) Ogni estensione definisce un'azione di G su A
(ii) $\mathrm{Ext}(G, A_*) = \{\text{estensioni di } G \text{ tramite } A \text{ con una data azione di } G \text{ su } A\}$
$\updownarrow 1{:}1$
$H^2(G, A_*)$

Oss $1 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$, $h : E \to A$, $s : G \to E$

Se ho h: $\ker h \lhd E$, $\ker \pi \lhd E \implies E \cong A \times G$
Se ho s: $i(A) \lhd E$, $s(G) < E$, $i(A) \cap s(G) = \{e\}$, $i(A) \cdot s(G) = E$
$\implies E \cong A \rtimes G$
In questo caso, E si dice split.

$$1 \longrightarrow A \longrightarrow E \underset{s}{\overset{\pi}{\rightleftarrows}} G \longrightarrow 1$$
s sezione insiemistica $s : G \to E$ t.c. $\pi \circ s = \mathrm{id}_G$

Def. $g * a := s(g) \cdot a \cdot s(g)^{-1} \in A$
È ben posta: se scelgo un'altra sezione $s' : G \to E$, $g \mapsto s(g) c(g)$, $c : G \to A$

$$s(g) a s'(g)^{-1} = s(g) c(g) a c^{-1}(g) s^{-1}(g) \underset{A \text{ ab.}}{=} s(g) a s(g)^{-1}$$

Teorema C'è una bigezione tra $H^2(G, A)$ (dove A ha una fissata struttura di G-modulo) e l'insieme delle estensioni di G tramite A (a meno di isomorfismo) con la proprietà che l'azione indotta di G su A è quella fissata.
Sotto questa bigezione, le estensioni split corrispondono a $0 \in H^2(G, A)$.

$$1 \longrightarrow A \longrightarrow E \underset{s}{\overset{\pi}{\rightleftarrows}} G \longrightarrow 1 \quad \rightsquigarrow \quad c : G \times G \longrightarrow A, \quad (g, h) \longmapsto s(g) s(h) s(gh)^{-1}$$

Verifiche: 0) c è un 2-cociclo
1) $[c] \in H^2(G, A)$ non dipende dalla scelta di s
2) $\mathrm{Ext}(G, A_*) \longrightarrow H^2(G, A)$ è iniettiva + surj.
3) se l'est. è split, $[c] = 0$

Costruzione:

G, A, azione di G su A. Fisso $c: G\times G \longrightarrow A$ normalizzato

$E := A\times G$ (Se E esiste, i suoi elementi sono della forma $a\cdot s(g)$

con legge di gruppo:

$$a_1 s(g_1)\cdot a_2 s(g_2) = a_1 s(g_1) a_2 s(g_1)^{-1} s(g_1) s(g_2) = a_1 (g_1 * a_2) s(g_1) s(g_2) s(g_1 g_2)^{-1} s(g_1 g_2)$$
$$= a_1 (g_1 * a_2)\cdot c(g_1, g_2)\, s(g_1 g_2))$$

$$(a_1, g_1)\cdot(a_2, g_2) = (a_1 + g_1 * a_2 + c(g_1, g_2),\ g_1 g_2)$$

Oss $1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$

$A \xrightarrow{\sim} A\times G$, $a \longmapsto (a, id_G)$

$s: G \longrightarrow E$, $g \longmapsto (id, g)$

$(a, g) \longmapsto g$

$$(id, g_1) * (id, g_2) * (id, g_1 g_2)^{-1} = (c(g_1, g_2),\ g_1 g_2)(id, g_1 g_2)^{-1} = (c(g_1 g_2),\ id)$$

corollario $1 \longrightarrow A \longrightarrow E \xrightarrow{\pi} G \longrightarrow 1$ successione esatta di gruppi con A abeliano e $(|A|, |G|) = 1$.
Allora la successione spezza: $\exists s: G \longrightarrow E$ omomorfismo di gruppi, sezione di π, t.c. $E \cong A \rtimes s(G)$.

DIMOSTRAZIONE

E induce un'azione di G su A

le est. con quella azione sono parametrizzate da $H^2(G, A_*) = (0) \Longrightarrow E$ è split. □

Lemma di Frattini G gruppo finito, $N \trianglelefteq G$, P p-Sylow di N.
(i) $G = N\cdot N_G(P)$
(ii) Se $P \trianglelefteq N$, anche $P \trianglelefteq G$ (cioè $N_G(P) = G$).

DIMOSTRAZIONE

(i) Sia $g\in G$. Considero $gPg^{-1} \subseteq gNg^{-1} = N$
$\Longrightarrow gPg^{-1}$ è p-Sylow di N
Per Sylow, $\exists n\in N$ t.c. $gPg^{-1} = nPn^{-1} \Longrightarrow n^{-1}gPg^{-1}n = P$
$\Longrightarrow n^{-1}g \in N_G(P) \Longrightarrow g = \underset{\in N}{n}\cdot \underset{\in N_G(P)}{x}$

(ii) gPg^{-1} = un p-Sylow di N, ma l'unico p-Sylow di N è P
$\Longrightarrow gPg^{-1} = P \Longrightarrow P \trianglelefteq G$. □

ES Sia S una R-alg piatta. Allora

(ii) $Tor_i^R(M,N) \otimes_R S \simeq Tor_i^S(M\otimes_R S, N\otimes_R S)$ $\forall M,N \in |Mod_R|, \forall i \geq 0$

(i) Se P è R-mod proiettivo, allora $P\otimes_R S$ è S-mod proiettivo

SOL (i) $\exists Q$ t.c. $P\oplus Q \simeq R^{\oplus I}$ $\Longrightarrow$ $(P\otimes_R S)\oplus(Q\otimes_R S) \simeq S^{\oplus I}$

(ii) $i=0$: $M\otimes_R N \otimes_R S \simeq (M\otimes_R S)\otimes_S (S\otimes_R N)$

$i=1$ $\quad 0 \to Q \to P \to N \to 0$ esatta

$\otimes S$

$0 \to Q\otimes S \to P\otimes S \to N\otimes S \to 0$

$\otimes_S (M\otimes_R S)$

$(M\otimes S)\otimes(Q\otimes S) \to (M\otimes S)\otimes(P\otimes S) \to (M\otimes S)\otimes(N\otimes S) \to 0$

$\uparrow$

$Tor_1^S(M\otimes S, N\otimes S) \leftarrow Tor_1^S(M\otimes S, P\otimes S) = 0$

$\Longrightarrow Tor_1^S(M\otimes S, N\otimes S) \cong Ker((M\otimes S)\otimes(Q\otimes S) \to (M\otimes S)\otimes(P\otimes S))$

Ripartendo:

$0 \to Tor_1^R(M,N) \to M\otimes Q \to M\otimes P \to M\otimes N \to 0$

$\otimes S$

$0 \to Tor_1^R(M,N)\otimes S \to M\otimes Q\otimes S \to M\otimes P\otimes S$

$\Longrightarrow Tor_1^R(M,N)\otimes S \cong Ker(M\otimes Q\otimes S \to M\otimes P\otimes S)$ $\cong$

