



Funzioni polinomiali su anelli locali

Federico Volpe





Indice

1 Gli ideali $\mathcal{Z}(S, J)$: definizioni, primi risultati e caratterizzazioni

► Gli ideali $\mathcal{Z}(S, J)$: definizioni, primi risultati e caratterizzazioni

► $\mathcal{Z}(R)$: decomposizione primaria e legame con $\mathcal{Z}(\mathfrak{m})$

► Il caso locale finito con ideale massimale principale



Gli ideali $\mathcal{Z}(S, J)$: definizioni

¹ Gli ideali $\mathcal{Z}(S, J)$: definizioni, primi risultati e caratterizzazioni

- Ad un polinomio $f \in R[x]$ associamo la funzione $\phi(f) : R \rightarrow R$ indotta dal polinomio.
- Dato R un qualsiasi anello, $S \subseteq R$ un sottoinsieme e $J \subseteq I$ un ideale, definiamo l'ideale $\mathcal{Z}(S, J) \subseteq R[x]$. Questo è l'ideale dei polinomi f tali che $f(S) \subseteq J$.
- Studiamo in particolare, nel caso di $(R, \mathfrak{m})$ locale noetheriano, gli ideali $\mathcal{Z}(R)$ e $\mathcal{Z}(\mathfrak{m})$ dei polinomi che inducono la funzione nulla su R e su $\mathfrak{m}$ rispettivamente.



Un problema non banale

1 Gli ideali $\mathcal{Z}(S, J)$: definizioni, primi risultati e caratterizzazioni

Anche solo nel caso “semplice” di $R = \mathbb{Z}/p^n\mathbb{Z}$, $\mathfrak{m} = pR$, il problema è di risoluzione tutt'altro che banale.

- Possiamo notare facilmente che $(x, p)^n \subseteq \mathcal{Z}(pR)$, per ogni n . Dimosteremo che questo contenimento è un'eguaglianza se $n \leq p$.
- Ma per $n = p + 1$, abbiamo ad esempio anche $x^p - p^{p-1}x \in \mathcal{Z}(pR)$.
- Per $n = 1 + p + p^2$, abbiamo $(x^p - p^{p-1}x)^p - p^{p^2-1}(x^p - x^{p-1}x) \in \mathcal{Z}(pR)$.

Alla fine della trattazione determineremo un insieme di generatori di $\mathcal{Z}(p\mathbb{Z}/p^n\mathbb{Z})$ e $\mathcal{Z}(\mathbb{Z}/p^n\mathbb{Z})$, per ogni n .



Risultati generali e π -polinomi

1 Gli ideali $\mathcal{Z}(S, J)$: definizioni, primi risultati e caratterizzazioni

Mostriamo subito alcune proprietà degli ideali $\mathcal{Z}(S, J)$ valide per qualsiasi R . Ad esempio si osserva che gli ideali $\mathcal{Z}(S, J)$ si comportano “bene” rispetto al passaggio al quoziente.

Lemma

Dati $I \subseteq J \subset R$ due ideali, ed $S \subseteq R$ un sottoinsieme, si ha che $\overline{\mathcal{Z}(S, J)} = \mathcal{Z}(\bar{S}, \bar{J})$, dove $\overline{\mathcal{Z}(S, J)} = \pi_{I[x]}(\mathcal{Z}(S, J)) \subseteq (R/I)[x]$ e con $\bar{S}, \bar{J}$ denotiamo $\pi_I(S), \pi_I(J)$ rispettivamente.

Definiamo inoltre, nel caso locale, i π -polinomi, che forniranno in seguito un collegamento fra $\mathcal{Z}(R)$ e $\mathcal{Z}(\mathfrak{m})$.

Definizione

Dato un insieme di rappresentanti $c_1, \dots, c_q$ dei laterali di $\mathfrak{m}$, i π -polinomi sono gli elementi di $R[x]$ della forma $\prod_{c_i \in C} (x - c_i)$.



