RADICALE IN TERMINI DI IDEALI PRIMI

A comm. con id.

$$\mathcal{N} := \sqrt{(0)} = \{ a \in A : \exists n > 0 \text{ t.c. } a^n = 0 \}$$

FATTO:

$$\boxed{\mathcal{N} = \sqrt{(0)} = \bigcap_{\substack{P \triangleleft A \\ P \text{ primo}}} P}$$

DIM

$\boxed{\subseteq}$ Supponiamo che $a \in \sqrt{(0)}$, cioè $a^n = 0$ per qualche n, e dimostriamo che $a \in P$ per ogni P primo.

Sicuramente $a^n \in P \ \forall P$, in quanto $a^n = 0$ e 0 sta in ogni ideale.

Mostriamo che $a \in P$ per ind. su n.

BASE $n = 1 \Rightarrow a \in P \quad \forall P$ ✓

IND Se $a^n \in P$ allora dato che $a^n = a \cdot a^{n-1}$ si ha che $a \in P$ oppure $a^{n-1} \in P$.
Nel primo caso si ha la tesi, nel secondo la tesi segue per ipotesi induttiva.

$\boxed{\supseteq}$ Dato a NON NILPOTENTE, mostriamo che esiste almeno un P primo tale che $a \notin P$. Sia $S := \{ a^n : n \geq 1 \}$

Sia $\mathcal{C} := \{ I \triangleleft A : I \cap S = \emptyset \}$ (*) → a tra un paio di pag

per l'inclusione

Osserviamo che $\mathcal{C}$ è un insieme induttivo:

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

un ms. maggiorante è $I_\infty := \bigcup_{j\geq 1} I_j$

Certamente $I_\infty \supseteq I_j \ \forall j$; basta mostrare che

$I_\infty \in \mathcal{C}$, cioè che

① $I_\infty \cap S = \emptyset$

ma questo è ovvio poiché se l'intersezione fosse non vuota, cioè $\exists n$ t.c. $a^n \in I_\infty \cap S$, allora esisterebbe

j_0 t.c. $a^n \in I_{j_0}$ e ciò è assurdo

② I_∞ è un ideale.

FATTO: unione crescente di ideali è sempre ideale

- se $x, y \in I_\infty$ allora $\exists j_1, j_2$ t.c. $x \in I_{j_1}, y \in I_{j_2}$

  Sia $j = \max\{j_1, j_2\} \Rightarrow x, y \in I_j \Rightarrow$

  $$x + y \in I_j \subseteq I_\infty;$$

- se $x \in I_\infty$ allora $\exists j$ t.c. $x \in I_j$;

  dunque $\forall b \in A$ si ha che $bx \in I_j \subseteq I_\infty$.

Per il Lemma di Zorn $\mathcal{C}$ ammette un elemento massimale Q.

SPERANZA: Q è un ideale primo

$\Rightarrow$ essendo $Q \in \mathcal{C}$ non contiene le potenze di a

e quindi non conterrà neanche $a = a^1$

Siano $x, y \in A$ t.c. $xy \in Q$. Voglio vedere che

$x \in Q$ oppure $y \in Q$

Se $x \notin Q$, l'ideale $(Q, x) \supsetneq Q$

$\Rightarrow$ (Q, x) non può stare in $\mathcal{C}$ poiché Q è max.

$\Rightarrow$ $\exists\, n$ t.c. $a^n \in (Q, x)$, ovvero $\exists\, q_1 \in Q, b_1 \in A$

"$Q + (x)$"

$$a^n = q_1 + b_1 x$$

Similmente se $y \notin Q$ $\exists\, m > 0$, $q_2 \in Q$, $b_2 \in A$

t.c. $a^m = q_2 + b_2 y$

Se per assurdo nessuno appartenesse a Q, allora

$$a^{n+m} = a^n a^m = (q_1 + b_1 x)(q_2 + b_2 y)$$

$$= \underbrace{q_1 q_2}_{\in Q} + \underbrace{q_1 b_2 y}_{\in Q} + \underbrace{q_2 b_1 x}_{\in Q} + \underbrace{b_1 b_2 xy}_{\in Q}$$

$$\in Q$$

Ma Q non contiene pot. di a $\Rightarrow$ ASSURDO.