$i\geq 1$: la successione esatta lunga continua

$0 \leftarrow Tor_1(M\otimes S, Q\otimes S) \leftarrow Tor_2(M\otimes S, N\otimes S) \leftarrow Tor_2(M\otimes S, P\otimes S) = (0)$

ossia $0 \to Tor_{i+1}^S(M\otimes S, N\otimes S) \xrightarrow{\sim} Tor_i^S(M\otimes S, Q\otimes S) \to 0$

$\wr\!\wr$ ip. induttiva

$Tor_{i+1}^R(M,N)\otimes_R S \xrightarrow{\sim} Tor_i^R(M,Q)\otimes_R S$

$\uparrow$

segue dalla s.e.l. per $0 \to Q \to P \to N \to 0$

ES $R = \mathbb{C}[t^2, t^3]$

$a\in\mathbb{C}$, $M_a = \{f(t)\in\mathbb{C}[t] \mid f'(0) = a f(0)\}$

M_a è un modulo su R: $rf \overset{?}{\in} M_a$ $\quad rf(0) = r(0)f(0)$

$(rf)'(0) = r'(0)f(0) + r(0)f'(0) = r(0)af(0)$

M_a è fin. gen: $M_a = \langle 1+at, t^2\rangle_R$

Mostriamo che $t^m \in \langle 1+at, t^2\rangle_R$ $\forall m\geq 2$

$t^m = t^m(1+at) - at^{m+1}(1+at) + a^2t^m\cdot t^2$

Oss · M_0 è libero: $M_0 = \langle 1\rangle_R = R$

· M_a è libero solo se $a=0$: $M_a = \langle g(t)\rangle \Longrightarrow \deg g \leq 1$

Supponiamo $a\neq 0$ Se $g(0)=0$, $g'(0)=0 \Longrightarrow g\equiv 0$. ↯

Se $g(0)\neq 0 \Longrightarrow g(t) = 1+at$ ma t^2 non è multiplo di $1+at$ ↯

Mostriamo che M_a è localmente libero:

basta vedere che $1+at$ e t^2 differiscono per molt. per un elemento di R_P $\forall P$.

Se $t^2 \notin P$, $1+at = \frac{t^2(1+at)}{t^4}\cdot t^2$

Similmente, se $t^2(1+at)\notin P$, allora $t^2 = \frac{t^4}{t^2(1+at)}(1+at)$

Se $t^2, t^2(1+at)\in P \overset{a\neq 0}{\Longrightarrow} P = (t^2, t^3)$ è massimale

$t^2 = \frac{(1-at+a^2t^2)t^2}{1+a^3t^3}(1+at)$

Oss $M_a \otimes M_b \simeq M_{a+b}$

$M_a \times M_b \longrightarrow M_{a+b}$

$(f_a, f_b) \longmapsto f_a f_b$ $\qquad (f_a f_b)'(0) = f_a'(0) f_b(0) + f_a(0) f_b'(0) = (a+b) f_a(0) f_b(0)$

È isomorfismo:

- surgettività: $t^2\, t^2 = t^4 \in \mathrm{Im}$

  $t^m \in \mathrm{Im}\ \forall m \geq 4$

  $t^3 = (1+at)t^3 - at^4$

  $t^2 = (1+at)t^2 - at^3$

  $1 + (a+b)t = (1+at)(1+bt) - abt^2$
- iniettività: localizziamo

Oss $M_a \otimes M_{-a} \simeq M_0 = R$

Oss $M_a \simeq M_b \implies M_a \otimes_R M_{-a} \simeq M_b \otimes_R M_{-a} \implies b - a = 0$

Quindi $\mathbb{C} \hookrightarrow \mathrm{Pic}(R)$, $a \mapsto M_a$

Teorema 90 di Hilbert Sia L/K est. di Galois con gruppo G. Allora $H^1(G, L^\times) = (0)$.

Es $K^{\times n} = \{a^n \mid a \in K^\times\}$

$\mathbb{Q}(\zeta_{24})^{\times 3} \cap \mathbb{Q}^\times = \mathbb{Q}^{\times 3}$

$1 \longrightarrow \langle \zeta_3 \rangle \xrightarrow{i} \mathbb{Q}(\zeta_{24})^\times \xrightarrow{a \mapsto a^3} \mathbb{Q}(\zeta_{24})^{\times 3} \longrightarrow 1$ esatta di G-moduli

$G := \mathrm{Gal}(\mathbb{Q}(\zeta_{24})/\mathbb{Q})$

Prendiamo $H^0(G, -)$

$1 \longrightarrow \{1\} \longrightarrow \mathbb{Q}^\times \longrightarrow \mathbb{Q}(\zeta_{24})^{\times 3} \cap \mathbb{Q}^\times \longrightarrow H^1(G, \langle \zeta_3 \rangle) = 1$

$|G| = \phi(24) = \phi(3)\phi(8) = 2 \cdot 4$

Es $\mathbb{Q}(i)/\mathbb{Q}$ $\qquad a + bi \in \mathbb{Q}(i)^\times$ con $a^2 + b^2 = 1$

$G = \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \langle g \rangle$

$c: G \longrightarrow \mathbb{Q}(i)^\times$, $1 \longmapsto 1$, $g \longmapsto a+bi$ $\qquad c(\sigma\tau) = c(\sigma)^{\sigma} c(\tau)$

- $\sigma = \mathrm{id}$: $c(\tau) = c(\tau)$ ✓
- $\tau = \mathrm{id}$: $c(\sigma) = c(\sigma)\, 1$ ✓
- $\sigma = \tau = g$: $c(1) = (a+bi)^{\sigma}(a+bi) = a^2 + b^2$, $c(1) = 1$

$[c] \in H^1(G, \mathbb{Q}(i)^\times) = \{1\}$

$\implies c$ è un coboundo: $\exists x+iy \in \mathbb{Q}(i)$ t.c. $c(g) = \frac{g(x+iy)}{x+iy}$

$\implies a + bi = \frac{x - iy}{x+iy} = \frac{x^2 - y^2 + 2ixy}{x^2+y^2}$

$A^2 + B^2 = C^2 \qquad \left(\frac{A}{C}\right)^2 + \left(\frac{B}{C}\right)^2 = 1$

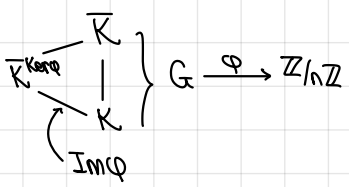
$a \qquad\quad b$

Teoria di Kummer

K campo di caratteristica p, n un intero non divisibile per p.
Supponiamo $\exists \zeta_n \in K$.
Classifichiamo le estensioni L/K di Galois con $Gal(L/K)$ ciclico di ord (n).
$[\exists a \in K^\times$ t.c. $L = K(\sqrt[n]{a})]$

