UNIVERSITÀ DI PISA

DIPARTIMENTO DI MATEMATICA

Laurea Triennale in Matematica

Funzioni polinomiali su anelli locali

Relatore:

Prof. Andrea Bandini

Candidato:

Federico Volpe

ANNO ACCADEMICO 2024/2025

Alla mia famiglia e a Daniele, Giulia, Gabriel Antonio, Valerio, Luca e Sara, per i quali non basterebbe alcun ringraziamento che possa entrare in questo spazio.

Indice

Introduzione 4

1 Gli ideali $\mathcal{Z}(S, J)$: definizioni, primi risultati e caratterizzazioni **6**
1.1 Gli ideali $\mathcal{Z}(S, J)$ 6
1.2 π-polinomi 10
1.3 Trivialità e regolarità di $\mathcal{Z}(R)$ e $\mathcal{Z}(\mathfrak{m})$ nel caso locale 11
1.4 Trivialità di $\mathcal{Z}(R)$ nel caso generale 15

2 $\mathcal{Z}(R)$: decomposizione primaria e legame con $\mathcal{Z}(\mathfrak{m})$ **18**
2.1 π-polinomi e decomposizione primaria 18
2.2 Casi in cui $\mathcal{Z}(R)$ e $\mathcal{Z}(\mathfrak{m})$ sono principali 22
2.3 Da $\mathcal{Z}(\mathfrak{m})$ a $\mathcal{Z}(R)$ 25

3 Il caso locale finito con ideale massimale principale **28**
3.1 q-espansioni e funzioni aritmetiche collegate 28
3.2 I polinomi $L_n(x)$ e $\pi_n(x)$, gli ideali B_n e A_n 37
3.3 Il caso DVR henseliano 44
3.4 Da DVR al caso locale ad ideali principali 51

Bibliografia **58**

Introduzione

Scopo principale di questa tesi è lo studio dei polinomi che inducono la funzione nulla su anelli locali noetheriani. L'approccio seguito riprende quello di Rogers e Wickham, sviluppato in [5] e [6].

Sia $M(R,R)$ l'anello delle funzioni dall'anello R in sé stesso, e definiamo l'omomorfismo di anelli $\phi^R : R[x] \to M(R,R)$ che associa ad un polinomio $f \in R[x]$ la funzione su R da lui indotta: i polinomi oggetto del nostro studio sono il nucleo di tale mappa, $\ker(\phi^R)$, che denotiamo con $\mathcal{Z}(R)$.

Nel Capitolo 1 introduciamo, più generalmente, gli ideali $\mathcal{Z}(S,J)$ dei polinomi tali che $f(S) \subseteq J$, e procediamo ad enunciare e dimostrare alcuni lemmi generali su quest'ultimi, validi per qualsiasi R. In particolare lo studio, per R locale, di $\mathcal{Z}(\mathfrak{m},0) := \mathcal{Z}(\mathfrak{m})$ sarà di fondamentale importanza per poter poi determinare $\mathcal{Z}(R)$.

Dopo aver introdotto il concetto di π-polinomio, studiamo $\mathcal{Z}(R)$ e $\mathcal{Z}(\mathfrak{m})$ nel caso locale noetheriano, arrivando a dare criteri precisi per quando $\mathcal{Z}(R)$ e $\mathcal{Z}(\mathfrak{m})$ sono non banali e per quando contengono elementi regolari. In particolare dimostreremo il seguente:

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

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

Concludiamo il primo capitolo estendendo il criterio per la banalità di $\mathcal{Z}(R)$ tramite l'uso di un risultato locale-globale che stabilisce un'equivalenza fra la banalità di $\mathcal{Z}(S)$ e quella degli ideali $\mathcal{Z}(i_{\mathfrak{p}}(S))$, con $i_{\mathfrak{p}}$ le mappe canoniche $R \to R_{\mathfrak{p}}$ al variare di $\mathfrak{p}$ fra i primi associati di R.

Il secondo capitolo invece si concentra, sempre nel caso locale e noetheriano, sul legame fra $\mathcal{Z}(R)$ e $\mathcal{Z}(\mathfrak{m})$.

La Sezione 2.1 fornisce infatti, sempre nel caso di R locale noetheriano, una decomposizione primaria minimale di $\mathcal{Z}(R)$, le cui componenti primarie si dimostrano essere $\mathcal{Z}(\mathfrak{m}+c_i)$, per un qualsiasi insieme $c_1,\dots,c_q$ di rappresentanti delle classi laterali di $\mathfrak{m}$. In seguito uno studio più approfondito dei π-polinomi consente di caratterizzare gli anelli locali con $\mathcal{Z}(\mathfrak{m})$ o $\mathcal{Z}(R)$ principali o generati da elementi regolari.

Nella Sezione 2.3 si mostra come il legame fra gli ideali $\mathcal{Z}(\mathfrak{m})$ e $\mathcal{Z}(R)$, nel caso degli anelli locali noetheriani henseliani, passi proprio per i π-polinomi introdotti nel Capitolo 1. Si osserva quasi immediatamente che, componendo un quasiasi π-polinomio con un elemento di $\mathcal{Z}(\mathfrak{m})$, si ottiene un elemento di $\mathcal{Z}(R)$. Sotto appropriate condizioni di henselianità su R, si dimostra il seguente:

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

Il terzo capitolo ha infine l'obiettivo, seguendo l'approccio di [6], di arrivare a fornire, nel caso in cui R sia un anello locale finito e con ideale massimale principale $\mathfrak{m} = (m)$, una descrizione esplicita di $\mathcal{Z}(\mathfrak{m})$ in termini di generatori. Questo, assieme ai risultati mostrati nelle Sezioni 2.1 e 2.3, permette di descrivere in tal caso l'ideale $\mathcal{Z}(R)$, sia attraverso un insieme di generatori che tramite una decomposizione primaria.