Dunque Q è primo, $a \notin Q$. $\blacksquare$

(*) Qui ho usato l'assunzione **a NON NILPOTENTE**:

se A fosse nilpotente allora $\exists\, n : a^n = 0$,

cioè $0 \in S = \{a^n : n \geq 0\}$, e quindi l'insieme

$$\mathcal{C} = \{ I \trianglelefteq A : I \cap S = \emptyset \}$$

sarebbe **VUOTO** in quanto ogni ideale di A contiene lo 0;

a quel punto non potrei applicare il Lemma di Zorn

Invece se $a \notin \mathcal{N}$ allora $a \notin (0) \Rightarrow (0) \in \mathcal{C}$.

COROLLARIO Sia $I \lhd A$. Allora

$$\sqrt{I} = \bigcap_{\substack{P \text{ primo di } A \\ P \supset I}} P$$

DIM Sia $B := A/I$, $\pi : A \twoheadrightarrow B$.

Osserviamo che $\pi(I) = (0)_B$.

Mostriamo che $\sqrt{(0)_B} = \pi(\sqrt{I})$

$\boxed{\subseteq}$ Se $b \in B$ è nilpotente ($b^n = 0_B$) allora

$$b = a + I \rightarrow b^n = a^n + I = 0 + I,$$

dunque $a^n \in I$.

Quindi se $b \in \sqrt{(0)_B}$ allora $b = \pi(a)$ per qualche $a \in \sqrt{I}$.

$\boxed{\supseteq}$ Viceversa se $a \in \sqrt{I}$, cioè $a^m = 0$ per qualche $m \geq 0$,

allora $\pi(a)^m = \pi(a^m) = \pi(0) = 0_B$,

cioè $\pi(a) \in \sqrt{(0)}$

Segue quindi che $\sqrt{(0)_B} = \pi(\sqrt{I})$.

Osserviamo che $\sqrt{I} \supseteq I$. Per il Teorema di corrisp. inoltre gli ideali di A contenenti I sono in bigezione con gli ideali di $B = A/I$.

$$\underset{\substack{\| \\ \pi(\sqrt{I})}}{(0)_B} = \bigcap_{Q \text{ primo di } B} Q = \bigcap_{\substack{P \text{ primo di } A \\ P \supseteq I}} \pi(P) \overset{?}{\supseteq} \pi\Big(\underbrace{\bigcap_{\substack{P \text{ primo di } A \\ P \supseteq I}} P}_{\text{è un id. contenente } I}\Big)$$

Mostriamo il contenimento in blu:

$\boxed{\supseteq}$ Ovvio: se prendo l'intersezione di tutti gli insiemi e poi la proietto ottengo elementi che sono necessariamente nella proiezione di ogni singolo insieme;

Segue quindi che $\pi(\sqrt{I}) \supseteq \pi\left(\bigcap_{\substack{P \text{ primo di } A \\ P \supseteq I}} P\right)$, e dal Teorema di corrispondenza

[che conserva le inclusioni tra ideali contenenti I e le loro immagini]

segue che

$$\sqrt{I} \supseteq \bigcap_{\substack{P \text{ primo di } A \\ P \supseteq I}} P$$

Manca quindi l'altro contenimento: se $a \in A$ t.c. $a^n \in I$ per qualche n, e se P è un primo t.c.

$$a^n \in I \subseteq P$$

allora per la stessa definizione di primo $a \in P$, e quindi la tesi. $\blacksquare$

~ o ~ o ~ o ~

APPLICAZIONE: ANELLI DI POLINOMI

A anello comm. con 1, $B = A[x]$.

OSS: se $P \trianglelefteq A$ è primo, posso costruire

$$P[x] := \{ a_0 + a_1 x + \dots + a_n x^n : a_i \in P \}$$

$P[x]$ è un ideale di $A[x]$:

- è chiuso per somma perché la somma è coeff. per coeff.
- $\forall q \in A[x], p \in P[x]$ si ha che $qp \in P[x]$

In effetti siamo

$$p = p_0 + p_1 x + \dots + p_n x^n \qquad p_i \in P$$
$$q = q_0 + q_1 x + \dots + q_m x^m \qquad q_i \in A$$

$$pq = \sum_{i=1}^{m} q_i x^i \left(p_0 + p_1 x^1 + \dots + p_n x^n\right)$$
$$= \underbrace{\sum_{i=1}^{m} \underbrace{\underbrace{q_i p_0 x^i}_{\in P} + \underbrace{q_i p_1 x^{1+i}}_{\in P} + \dots + \underbrace{q_i p_n x^{n+i}}_{\in P}}_{\in P}}_{\in P} \quad \checkmark$$