$1 \longrightarrow \langle \zeta_n \rangle \longrightarrow \overline{K}^\times \xrightarrow{a \to a^n} \overline{K}^\times \longrightarrow 1$ successione esatta di $G := Gal(\overline{K}/K)$ - moduli

$1 \longrightarrow \langle \zeta_n \rangle \longrightarrow K^\times \longrightarrow K^\times \xrightarrow{\partial} H^1(G, \langle \zeta_n \rangle) \longrightarrow 0$
$K^\times / K^{\times n} \simeq H^1(G, \langle \zeta_n \rangle) = Hom(G, \mathbb{Z}/n\mathbb{Z})$



$\partial(\beta) = \left(g \longmapsto \frac{g(\beta^{1/n})}{\beta^{1/n}}\right)$
$\Longrightarrow \overline{K}^{Ker\varphi} = K(\sqrt[n]{\beta})$

Risoluzione proiettiva di $\mathbb{Z}$ come $\mathbb{Z}[G]$-modulo, $G = \langle \sigma \rangle$

$|G| = n$

$$\ldots \longrightarrow \mathbb{Z}[G] \xrightarrow{\cdot(\sigma-1)} \mathbb{Z}[G] \xrightarrow{\cdot N} \mathbb{Z}[G] \xrightarrow{\cdot(\sigma-1)} \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0$$
$$g \longmapsto 1$$

$\mathbb{Z}[G] = \frac{\mathbb{Z}[\sigma]}{(\sigma^n - 1)} \ni a_0 + a_1\sigma + a_2\sigma^2 + \ldots + a_{n-1}\sigma^{n-1}$
$(a_0 + a_1\sigma + \ldots + a_{n-1}\sigma^{n-1})(\sigma - 1) = 0 \iff a_0\sigma + a_1\sigma^2 + \ldots + a_{n-1}\sigma^n = a_0 + a_1\sigma + \ldots + a_{n-1}\sigma^{n-1}$
$Ker(\cdot(\sigma-1)) = \{a(\underbrace{1 + \sigma + \ldots + \sigma^{n-1}}_{N}) \mid a \in \mathbb{Z}\} = \mathbb{Z}[G] \cdot N$
$(c_0 + c_0\sigma + \ldots + c_{n-1}\sigma^{n-1}) \cdot N = (c_0 + c_1 + \ldots + c_{n-1}) \cdot N$

Chi è $Ker(\cdot N)$? Sono i "polinomi" in σ che si annullano in $1 \longrightarrow$ è $(\sigma - 1)$

Conseguenza: calcolo di $H^i(G, A)$ se $G = \langle \sigma \rangle$

$$\ldots \longleftarrow Hom(\mathbb{Z}[G], A) \xleftarrow{(\cdot N)^*} Hom(\mathbb{Z}[G], A) \xleftarrow{(\sigma-1)^*} Hom(\mathbb{Z}[G], A) \xleftarrow{\Phi} 0$$
$$A \xleftarrow{N^*} A \xleftarrow{} A$$
$$\varphi(\sigma - 1) \longleftarrow \varphi(1)$$
$$x + \sigma x + \sigma^2 x + \ldots \qquad \varphi(\sigma) - \varphi(1)$$
$$N(x) \longleftarrow x$$

$H^0(G, A) = A^G$

$$H^i(G, A) = \begin{cases} A^G & \text{per } i = 0 \\ Ker(N: A \to A)/Im(\sigma - 1) & \text{per } i \geq 1 \text{ dispari} \\ A^G/N(A) & \text{per } i \geq 2 \text{ pari} \end{cases}$$

Es $H^2(\underbrace{\mathbb{Z}/2\mathbb{Z}}_{G}, \underbrace{\mathbb{Z}/2\mathbb{Z}}_{A}) = \frac{\mathbb{Z}/2\mathbb{Z}}{\{0\}} = \mathbb{Z}/2\mathbb{Z} \longleftrightarrow Ext(G, A)$
$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow E \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$

la classe non banale corrisponde a $\mathbb{Z}/4\mathbb{Z}$

$c: G \times G \longrightarrow \mathbb{Z}/2\mathbb{Z} \rightsquigarrow E = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$(0,*) \longmapsto 0$
$(*,0) \longmapsto 0$
$(1,1) \longmapsto 1$
$(a_1, g_1) * (a_2, g_2) = (a_1 + a_2 + c(g_1, g_2), g_1 g_2)$
$(1,1) * (1,1) = (1,0)$

Teorema di Schur-Zassenhaus

Sia G gruppo finito, $N \trianglelefteq G$. Supponiamo $(|N|, |G/N|) = 1$.
Allora $G \simeq N \rtimes G/N$.
Equivalentemente: $1 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 1$
$\exists s$ omo di gruppi.

Oss Se N è abeliano: già visto.

DIMOSTRAZIONE
Per induzione su $|G| = a \cdot b$, $a = |N|$, $b = |G/N|$.
Se $|G| = 1$, ok; anche se $a = 1$ o $b = 1$.
Passo 1 Posso supporre N minimale tra i sgp normali di G.
Se esiste $\{e\} \subsetneq N' \subsetneq N$, $N' \trianglelefteq G$, considero
$1 \longrightarrow \underbrace{N/N'}_{\#N/\#N' \mid \#N} \longrightarrow G/N' \longrightarrow \underbrace{G/N}_{b} \longrightarrow 1$
Per hp. ind., G/N' contiene un sgp $K/N' \simeq G/N$ (con $K < G$, $K \supseteq N'$).
Ora $|K| = |G/N| \cdot |N'| < |G|$
$1 \longrightarrow N' \longrightarrow K \longrightarrow K/N' \longrightarrow 1$
e riapplico l'hp. ind.: $\#N' \mid \#N$ è coprimo con $\#G/\#N$
$\Longrightarrow$ K contiene sgp isomorfo a $G/N \Longrightarrow$ G contiene sgp isomorfo a G/N.
Passo 2 Posso supporre N sia un p-gruppo.
Fisso $p \mid \#N$ e fisso P p-Sylow di N. Per Frattini,
$G = N \cdot N_G(P) \Longrightarrow G/N \simeq N_G(P)/N \cap N_G(P)$
Se $N_G(P) \neq G \iff P \not\trianglelefteq N$ (e quindi in particolare $N \cap N_G(P) \subsetneq N$)
considero $1 \longrightarrow N \cap N_G(P) \longrightarrow \underbrace{N_G(P)}_{\text{ha card} < \#G} \longrightarrow G/N \longrightarrow 1$
$\Longrightarrow$ per hp. ind. $\exists$ sgp di $N_G(P)$ isomorfo a G/N.
Se invece $N_G(P) = G \Longrightarrow P \trianglelefteq G \Longrightarrow P \trianglelefteq N$
Siccome N è minimale, $P = N$.
Passo 3 $\{e\} \subsetneq \underbrace{Z(P) \subseteq P}_{\text{caratt}} = N \trianglelefteq G \Longrightarrow Z(P) \trianglelefteq G$

Per minimalità di N, $Z(P) = P$.
Passo 4 Basta farlo per $N = Z(P)$ abeliano. □

Ext¹ ed estensioni

Def. Sia R un anello con unità, A, C due R-moduli.
Un'estensione di C tramite A è una successione esatta di R-moduli

$$0 \longrightarrow A \longrightarrow E \longrightarrow C \longrightarrow 0$$

Due estensioni E, E' sono isomorfe se $\exists \varphi : E \longrightarrow E'$ che fa commutare

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & C & \longrightarrow & 0 \\ & & \| & & \downarrow \varphi & & \| & & \\ 0 & \longrightarrow & A & \longrightarrow & E' & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

Se φ esiste, è automaticamente un isomorfismo.