Trivialità e regolarità di $\mathcal{Z}(R)$ e $\mathcal{Z}(\mathfrak{m})$ nel caso locale

1 Gli ideali $\mathcal{Z}(S, J)$: definizioni, primi risultati e caratterizzazioni

Nel caso in cui $R, \mathfrak{m}$ sia un anello locale, mostriamo alcune caratterizzazioni generali, ad esempio

Teorema

Sia $(R, \mathfrak{m})$ un anello locale noetheriano. Allora si ha:

1. $\mathcal{Z}(\mathfrak{m}) \neq (0) \iff \text{depth}(R) = 0$;
2. $\mathcal{Z}(R) \neq (0) \iff \text{depth}(R) = 0$ e $\bar{R} = R/\mathfrak{m}$ è finito.

Teorema

Sia $(R, \mathfrak{m})$ un anello locale noetheriano. Allora si ha:

1. $\mathcal{Z}(\mathfrak{m})$ contiene elementi regolari di $R[x] \iff R$ è artiniano;
2. $\mathcal{Z}(R)$ contiene elementi regolari di $R[x] \iff R$ è finito.



Indice

2 $\mathcal{Z}(R)$: decomposizione primaria e legame con $\mathcal{Z}(\mathfrak{m})$

- ▶ Gli ideali $\mathcal{Z}(S, J)$: definizioni, primi risultati e caratterizzazioni
- ▶ $\mathcal{Z}(R)$: decomposizione primaria e legame con $\mathcal{Z}(\mathfrak{m})$
- ▶ Il caso locale finito con ideale massimale principale



Una decomposizione primaria minimale

$\mathcal{Z}(R)$: decomposizione primaria e legame con $\mathcal{Z}(\mathfrak{m})$

Un primo collegamento fra l'ideale $\mathcal{Z}(R)$ e l'ideale $\mathcal{Z}(\mathfrak{m})$ è dato dal seguente teorema, che ci fornisce una decomposizione primaria minimale di $\mathcal{Z}(R)$ “in funzione” di $\mathcal{Z}(\mathfrak{m})$.

Teorema

Sia $(R, \mathfrak{m})$ un anello locale finito e $c_1, \dots, c_q$ un insieme di rappresentanti per le classi laterali di $\mathfrak{m}$. Allora $\bigcap_{i=1}^q \mathcal{Z}(c_i + \mathfrak{m})$ è una decomposizione primaria minimale di $\mathcal{Z}(R)$.



Da $\mathcal{Z}(\mathfrak{m})$ a $\mathcal{Z}(R)$, passando per i π -polinomi

$\mathcal{Z}(R)$: decomposizione primaria e legame con $\mathcal{Z}(\mathfrak{m})$

Dato un π -polinomio $f \in R[x]$, $f \in \mathcal{Z}(R, \mathfrak{m})$. Quindi, per ogni $g \in \mathcal{Z}(\mathfrak{m})$, $g \circ f \in \mathcal{Z}(R)$. Il seguente teorema ci fornisce, sotto un'opportuna ipotesi di henselianità, una sorta di viceversa:

Teorema

Siano $(R, \mathfrak{m})$ un anello locale henseliano con $|R/\mathfrak{m}| = q$ e $f(x) \in R[x]$ un π -polinomio. Allora se $\mathcal{Z}(\mathfrak{m}) = (F_1(x), \dots, F_n(x))$, si ha che $\mathcal{Z}(R) = (F_1(f(x)), \dots, F_n(f(x)))$.

Possiamo quindi ridurci a studiare $\mathcal{Z}(\mathfrak{m})$, per poi precomporre un suo insieme di generatori con un π -polinomio ed ottenere dei generatori per $\mathcal{Z}(R)$.