Ma allora in che relazione sono

$$\frac{A[x]}{P[x]} \quad e \quad (A/P)[x] \ ?$$

SONO ISOMORFI

$$\pi : A[x] \twoheadrightarrow (A/P)[x]$$
$$\sum_{i=0}^{n} a_i x^i \longmapsto \sum_{i=0}^{n} (a_i + P)\, x^i$$

$$\operatorname{Ker} \pi = \{ p \in A[x] : \pi(p) = 0 \}$$
$$= \{ p \in A[x] : \forall i : p_i + P = 0 + P \}$$
$$= \{ p \in A[x] : \forall i \ p_i \in P \} = P[x]$$

$$\Rightarrow \frac{A[x]}{\operatorname{Ker} \pi} = \frac{A[x]}{P[x]} \simeq \operatorname{Im} \pi = (A/P)[x]$$

Segue dunque che $P[x]$ è primo: infatti

essendo P primo A/P è dominio $\Rightarrow (A/P)[x]$ è dominio

ma $(A/P)[x] \simeq \frac{A[x]}{P[x]}$, dunque $P[x]$ è primo.

① INVERTIBILI IN $A[x]$

Sia $p = a_0 + a_1 x + \dots + a_n x^n \in A[x]$

p è invertibile $\iff a_0 \in A^\times$ e $a_i \in \mathcal{N}_A \ \forall i > 0$

ES: $p = 1 + 2x \in \mathbb{Z}/_{4\mathbb{Z}}[x]$ è invertibile e il suo inverso è $1 - 2x$: infatti

$$(1+2x)(1-2x) = 1 - 4x^2 = 1$$

DIM $\boxed{\Leftarrow}$ Posso supporre $a_0 = 1$. In effetti

$$p = a_0 \cdot \left(1 + \underbrace{(a_0^{-1} a_1)}_{\in \mathcal{N}_A} x + \dots + \underbrace{(a_0^{-1} a_n)}_{\in \mathcal{N}_A} x^n\right)$$

$\mathcal{N}_A \to$ perché $\mathcal{N}_A = \sqrt{0}$ è un ideale

Sia quindi $p = 1 + q$ in cui ogni coeff. di q è nilp.

Affermo che $\exists N > 0$ t.c. $q^N = 0$.

Sia in effetti $d := \deg q$ e sia $m > 0$ t.c. $q_i^m = 0 \ \forall i$.

Allora $N = m(d+1)$ è sufficiente:

$$q^N = \left(\sum_{i=1}^{d} q_i x^i\right)^N$$

$$= \underbrace{\sum_{\substack{0 \le m_i \le N \\ m_1 + \dots + m_d = N}}}_{} \binom{N}{m_1, \dots, m_n} \cdot (q_1 x)^{m_1} \cdots (q_n x^d)^{m_d}$$

$\hookrightarrow$ almeno un m_i è $\geq \frac{N}{d} > m$ $\Rightarrow$ almeno uno è $> m$

$\Rightarrow$ almeno un termine nel prodotto è 0

$$= 0.$$

$\ulcorner$ Più FACILE: $\mathcal{N}_A$ è un ideale: q_i nilp. $\Rightarrow q_i x^i$ nilp.

e quindi $\mathcal{N}_A[x]$ è ideale di $A[x]$

$\Rightarrow q = \sum q_i x^i$ è nilpotente, ovvero $\exists N$ t.c. $q^N = 0$. $\lrcorner$

L'inverso di $1+q$ è quindi

$$1 - q + q^2 - \dots + (-1)^{N-1} q^{N-1}$$

Infatti

$$(1+q)(1 - q + q^2 - \dots + (-1)^{N-1} q^{N-1})$$
$$= 1 + q^N = 1.$$

$\boxed{\Rightarrow}$ Sia $p \in A[x]^\times$. Per def di $A[x]^\times$ $\exists r \in A[x]$ t.c.

$$p \cdot r = 1.$$

Valutando in 0 (cioè confrontando i termini noti) si ha che

$$p(0) \cdot r(0) = a_0 \cdot r(0) = 1$$

cioè a_0 è invertibile in A.

Per ora che gli altri a_i $(i \geq 1)$ sono nilpotenti di A

basta oltre che appartengano ad ogni $P \trianglelefteq A$ primo.