Dimostreremo che $\mathrm{Ext}^1_R(C,A) \longleftrightarrow \{\text{est. di } C \text{ tramite } A\}/_{\text{isom}}$.

Def. Data $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ estensione,
applichiamo $\mathrm{Hom}(-, A)$:

$$0 \longrightarrow \mathrm{Hom}(C,A) \longrightarrow \mathrm{Hom}(B,A) \longrightarrow \mathrm{Hom}(A,A) \xrightarrow{\partial} \mathrm{Ext}^1(C,A)$$
$$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \varphi \mid \mathrm{id}$$

Definiamo la classe associata all'estensione come $\partial(\mathrm{id}_A)$

Oss Se l'estensione è split, la classe in Ext^1 è zero:

$$0 \longrightarrow A \xrightarrow{i} A \oplus C \xrightarrow{\pi} C \longrightarrow 0$$

Siccome $\mathrm{Hom}(-, A)$ è additivo

$$0 \longrightarrow \mathrm{Hom}(C,A) \longrightarrow \mathrm{Hom}(A \oplus C, A) \longrightarrow \mathrm{Hom}(A,A) \longrightarrow 0 \quad \text{esatta}$$
$$0 \longrightarrow \mathrm{Hom}(C,A) \longrightarrow \mathrm{Hom}(A \oplus C, A) \longrightarrow \mathrm{Hom}(A,A) \xrightarrow{\partial} \mathrm{Ext}^1(C,A)$$
$$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \| \mid 0$$

e quindi $\partial(\mathrm{id}_A) = 0$.

Controlliamo che questa def. dipende solo dalla classe di isom. dell'est.

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & C & \longrightarrow & 0 \\ & & \| & & \downarrow \varphi & & \| & & \\ 0 & \longrightarrow & A & \longrightarrow & E' & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

$$\rightsquigarrow \quad \begin{array}{ccc} \mathrm{Hom}(A,A) & \xrightarrow{\partial} & \mathrm{Ext}^1(C,A) \\ \downarrow \mathrm{id} & \circlearrowright & \downarrow \mathrm{id} \\ \mathrm{Hom}(A,A) & \xrightarrow{\partial'} & \mathrm{Ext}^1(C,A) \end{array}$$

Sia $\Theta : \{\text{est di } C \text{ tramite } A\}/_{\text{isom}} \longrightarrow \mathrm{Ext}^1(C,A)$ tale mappa.
Per mostrare che è una bigezione, costruiamo un'inversa.

Pushout Supponiamo di avere un'estensione

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & B & \xrightarrow{p} & C & \longrightarrow & 0 \\ & & \downarrow \phi & & \vdots \psi & & \| & & \\ 0 & \longrightarrow & A' & \xrightarrow{i'} & B' & \xrightarrow{p'} & C & \longrightarrow & 0 \end{array}$$

e un omo di R-moduli $\phi : A \longrightarrow A'$

Prendiamo $B' := A' \amalg_\phi B = A' \oplus B / \langle (\phi(a), -i(a)) \mid a \in A \rangle$

Chi sono le mappe?

- $i' : A' \longrightarrow A' \oplus B \longrightarrow A' \amalg_\phi B$

  $\psi : B \hookrightarrow A' \oplus B \longrightarrow A' \amalg_\phi B$

  Il quadrato di sx commuta:

  $a \longmapsto i(a) \longmapsto \overline{(0, i(a))}$

  $a \longmapsto \phi(a) \longmapsto \overline{(\phi(a), 0)} = \overline{(0, i(a))}$

- i' iniettiva.
- $p' : A' \oplus B / \langle \dots \rangle \longrightarrow C$

  $\overline{(a', b)} \longmapsto p(b)$

  Per la buona def serve che $(\phi(a), -i(a)) \longmapsto p(-i(a)) = -p(i(a)) = 0$

Teorema Θ è bigettiva.

DIMOSTRAZIONE

Costruiamo l'inversa. Fissiamo una succ. esatta

$0 \longrightarrow M \xrightarrow{j} P \longrightarrow C \longrightarrow 0$ con P proiettivo.

Applichiamo $\mathrm{Hom}(-, A)$:

$0 \longrightarrow \mathrm{Hom}(C,A) \longrightarrow \mathrm{Hom}(P,A) \longrightarrow \mathrm{Hom}(M,A) \xrightarrow{\partial} \mathrm{Ext}^1(C,A) \longrightarrow \mathrm{Ext}^1(P,A) = 0$

Data $x \in \mathrm{Ext}^1(C,A)$, $\exists \alpha \in \mathrm{Hom}(M,A)$ t.c. $\partial\alpha = x$.

$$\begin{array}{ccccccc} 0 & \longrightarrow & M & \xrightarrow{j} & P & \longrightarrow & C \longrightarrow 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \phi} & & \| \\ E: \ 0 & \longrightarrow & A & \longrightarrow & A \amalg_\alpha P & \longrightarrow & C \longrightarrow 0 \end{array}$$

Affermo che $\Theta(E) = x$.

Applico $\mathrm{Hom}(-, A)$.

$$\begin{array}{ccccc} \alpha \in \mathrm{Hom}(M,A) & \xrightarrow{\partial} & \mathrm{Ext}^1(C,A) & \ni \partial\alpha = \Theta(E) = x \\ \uparrow{\scriptstyle \alpha^*} & \circlearrowright & \| & \\ \mathrm{Hom}(A,A) & \xrightarrow{\partial_E} & \mathrm{Ext}^1(C,A) & \\ \mathrm{id} \in & & \Theta(E) & \end{array}$$

Quindi ho costruito un'est. con classe x.

Controlliamo cosa succede se scelgo un diverso $\alpha' \in \mathrm{Hom}(M,A)$ con $\partial\alpha' = x$.

$\partial\alpha = \partial\alpha' \iff \partial(\alpha - \alpha') = 0 \iff \alpha - \alpha' \in \mathrm{Im}(\mathrm{Hom}(P,A) \xrightarrow{j^*} \mathrm{Hom}(M,A))$

$\iff \exists f : P \to A$ con $\alpha - \alpha' = f \circ j$

Voglio costruire un omomorfismo

$$A \amalg_\alpha P \longrightarrow A \amalg_{\alpha'} P$$

Prendo $i : A \longrightarrow A \amalg_\alpha P$ e $\sigma + if : P \longrightarrow A \amalg_\alpha P$

Prendo $(\alpha'(m), -j(m))$ con $m \in M$: sta nel nucleo perché

$i(\alpha'(m)) + (\sigma + if)(-j(m)) = (i\alpha' - \sigma j - if j)(m) = (i\alpha' - i\alpha - if j)(m)$

$= i\alpha(\alpha' - \alpha - fj)(m) = 0$ □

⚠ Si potrebbe fare tutto usando solo moduli iniettivi.