Indice

3 Il caso locale finito con ideale massimale principale

- ▶ Gli ideali $\mathcal{Z}(S, J)$: definizioni, primi risultati e caratterizzazioni
- ▶ $\mathcal{Z}(R)$: decomposizione primaria e legame con $\mathcal{Z}(\mathfrak{m})$
- ▶ Il caso locale finito con ideale massimale principale



Le q -espansioni

3 Il caso locale finito con ideale massimale principale

Vogliamo descrivere, nel caso in cui R sia locale finito con ideale $\mathfrak{m} = (m)$ massimale principale, $\mathcal{Z}(R)$ in termini di generatori. Questo è il caso, ad esempio, di $R = \mathbb{Z}/p^n\mathbb{Z}$. A tale scopo poniamo $q = R/\mathfrak{m}$ ed introduciamo il concetto di q -espansione di un intero n :

Definizione

Dato un intero $q \geq 2$, sia, per ogni $i \geq 0$, $Q_i = \frac{q^i - 1}{q - 1} = \sum_{j=0}^{i-1} q^j$.

Definiamo l'espressione $n = \sum_{i=1}^t \mu_i Q_i$ con $t \geq 1$, $0 \leq \mu_i \leq q$ per ogni i e $\mu_i = 0$ se $\mu_j = q$ per qualche $j > i$ una q -espansione di n .

Si mostra l'esistenza e l'unicità della q -espansione per ogni intero n .



Numeri q -liberi e le funzioni D ed E

3 Il caso locale finito con ideale massimale principale

Mediante le q -espansioni, definiamo l'insieme degli interi q -liberi $\mathcal{F}_q$ e le funzioni D ed E .

Definizione

L'insieme degli interi q -liberi $\mathcal{F}_q$ è l'insieme degli interi nella cui q -espansione compaiono solo coefficienti $< q$.

Definizione

Dato un intero n con q -espansione $\sum_{i=0}^{t_n} \mu_i(n)Q_i$, si ha $D(n) = \sum_{i=1}^{t_n} q^{i-1} \mu_i(n)$.

Definizione

Definiamo la funzione E come l'inversa della restrizione $D|_{\mathcal{F}_q} : \mathcal{F}_q \rightarrow \mathbb{N}$.



I polinomi L_n

3 Il caso locale finito con ideale massimale principale

Mediante queste funzioni, definiamo a loro volta varie classi di polinomi, nel caso di un anello locale con ideale massimale $\mathfrak{m} = (m)$ di indice q . In particolare si mostra che $L_n \in \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^n)$.

Definizione

Per ogni intero $n \geq 0$ definiamo $\pi_n(x) = x^q - m^{q^n-1}x \in R[x]$.

Definizione

Definiamo ricorsivamente $T_n(x) = x$ se $n = 1$, $T_n(x) = \pi_{n-1}(T_{n-1}(x))$ se $n > 1$.

Definizione

Per ogni intero $n \geq 0$ definiamo $L_n = \prod_{i=1}^{\infty} T_i(x)^{\mu_i(n)} \in R[x]$.



Gli ideali A_n e B_n

3 Il caso locale finito con ideale massimale principale

Tramite il polinomi L_n , definiamo gli ideali A_n e B_n .

Definizione

$$B_n = (\{m^{n-i}L_i \mid 0 \leq i \leq n\})$$

$$A_n = (\{m^{n-E(i)}L_{E(i)} \mid 0 \leq i \leq D(n) - 1\}) + (L_{E(D(n))}).$$

Teorema

In un anello locale con ideale massimale principale di indice finito, $A_n = B_n \subseteq \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^n)$.

Lemma

Si ha che $(x, \mathfrak{m})A_n \subseteq A_{n+1}$, e che $A_n/(\mathcal{Z}(\mathfrak{m}, \mathfrak{m}^{n+1}) \cap A_n)$ ammette una naturale struttura di $\bar{R}$ -spazio vettoriale.



Il caso DVR henseliano

3 Il caso locale finito con ideale massimale principale

Nel caso in cui R sia un DVR henseliano, si mostra il seguente risultato di (quasi) lineare indipendenza delle proiezioni su $(\mathcal{Z}(\mathfrak{m}, \mathfrak{m}^{n+1}) \cap A_n)$ degli elementi di A_n .