Sia quindi P primo di A. L'uguaglianza $p \cdot r = 1$ in $A[x]$ implica che $\bar{p} \cdot \bar{r} \equiv \bar{1} \pmod{P[x]}$

cioè $\bar{p} \cdot \bar{r} = \bar{1}$ in $\dfrac{A[x]}{P[x]} \simeq (A/P)[x]$

OSS: Se R è dominio di int., in $R[x]$ vale che

$$\deg ab = \deg a + \deg b \quad (\text{con } a, b \neq 0)$$

$$a = a_n x^n + \dots + a_0 \quad , \quad b = b_m x^m + \dots + b_0$$

$$\Rightarrow \quad ab = \underbrace{(a_n b_m)}_{\neq 0 \text{ perché } R \text{ è dominio}} x^{n+m} + \dots$$

Dunque $R[x]$ è un dominio

In particolare A/P dominio $\Rightarrow (A/P)[x]$ dominio

$$\Rightarrow \quad \deg \bar{p} + \deg \bar{r} = \deg \bar{1} = 0$$

Ovvero $\bar{p}$ e $\bar{r}$ hanno solo il termine noto, cioè

$$\bar{p} = \bar{a}_0 + \underset{0}{\underset{\parallel}{\bar{a}_1}} x + \dots + \underset{0}{\underset{\parallel}{\bar{a}_n}} x^n$$

dunque $\bar{a}_i = \bar{0}$, cioè $a_i + P = 0 + P$, cioè $a_i \in P$. Dunque $a_i \in P \ \forall P$ primo

$$\Rightarrow \quad a_i \in \bigcap_{\substack{P \trianglelefteq A \\ \text{primo}}} P \quad \Rightarrow \quad a_i \text{ nilpotente.} \qquad \blacksquare$$

Localizzazione

$A = \mathbb{Z}$, $\quad P = (2) = \mathbb{Z}/2\mathbb{Z} \Rightarrow S = A \setminus P$

$S^{-1}A = \mathbb{Z}_{(2)} = \left\{ \frac{n}{d} : n \in \mathbb{Z},\ d \text{ dispari} \right\}$

① IDEALI DI $\mathbb{Z}_{(2)}$

Sono tutti della forma $S^{-1}I$ dove $I \trianglelefteq \mathbb{Z}$ t.c. $\underset{= (n)}{I} \cap S = \emptyset$

$(n) \cap S = \emptyset \Rightarrow n$ pari (sennò $n \in S$)

Ma a questo punto $(n) = \{ kn : k \in \mathbb{Z} \}$ e quindi tutti gli el. di (n) sono pari

$\Rightarrow (n) \cap S = \emptyset \iff n$ pari

OSS: voglio mostrare che se d è dispari
$S^{-1}(2^k \cdot d) = S^{-1}(2^k)$ come ideali in $\mathbb{Z}_{(2)}$

cioè $(2^k d)_{\mathbb{Z}_{(2)}} = (2^k)_{\mathbb{Z}_{(2)}}$.

Ma due ideali principali sono uguali se i generatori sono associati, e in questo caso lo sono perché d è invertibile e $d^{-1} = \frac{1}{d} \in \mathbb{Z}_{(2)}$

Al contrario $S^{-1}(2^a) = S^{-1}(2^b)$ se $2^{a-b} \in \mathbb{Z}_{(2)}$ ed è invertibile in $\mathbb{Z}_{(2)}$.

Per fare in modo che $2^{a-b} \in \mathbb{Z}_{(2)}$ è necessario che $a - b \geq 0$,
per fare in modo che sia invertibile deve essere $2^{b-a} \in \mathbb{Z}_{(2)}$,

cioè $b-a \geq 0$. Dunque $S^{-1}(2^a) = S^{-1}(2^b)$ se $a=b$.

CONCLUSIONE:

$$\{\text{ideali di } \mathbb{Z}_{(2)}\} = \{(0),\ (2^k)_{\mathbb{Z}_{(2)}} \text{ con } k \geq 0\}$$

Es. Numerici

① $A = \mathbb{F}_5[x]$, $I = (x^2+1)$, $J = (x^3-1)$

- $I + J = (x^2+1,\ x^3-1)$ ma $\mathbb{F}_5[x]$ è PID

$$= (x^2-4,\ x^3-1)$$

$$= ((x+2)(x-2),\ \underbrace{x^3-1}_{})$$

↳ ± 2 non sono radici

$$= 1$$

② $\mathbb{Q}[x,y]$: $I = (x-1,\ y-1)$, $J = (1-xy)$

* I max
* $J \subseteq I$
* J non è max

* I massimale: studiamo $\frac{\mathbb{Q}[x,y]}{I}$ e speriamo che sia un campo

SPERANZA:

$\pi : \mathbb{Q}[x,y] \twoheadrightarrow$ campo con $\operatorname{Ker}\pi = I$

A quel punto 1° t. di Iso : $\frac{\mathbb{Q}[x,y]}{I} \simeq$ campo

Prendiamo $\pi : \mathbb{Q}[x,y] \twoheadrightarrow \mathbb{Q}$

$p \longmapsto p(1,1)$

π è surgettiva, basta prendere i pol. costanti.