Dimensione proiettiva e dimensione globale

Def. Sia A un anello, M un A-modulo.
La dimensione proiettiva di M è
$$pd = \inf\{n \geq 0 \mid 0 \to P_n \to \dots \to P_1 \to P_0 \to M \to 0 \text{ con } P_i \text{ proiettivi}\}$$
Se M non ammette una ris. proiettiva finita, $pd(M) = +\infty$.

Esempio
- A campo: ogni M è proiettivo $\quad 0 \to M \to M \to 0$ e $pd(M) = 0 \ \forall M$
- $A = \mathbb{Z}$ (PID): $\quad 0 \to \mathbb{Z}^{\oplus J} \to \mathbb{Z}^{\oplus I} \to M \to 0 \quad \to pd(M) \leq 1$
  Esistono esempi con $pd(M) = 0$ (ad es. $M = \mathbb{Z}$)
  e con $pd(M) = 1$ (ad es. $M = \mathbb{Q}$, non proiettivo)
- $M = \mathbb{Z}/2\mathbb{Z}$: calcoliamo $Ext^1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \neq (0)$
  1° modo ci sono almeno 2 est. di $\mathbb{Z}/2\mathbb{Z}$ tramite $\mathbb{Z}/2\mathbb{Z}$ nella categoria degli $\mathbb{Z}$-moduli.
  2° modo $\quad 0 \to \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$
  $\quad \downarrow \ \mathrm{Hom}(-, \mathbb{Z}/2\mathbb{Z})$
  $0 \leftarrow \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \xleftarrow{(\cdot 2)^*} \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \leftarrow 0$
  $0 \leftarrow \mathbb{Z}/2\mathbb{Z} \xleftarrow{0} \mathbb{Z}/2\mathbb{Z} \leftarrow 0$
  $\Longrightarrow Ext^0(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) = Ext^1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$
  In generale, $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/(m,n)\mathbb{Z}$
  $Ext^1(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/m\mathbb{Z} \,/\, n(\mathbb{Z}/m\mathbb{Z}) \simeq \frac{\mathbb{Z}/m\mathbb{Z}}{(n\mathbb{Z}+m\mathbb{Z})/m\mathbb{Z}} \simeq \frac{\mathbb{Z}}{(m,n)\mathbb{Z}}$

Def. La dimensione globale di A è
$$gldim(A) = \sup\{pd(M) \mid M \in |Mod_A|\}$$

Esempio $gldim(K) = 0$
$gldim(\mathbb{Z}) = 1$

Teorema di Auslander-Buchsbaum-Serre $(A, \mathfrak{M})$ locale Noetheriano.
(i) $gldim(A) < +\infty \iff A$ regolare.
(ii) Se vale una delle condizioni in (i), allora
$$gldim(A) = \dim(A).$$

Conseguenze
1) A Noeth. regolare, P primo $\Longrightarrow A_P$ regolare
2) A Noeth. di dim Krull d finita. Allora
   A è regolare $\iff gldim \leq d$
   e in tal caso coincidono.
3) Teorema delle syzigie di Hilbert:
   se K è un campo e $A = K[x_1, \dots, x_n]$, ogni A-modulo
   ha una ris. proiettiva di lunghezza $\leq n$.

Fatto Ogni mod. proiettivo fin.gen. su $K[x_1, \dots, x_n]$ è libero
$\Longrightarrow$ ogni A-mod fin.gen. ha una ris. proiettiva libera finita.

Lemma A anello, $M \in Mod_A$. Sono equivalenti:

(i) $pd(M) \leq d$

(ii) $Ext^i(M,N)=0 \quad \forall N \in Mod_A \quad \forall i>d$

(iii) $Ext^{d+1}(M,N)=0 \quad \forall N \in Mod_A$

(iv) Per ogni succ. esatta

$$0 \longrightarrow M_d \longrightarrow P_{d-1} \longrightarrow \dots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

con $P_0, \dots, P_{d-1}$ proiettivi, anche M_d è proiettivo.

DIMOSTRAZIONE

(ii) $\Rightarrow$ (iii) ovvio

(i) $\Rightarrow$ (ii) usando una ris. di lungh $\leq d$ per calcolare Ext^i

(iv) $\Rightarrow$ (i) comincio a costruire una ris. proiettiva al solito modo

(iv) mostra che a lungh. d mi fermo.

(iii) $\Rightarrow$ (iv) Partiamo da una succ. esatta

$$0 \longrightarrow M_d \longrightarrow P_{d-1} \longrightarrow \dots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

e la spezziamo in succ. esatte corte

$$0 \longrightarrow M_{j+1} \longrightarrow P_j \longrightarrow M_j \longrightarrow 0$$

dove $M_0 = M$ e M_d compaiono nella succ.

Per ogni $N \in Mod_A$, applicando la s.e.l. di $Hom(_,N)$ trovo

$$\underset{0}{\underset{\parallel}{Ext^{i-1}(P_j,N)}} \longrightarrow Ext^{i-1}(M_{j+1},N) \xrightarrow{\sim} Ext^i(M_j,N) \longrightarrow \underset{0}{\underset{\parallel}{Ext^i(P_j,N)}} \qquad \forall i \geq 2$$

Quindi $Ext^{i-1}(M_{j+1},N) \cong Ext^i(M_j,N)$

$$\Rightarrow Ext^1(M_d,N) \cong Ext^2(M_{d-1},N) \cong \dots \cong \underset{0 \text{ per (iii)}}{\underset{\parallel}{Ext^{d+1}(M_0,N)}}$$

Per la caratterizzazione dei proiettivi, M_d è proiettivo. □

corollario $gldim(A) = \inf\{d \geq 0 \mid Ext^d(M,N)=(0) \ \forall M,N\}$

Lemma $Ext^i(M,N)=(0) \ \forall M,N \iff Ext^i(M,N)=(0) \ \forall N \ \forall M$ fin.gen.

DIMOSTRAZIONE

Baer per $i=1$ + dimension shifting

corollario $gldim(A) = \sup\{pd(M) \mid M \text{ fin.gen}\}$.

proposizione $(A,\mathfrak{m},k)$ locale Noetheriano, M A-mod fin.gen. Allora
$$\mathrm{pd}(M)\le d \iff \mathrm{Tor}_{d+1}(M,k)=(0)$$

DIMOSTRAZIONE

($\Longrightarrow$) Usando una ris. proiettiva di lungh $\le d$.

($\Longleftarrow$) Per induzione su d

- $d=0$: abbiamo visto che $\mathrm{Tor}_1(M,k)=0 \Longrightarrow M$ libero $\Longrightarrow \mathrm{pd}(M)=0$.
- $d\ge 1$: prendiamo $0\to N\to P\to M\to 0$ con P proiettivo.