Teorema

$$\text{Poniamo } S_n = \begin{cases} \{m^{n-E(i)}L_{E(i)} \mid 0 \leq i \leq D(n)\} & \text{se } \iota(n) = 0, \\ \{m^{n-E(i)}L_{E(i)} \mid 0 \leq i \leq D(n) - 1\} & \text{altrimenti.} \end{cases}$$

Allora $\overline{S_n}$ è un sottoinsieme di $A_n / (A_n \cap \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^{n+1}))$ linearmente indipendente su $\overline{R}$.

Questo risultato a sua volta ci permette di dimostrare un fondamentale teorema:

Teorema

Se R è un DVR henseliano, si ha che $A_n = B_n = \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^n)$.



Da DVR henseliano al caso finito con ideale principale

3 Il caso locale finito con ideale massimale principale

Usando il Teorema di Struttura di Cohen, otteniamo il seguente risultato:

Lemma

Sia R un anello locale finito con ideale massimale principale $\mathfrak{m} = (m)$ e indice di nilpotenza n . Sia $q = |R/\mathfrak{m}|$ la cardinalità del suo campo residuo. Allora esistono un DVR completo T con ideale massimale (t) tale che $|T/(t)| = q$ ed un isomorfismo $\psi : T/(t^n) \rightarrow R$ tale che $\psi(\bar{t}) = m$.

Quindi $\mathcal{Z}(\mathfrak{m}) \cong \mathcal{Z}((t)/(t^n)) \cong \overline{\mathcal{Z}((t), (t)^n)}$ tramite isomorfismi che “conservano” A_n . Otteniamo dunque il principale risultato di questa parte di trattazione:

Teorema

Per un anello locale finito con ideale massimale principale con indice di nilpotenza n si ha

$$\mathcal{Z}(\mathfrak{m}) = A_n.$$



Risultati finali

3 Il caso locale finito con ideale massimale principale

Da $\mathcal{Z}(\mathfrak{m})$ è ora semplice determinare $\mathcal{Z}(R)$.

Teorema

Sia R un anello locale finito con ideale massimale principale $\mathfrak{m} = (m)$ avente indice di nilpotenza n . Sia $f(x) \in R[x]$ un qualsiasi π -polinomio. Sia inoltre $\{c_1, \dots, c_q\}$ un insieme di rappresentanti per le classi laterali di $\mathfrak{m}$ e per ogni i sia $\psi_i : R[x] \rightarrow R[x]$ l'automorfismo di anelli tale che $\psi_i(x) = x - c_i$. Allora si ha che:

- $\mathcal{Z}(\mathfrak{m}) = A_n$.
- $\mathcal{Z}(R) = (\{m^{n-E(i)} L_{E(i)}(f(x)) \mid 0 \leq i \leq D(n) - 1\}) + (L_{E(D(n))}(f(x)))$.
- $\mathcal{Z}(R) = (\{m^{n-i} L_i(f(x)) \mid 0 \leq i \leq n\})$.
- $\bigcap_{i=1}^q \psi_i(A_n)$ è una decomposizione primaria minimale di $\mathcal{Z}(R)$.



Perché le q -espansioni?

3 Il caso locale finito con ideale massimale principale

Supponiamo di costruire degli ideali B_n^{dec} , analoghi ai B_n ma utilizzando la normale espansione in base q al posto delle q -espansioni nella costruzione degli L_i . Per $R = \mathbb{Z}/p^{p+1}\mathbb{Z}$ si avrebbe:

$$B_n^{dec} = (pT_1, \dots, p^2T_1^{p-1}, pT_2, T_1T_2) = p^2(p, x)^{p-2} + (p, x)(x^p - p^{p-1}x) \not\equiv x^p - p^{p-1}x,$$

$$\text{ma } \mathcal{Z}(p\mathbb{Z}/p^{p+1}\mathbb{Z}) = B_n = (pT_1, \dots, p^2T_1^{p-1}, pT_1^p, T_2) = p(x, p)^p + (x^p - p^{p-1}x).$$



Grazie per l'attenzione!