$\ker \pi \overset{?}{=} I$?? $\boxed{\supseteq}$ FACILE: $x-1 \in \ker \pi$

$y-1 \in \ker \pi$

$\Rightarrow (x-1, y-1) \subseteq \ker \pi$

$\boxed{\subseteq}$ Sia $p = \sum_{i,j=0}^{N} a_{ij} x^i y^j$. Supponiamo $p \in \ker \pi$.

Cerchiamo di mostrare che $p \equiv 0 \pmod I$

Ma modulo I si ha che $x \equiv 1$ e $y \equiv 1$

$$\Rightarrow \sum_{i,j=0}^{N} a_{ij} x^i y^j \equiv \sum_{i,j=0}^{N} a_{ij}$$

Ma per ipotesi $p \in \ker \pi$, dunque $p(1,1) = \sum a_{ij} = 0$,

e in particolare $\sum a_{ij} \equiv 0 \pmod I$, che è la tesi.

Dunque $\dfrac{\mathbb{Q}[x,y]}{I} \cong \mathbb{Q}$ e quindi I è max.

* $J \subseteq I$: basta mostrare che $J \subseteq \ker \pi$, cioè

$1-xy \in \ker \pi$ e questo è ovvio perché

$\pi(1-xy) = 1 - 1 \cdot 1 = 0$ ✓

* Basta mostrare che $J \neq I$: se fosse $J = I$ allora

$$(x-1, y-1) = (xy-1)$$

In particolare $x-1 \in (xy-1)$, cioè $x-1 = (xy-1) \cdot q$

e ciò è assurdo perché a sx non compare y.

BONUS Mostrare che J è primo

DIM Basta far vedere che $\dfrac{\mathbb{Q}[x,y]}{(xy-1)} \simeq$ dominio

IDEA: quozientare per $J=(xy-1)$ significa che in A/J: $\bar{x}\cdot\bar{y}=\bar{1}$, cioè che $\bar{x}$ è invertibile e il suo inverso è $\bar{y}$

$\rightsquigarrow$ Provo a dimostrare che

$$\frac{\mathbb{Q}[x,y]}{(xy-1)} \simeq S^{-1}\mathbb{Q}[x]$$

dove $S := \{x^i : i \geq 0\}$ $\begin{cases} 0 \notin S \\ 1 = x^0 \in S \\ x^k \cdot x^h = x^{k+h} \in S \end{cases}$

Mi serve una mappa

$$\pi : \mathbb{Q}[x,y] \twoheadrightarrow S^{-1}\mathbb{Q}[x]$$
$$p \longmapsto p(x, \tfrac{1}{x})$$

OMO: perché è valutazione

SURG: boh credo di sì mamma ⊛

Kernel: $\ker\pi \stackrel{?}{=} J$

$\boxed{J \subseteq \ker\pi}$: $\pi(xy-1) = x\cdot\frac{1}{x} - 1 = 1-1 = 0$ ✓

$\boxed{\ker\pi \subseteq J}$: sia $p \in \ker\pi$, cioè $\pi(p)=0$

e voglio mostrare che $p \in J$.

Se $p = \sum_{i,j=0}^{N} a_{ij}x^iy^j \implies$

$$\overline{p} \equiv \sum a_{ij} \overline{x^i}\,\overline{y^j} \equiv \sum a_{ij} \overline{x^i}\,\overline{\frac{1}{x^j}} \equiv \sum a_{ij}\, \overline{x^{i-j}} \qquad (\mathrm{mod}\ J)$$

L'hp. $\pi(p) = 0$ ci dice che

$$\pi\left(\sum a_{ij} x^i y^j\right) = \sum a_{ij}\, x^{i-j} = 0$$

$$\Rightarrow \overline{p} \equiv \overline{0} \quad (\mathrm{mod}\ J) \quad \text{cioè} \quad p \in J.$$

Dunque $\dfrac{\mathbb{Q}[x,y]}{(xy-1)} \simeq S^{-1}\mathbb{Q}[x]$ che è un dominio in quanto localizzazione di un dominio, e quindi $(xy-1) = J$ è primo. ∎

(*) Rettifica: è surg.

Infatti un generico elemento di $S^{-1}\mathbb{Q}[x]$ è $\left[\dfrac{p(x)}{x^k}\right]$ dove $p(x) \in \mathbb{Q}[x]$, e ad esempio questo el. è immagine di

$$\mathbb{Q}[x,y] \ni P(x,y) = p(x) \cdot y^k$$