  Prendendo ok troviamo
  $$\mathrm{Tor}_i(P,k)\to \mathrm{Tor}_i(M,k)\xrightarrow{\sim}\mathrm{Tor}_{i-1}(N,k)\to \mathrm{Tor}_{i-1}(P,k) \quad \forall i\ge 2$$
  $$\qquad\quad 0 \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad 0$$
  In particolare $0=\mathrm{Tor}_{d+1}(M,k)\cong \mathrm{Tor}_d(N,k)$

  Wlog P è fin.gen (lo prendo libero di rango $=$ n° di generatori di M);
  anche $N\subseteq P$ è fin.gen. perché A è Noeth.

  Per hp. ind. so N, $\mathrm{pd}(N)\le d-1$.

  Se $0\to Q_{\bullet}\to N\to 0$ è tale ris, allora

  $0\to Q_{\bullet}\to P\to M\to 0$ è ris. di M di lungh $\le d$. □

teorema A anello Noetheriano regolare, $P\in \mathrm{Spec}A$.
Allora A_P è regolare.

DIMOSTRAZIONE

Sia M un massimale che contiene P. Vale $(A_M)_P\cong A_P$

Quindi posso supporre A locale regolare

Per ABS, $\mathrm{gldim}(A)<+\infty$: ogni A-mod ha una ris. proiettiva finita.

Sia $r=\dim A<+\infty$. Considero
$$0\to K_r\to A^{d_{r-1}}\to\cdots\to A^{d_1}\to A^{d_0}\to A/P\to 0$$
Siccome $\mathrm{pd}(A/P)\le \mathrm{gldim}(A)\underset{ABS}{=}\dim A=r$, per il lemma K_r è proiettivo e fin.gen.
$\Longrightarrow K_r$ è libero: $K_r=A^{d_r}$

Tensorizzo per A_P, che è piatto su A:
$$0\to A_P^{d_r}\to A_P^{d_{r-1}}\to\cdots\to A_P^{d_0}\to A_P\underset{A_P}{\otimes}A/P\to 0$$
$$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \cong A_P/PA_P$$
è una ris. proiettiva finita di A_P/PA_P.

Questo implica $\mathrm{gldim}(A_P)<+\infty$.

In effetti, usando tale ris. proiettiva, posso calcolare
$$\mathrm{Tor}_{r+1}(M,A_P/PA_P)=(0)\ \forall M\in \mathrm{Mod}_{A_P}\Longrightarrow \mathrm{pd}(M)\le r$$
$$\Longrightarrow \mathrm{gldim}(A_P)\le r \overset{ABS}{\Longrightarrow} A_P \text{ è regolare.}$$ □

Teorema A anello Noetheriano di dim Krull $d<+\infty$.
Vale A regolare $\iff$ $\mathrm{gldim}(A)\leq d$
e in tal caso $\mathrm{gldim}(A)=d$.

DIMOSTRAZIONE
($\Longleftarrow$) Fissiamo P un ideale massimale di A.
Sappiamo $r=\mathrm{gldim}(A)<+\infty$, c'è una ris. di lungh. $\leq r$ di A/P come A-mod
$Q_\bullet \longrightarrow A/P \longrightarrow 0$. Tensorizzo per A_P (che è piatto) e
trovo una ris. proiettiva $Q_\bullet \otimes A_P \longrightarrow A_P/PA_P \longrightarrow 0$ come A_P-moduli
Come prima $\mathrm{gldim}(A_P)<+\infty \overset{\text{ABS}}{\Longrightarrow} A_P$ regolare e $\dim(A_P)=\mathrm{gldim}(A_P)\leq r$
$\dim A=\sup_P \dim A_P \leq r=\mathrm{gldim}(A)\leq \dim A \implies \dim A=\mathrm{gldim}\,A$
($\Longrightarrow$) Sia A regolare, M A-modulo fin.gen. Scriviamo
$$0\longrightarrow M_d\longrightarrow P_{d-1}\longrightarrow \dots\longrightarrow P_1\longrightarrow P_0\longrightarrow M\longrightarrow 0$$
con P_i proiettivi. Devo dim. che M_d è proiettivo, equiv. loc. liberi
Sia Q un primo. La localizzazione A_Q è regolare, quindi per ABS
$\mathrm{gldim}(A_Q)=\dim(A_Q)\leq \dim A \implies \mathrm{pd}(M\otimes A_Q)\leq \mathrm{gldim}(A_Q)\leq d$
$$0\longrightarrow M_d\otimes A_Q\longrightarrow P_{d-1}\otimes A_Q\longrightarrow \dots\longrightarrow P_0\otimes A_Q\longrightarrow M\otimes A_Q\longrightarrow 0$$
Per il lemma, $M_d\otimes A_Q$ è proiettivo $\implies$ libero.
Questo vale $\forall Q$, quindi M_d è proiettivo $\implies \mathrm{pd}(M)\leq d$ $\forall M$
$\implies \mathrm{gldim}(A)\leq d$. □

Lemma $(A,\mathfrak{m},k=A/\mathfrak{m})$ locale Noetheriano.
$\mathrm{gldim}(A)\leq r \iff \mathrm{Tor}_{r+1}(M,k)=0\ \forall M\in \mathrm{Mod}_A \iff k$ ammette una ris. proiettiva di lunghezza al massimo r

ES $H^2(S_3,\mathbb{Z})$ dove $\mathbb{Z}=S_3$-modulo banale

SOL $0\longrightarrow \mathbb{Z}\longrightarrow \mathbb{Q}\longrightarrow \mathbb{Q}/\mathbb{Z}\longrightarrow 0$ succ. esatta di gruppi con azione banale
$$0\longrightarrow \mathbb{Z}\longrightarrow \mathbb{Q}\longrightarrow \mathbb{Q}/\mathbb{Z}\xrightarrow{0} H^1(S_3,\mathbb{Z})\longrightarrow H^1(S_3,\mathbb{Q})\longrightarrow H^1(S_3,\mathbb{Q}/\mathbb{Z})\longrightarrow$$
$$\longrightarrow H^2(S_3,\mathbb{Z})\longrightarrow H^2(S_3,\mathbb{Q})\longrightarrow \dots$$
$H^1(S_3,\mathbb{Z})=\mathrm{Hom}(S_3,\mathbb{Z})=(0)$
$H^1(S_3,\mathbb{Q})=\mathrm{Hom}(S_3,\mathbb{Q})=(0)$
$H^1(S_3,\mathbb{Q}/\mathbb{Z})=\mathrm{Hom}(S_3,\mathbb{Q}/\mathbb{Z})=\mathrm{Hom}(S_3/S_3',\mathbb{Q}/\mathbb{Z})=\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z},\mathbb{Q}/\mathbb{Z})=\mathbb{Z}/2\mathbb{Z}$
$H^2(S_3,\mathbb{Q})$ è un gruppo abeliano di 6-torsione su cui
- 6 è un isomorfismo (perché $6\in S_3$)
$\implies H^2(S_3,\mathbb{Q})=(0)$
$\implies H^2(S_3,\mathbb{Z})\cong \mathbb{Z}/2\mathbb{Z}$

ES $1\longrightarrow A\times A\longrightarrow G\longrightarrow \mathbb{Z}/2\mathbb{Z}\longrightarrow 1$ dove $\mathbb{Z}/2\mathbb{Z}$ agisce su A tramite $1\cdot(a_1,a_2)=(a_2,a_1)$
Dimostrare che $G\cong (A\times A)\rtimes \mathbb{Z}/2\mathbb{Z}$

SOL $H^2(\mathbb{Z}/2\mathbb{Z},A\times A)=(A\times A)^G/N(A\times A)=\{(a,a)\}/\langle (a_1,a_2)+(a_2,a_1)\rangle=0$
Prendendo (a,id) trovo $N(a,\mathrm{id})=(a,a)$

Def. (i) Dato un complesso $B_\bullet$, chiamiamo $B[-1]_\bullet$ il complesso

$$B[-1]_n := B_{n-1}, \qquad d_n^{B[-1]} := (-1)\, d_{n-1}^B$$

(ii) Sia $f_\bullet : B_\bullet \longrightarrow C_\bullet$ un morfismo di complessi.
Definiamo il complesso $\mathrm{cone}(f)_\bullet$ come

$$\begin{array}{ccccc} C_{n+1} & \longrightarrow & C_n & \longrightarrow & C_{n-1} \\ {\scriptstyle f_{n+1}}\uparrow & & {\scriptstyle f_n}\uparrow & & {\scriptstyle f_{n-1}}\uparrow \\ B_{n+1} & \longrightarrow & B_n & \longrightarrow & B_{n-1} \end{array}$$

$$\begin{array}{ccccc} C_{n+1} & \longrightarrow & C_n & \longrightarrow & C_{n-1} \\ & \nearrow_{f_n} & & \nearrow_{f_{n-1}} & \\ B_n & \longrightarrow & B_{n-1} & \longrightarrow & B_{n-2} \end{array}$$

$$\mathrm{cone}(f)_n := C_n \oplus B[-1]_n = C_n \oplus B_{n-1}$$

$$d_n^{\mathrm{cone}(f)} : C_n \oplus B_{n-1} \longrightarrow C_{n-1} \oplus B_{n-2}$$
$$(c, b) \longmapsto (d_n^C(c) + f_{n-1}(b), -d_{n-1}^B(b))$$

$$d_n^{\mathrm{cone}(f)} = \left(\begin{array}{c|c} d_n^C & f_{n-1} \\ \hline & -d_{n-1}^B \end{array}\right)$$

$$d_{n-1}^{\mathrm{cone}(f)} \circ d_n^{\mathrm{cone}(f)} = \left(\begin{array}{c|c} d_{n-1}^C & f_{n-2} \\ \hline & -d_{n-2}^B \end{array}\right)\left(\begin{array}{c|c} d_n^C & f_{n-1} \\ \hline & -d_{n-1}^B \end{array}\right) = \left(\begin{array}{c|c} d_{n-1}^C \circ d_n^C = 0 & d_{n-1}^C \circ f_{n-1} - f_{n-2} \circ d_{n-1}^B = 0 \\ \hline 0 & d_{n-2}^B \circ d_{n-1}^B = 0 \end{array}\right)$$

Lemma C'è una successione esatta corta

$$0 \longrightarrow C_\bullet \longrightarrow \mathrm{cone}(f_\bullet) \longrightarrow B[-1]_\bullet \longrightarrow 0$$
$$C_n \hookrightarrow C_n \oplus B_{n-1} \twoheadrightarrow B_{n-1}$$

DIMOSTRAZIONE

Esattezza come moduli $\forall$

$$\begin{array}{ccc} C_n & \xrightarrow{i_n} & \mathrm{cone}(f_\bullet)_n \\ {\scriptstyle d_n^C}\downarrow & & \downarrow{\scriptstyle d_n^{\mathrm{cone}(f)}} \\ C_{n-1} & \xrightarrow{i_{n-1}} & \mathrm{cone}(f_\bullet)_{n-1} \end{array}$$

$$\begin{array}{ccc} c & \longmapsto & (c, 0) \\ \downarrow & & \downarrow \\ d_n^C(c) & \longmapsto & (d_n^C(c), 0) \end{array} \qquad \begin{pmatrix} d_n^C & f_{n-1} \\ 0 & d_{n-1}^B \end{pmatrix}\begin{pmatrix} c \\ 0 \end{pmatrix} = \begin{pmatrix} d_n^C(c) \\ 0 \end{pmatrix}$$

Similmente per la proiezione. □

Def. Sia M un A-modulo e $x_1, \dots, x_d \in A$.
Definiamo il complesso di Koszul $K(x_1, \dots, x_d; M) = K(d; M)$ come

$d=1$ $K(1; M)$: $\underset{2}{0} \longrightarrow \underset{1}{M} \xrightarrow{\cdot x_1} \underset{0}{M} \longrightarrow 0$

$d \geq 2$ $K(d; M) = \mathrm{cone}\left(K(d-1, M) \xrightarrow{\cdot x_d} K(d-1; M)\right)$

esempio $K(1,M)$

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M & \xrightarrow{\cdot x_1} & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \cdot x_2} & & \downarrow{\scriptstyle \cdot x_2} & & \\
0 & \longrightarrow & M & \xrightarrow{\cdot x_1} & M & \longrightarrow & 0
\end{array}$$

$$\begin{array}{ccccccccc}
 & & 0 & \longrightarrow & M & \xrightarrow{\cdot x_1} & M & \longrightarrow & 0 \\
 & & \oplus & \nearrow{\scriptstyle \cdot x_2} & \oplus & \nearrow{\scriptstyle \cdot x_2} & \oplus & & \\
0 & \longrightarrow & M & \xrightarrow[\cdot(-x_1)]{} & M & \longrightarrow & 0 & &
\end{array}$$

$K(2,M)$

$$0 \longrightarrow M \xrightarrow{\iota} M^2 \xrightarrow{\pi} M \longrightarrow 0$$

$$\begin{pmatrix} m_1 \\ m_2 \end{pmatrix} \longmapsto x_1 m_1 + x_2 m_2$$

$$m \longmapsto (x_2 m, -x_1 m)$$

$K(3,M)$

$$0 \longrightarrow M \longrightarrow M^3 \longrightarrow M^3 \longrightarrow M \longrightarrow 0$$

$$\begin{pmatrix} m_1 \\ m_2 \\ m_3 \end{pmatrix} \longmapsto x_1 m_1 + x_2 m_2 + x_3 m_3$$

$$\begin{pmatrix} m_1 \\ m_2 \\ m_3 \end{pmatrix} \longmapsto \begin{pmatrix} x_2 m_3 - x_3 m_2 \\ x_3 m_1 - x_1 m_3 \\ x_1 m_2 - x_2 m_1 \end{pmatrix}$$

Lemma $K(d;M)_i \simeq M^{\binom{d}{i}}$

DIMOSTRAZIONE

È vero per $d=1$;

$$K(d+1;M)_i = K(d;M)_i \oplus K(d;M)_{i-1} \simeq M^{\binom{d}{i}} \oplus M^{\binom{d}{i-1}} = M^{\binom{d+1}{i}} \quad \square$$

Coomologia di $K(d;M)$

$0 \longrightarrow K(d-1;M)_\bullet \longrightarrow K(d;M)_\bullet \longrightarrow K(d-1;M)[-1]_\bullet \longrightarrow 0$ per il lemma sai coni

In omologia ottengo:

$$H_i(K(d-1;M)_\bullet) \longrightarrow H_i(K(d;M)_\bullet) \longrightarrow H_i(K(d-1;M)[-1]_\bullet) \xrightarrow{\partial} H_{i-1}(K(d-1;M)_\bullet)$$

$$\| \quad H_{i-1}(K(d-1;M)_\bullet)$$

Calcolo di ∂:

$$0 \longrightarrow A_\bullet \longrightarrow B_\bullet \longrightarrow C_\bullet \longrightarrow 0 \qquad H_i(C_\bullet) \longrightarrow H_{i-1}(A_\bullet)$$

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A_i & \longrightarrow & B_i & \xrightarrow{c} & C_i & \longrightarrow & 0 \\
 & & & & \uparrow{\scriptstyle b} & & & & \\
0 & \longrightarrow & A_{i-1} & \longrightarrow & B_{i-1} & \longrightarrow & C_{i-1} & \longrightarrow & 0 \\
 & & a_{i-1} & \rightsquigarrow & d_i^B(b) & & & &
\end{array}$$

$$\partial[c] = [a_{i-1}]$$

Nel nostro caso: sia $c \in K(d-1;M)_{i-1} = K(d-1;M)[-1]_i$

sollevamento di c in $K(d;M)_i = K(d-1;M)_i \oplus K(d-1;M)_{i-1}$ $\quad (0,c)$

Applico il differenziale: $(x_d c, d_{i-1}^{K(d-1;M)}(c)) = (x_d c, 0)$ perché c è un ciclo

Quindi $\partial[c] = [x_d c]$: ∂ è semplicemente $\cdot x_d$

Otteniamo

$$0 \longrightarrow \frac{H_i(K(d-1;M))}{x_d H_i(K(d-1;M))} \longrightarrow H_i(K(d;M)) \longrightarrow H_{i-1}(K(d-1;M))[x_d] \longrightarrow 0$$

proposizione $H_0(K(d;M)) = M/(x_1,\dots,x_d)M$

DIMOSTRAZIONE

$d=1$: $0 \longrightarrow M \xrightarrow{\cdot x_1} M \longrightarrow 0$

$H_0(K(1;M)) = M/x_1M$

$d\geq 2$: uso la successione costruita sopra con $i=0$

$$0 \longrightarrow \frac{H_0(K(d-1;M))}{x_d H_0(K(d-1;M))} \xrightarrow{\sim} H_0(K(d;M)) \longrightarrow 0$$

$$H_0(K(d;M)) \simeq \frac{M/(x_1,\dots,x_{d-1})M}{x_d M/(x_1,\dots,x_{d-1})M} \simeq M/(x_1,\dots,x_d)M \qquad \square$$

def. $x_1,\dots,x_d \in A$, M un A-modulo.
Diciamo che $x_1,\dots,x_d$ è regolare in M se
(i) $[x_i]: M/(x_1,\dots,x_{i-1})M \longrightarrow M/(x_1,\dots,x_{i-1})M$ è iniettiva
(ii) $M/(x_1,\dots,x_d)M \neq (0)$

teorema Se $x_1,\dots,x_d$ è regolare in M si ha
$H_i(K(d;M)) = 0 \quad \forall i \geq 1$.

DIMOSTRAZIONE

Intanto $H_i = 0 \ \forall i \geq d+1$ perché $K(d;M)_i \simeq M^{\binom{d}{i}}$, che è zero per $i > d$.

$d=1$: $0 \longrightarrow M \xrightarrow{\cdot x_1} M \longrightarrow 0 \quad \rightsquigarrow H_1 = M[x_1] = (0)$

$d\geq 2, i\geq 2$:

$$0 \longrightarrow \underbrace{\frac{H_i(K(d-1;M))}{x_d H_i(K(d-1;M))}}_{=0} \longrightarrow H_i(K(d;M)) \longrightarrow \underbrace{H_{i-1}(K(d-1;M))}_{=0}[x_d] \longrightarrow 0$$

per hp ind.

$d\geq 2, i=1$: $0 \longrightarrow 0 \longrightarrow H_1(K(d;M)) \xrightarrow{\sim} H_0(K(d-1;M))[x_d] \longrightarrow 0$

ma $H_0(K(d-1;M)) = M/(x_1,\dots,x_{d-1})M$

Per ipotesi, $\cdot x_d : M/(x_1,\dots,x_{d-1})M \longrightarrow M/(x_1,\dots,x_{d-1})M$ è iniettiva

$\Longrightarrow H_1(K(d;M)) = (0)$.

$\square$

Teorema Sia $(A, \mathfrak{m})$ locale Noetheriano.
Se A è regolare, allora $\operatorname{gldim}(A)$ è finita
e in effetti $\operatorname{gldim}(A) = \dim(A)$.

DIMOSTRAZIONE

Per dimostrare che $\operatorname{gldim}(A) < +\infty$, basta trovare d t.c.
$\operatorname{Tor}_{d+1}(k, M) = (0) \quad \forall M$

Basta trovare una risoluzione proiettiva di k di lungh $\leq d$.

A regolare $\Rightarrow \exists\, x_1, \dots, x_d$ sist. reg. di parametri
che è anche una succ. regolare in A

Il complesso $K(x_1, \dots, x_d; A)$. è esatto in grado ≥ 1 e

$$H_0 = A/(x_1, \dots, x_d)A \simeq k$$

$$0 \to \underset{d}{A} \to \dots \to \underset{2}{A^{\binom{d}{2}}} \to \underset{1}{A^d} \to \underset{0}{A} \to k \to 0$$

è esatta in ogni grado $\Rightarrow$ è una ris. proiettiva di lungh $\leq d$

Per dire $\operatorname{gldim}(A) = d$, basta esibire un modulo che ha dimensione proiettiva d

Dimostriamo che $\operatorname{pd}(k) \geq d$ facendo vedere che $\operatorname{Tor}_d(k, k) \neq 0$

Per calcolarlo prendo $\otimes k$ del complesso sopra:

$$0 \to k \xrightarrow{0} k^d \xrightarrow{0} \dots \xrightarrow{0} k^d \xrightarrow{0} k \to 0$$

I differenziali sono 0 perché combinazioni di $x_1, \dots, x_d$, che sono 0 su k

$\Rightarrow \operatorname{Tor}_d(k, k) \simeq k \neq (0)$. □