Nella Sezione 3.1 introduciamo il concetto di q-espansione di un numero naturale n e le funzioni aritmetiche D ed E definite sulle q-espansioni. La q-espansione differisce dalla classica espansione in base q e, tramite le proprietà delle funzioni D ed E, servirà a definire esponenti ed indici per i generatori di $\mathcal{Z}(\mathfrak{m})$.

Nella Sezione 3.2 vengono introdotte varie famiglie di polinomi π_n, T_n ed L_n nel contesto generale di un anello locale con ideale massimale principale $\mathfrak{m} = (m)$ e campo residuo finito. Tramite tali polinomi vengono definite due famiglie di ideali:

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

e

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

La sezione si conclude mostrando che $A_n = B_n$, per ogni n.

Nel caso in cui R sia un anello di valutazione discreta henseliano si dimostra l'eguaglianza fra A_n, B_n e $\mathcal{Z}(\mathfrak{m}, \mathfrak{m}^n)$, l'ideale dei polinomi che mandano l'ideale massimale nella sua n-esima potenza.

Nella Sezione 3.4 infine ci serviremo del Teorema di Struttura di Cohen nel caso in cui R abbia caratteristica finita e di alcuni semplici lemmi sul comportamento degli ideali $\mathcal{Z}(S, J)$ e delle famiglie di polinomi e di ideali in precedenza definiti rispetto ad isomorfismi e passaggi al quoziente, per arrivare a dare una descrizione esplicita di $\mathcal{Z}(\mathfrak{m})$ e $\mathcal{Z}(R)$:

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 $\{c_1, \ldots, c_q\}$ un insieme di rappresentanti per le classi laterali di $\mathfrak{m}$ e per ogni i sia $\psi_i : R[x] \to R[x]$ l'automorfismo di anelli tale che $\psi_i(x) = x - c_i$.*
Allora si ha che:

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

Capitolo 1

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

Scopo di questo capitolo è la definizione ed un primo studio degli ideali $\mathcal{Z}(S, J)$ dei polinomi che inducono una funzione $f : R \to R$ tale che $f(S) \subseteq J$, dove $S \subseteq R$ è un sottoinsieme e $J \subseteq R$ un ideale. Gli ideali $\mathcal{Z}(S, J)$ saranno l'oggetto centrale di tutta la trattazione. Dopo averli definiti ed averne enunciato e dimostrato alcune proprietà valide per qualunque anello R, ci concentreremo sul caso in cui R sia locale e noetheriano. Nella Sezione 1.2 introdurremo quindi il concetto di π-polinomio, fondamentale per tutto il resto della trattazione, per poi concentrarci sullo studio degli ideali $\mathcal{Z}(R)$ e $\mathcal{Z}(\mathfrak{m})$, composti rispettivamente dai polinomi che inducono la funzione nulla sull'intero anello R e sul suo ideale massimale. In particolare forniremo caratterizzazioni degli anelli noetheriani locali per cui $\mathcal{Z}(R)$ o $\mathcal{Z}(\mathfrak{m})$ sono banali o contengono elementi regolari. Concluderà il capitolo un excursus sul caso noetheriano generale, con l'uso di una sorta di principio locale-globale per ottenere una caratterizzazione degli anelli R noetheriani (ma non necessariamente locali) con ideale $\mathcal{Z}(R)$ banale.

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

In tutto questo testo indichiamo sempre col termine anello un anello commutativo con unità. Cominciamo definendo l'anello delle funzioni da un insieme S a valori in R.

Definizione 1.1.1. *Sia R un anello e S un insieme. Si denota con $M(S, R) = \{f : S \to R\}$ l'anello delle funzioni da un insieme S a valori in R con le operazioni date dalla somma e dal prodotto puntuale, ossia tali che*

$$\forall s \in S \quad (f + g)(s) = f(s) + g(s), \quad (f \cdot g)(s) = f(s)g(s).$$

Definiamo ora due classi di funtori, strettamente collegati alla precedente definizione, $M(-, R)$ e $M(S, -)$.

Definizione 1.1.2. *Sia R un anello, allora il funtore controvariante $M(-, R) : \mathbf{Set} \to \mathbf{Ring}$ è definito in modo che per ogni insieme S si abbia $M(-, R)(S) = M(S, R)$ e per ogni mappa fra insiemi $f : S \to T$ si abbia*

$$M(-, R)(f) : M(T, R) \to M(S, R), \quad \phi \mapsto \phi \circ f.$$

Definizione 1.1.3. *Sia R un anello, allora il funtore covariante $M(S, -) : \mathbf{Ring} \to \mathbf{Ring}$ è definito in modo che per ogni anello R si abbia $M(S, -)(R) = M(S, R)$ e per ogni omomorfismo di anelli $f : A \to B$ si abbia*

$$M(S, -)(f) : M(S, A) \to M(S, B), \quad \phi \mapsto f \circ \phi.$$

Definiamo infine un terzo funtore $-[x] : \mathbf{Ring} \to \mathbf{Ring}$, che verrà usato più volte nel corso della trattazione.

Definizione 1.1.4. *Sia R un anello, allora il funtore covariante $-[x] : \mathbf{Ring} \to \mathbf{Ring}$ è definito in modo che per ogni anello R si abbia $-[x](R) = R[x]$ e per $f : A \to B$ omomorfismo di anelli si abbia*

$$-[x](f) : A[x] \to B[x], \quad \sum_{i=0}^{k} a_i x^i \mapsto \sum_{i=0}^{k} f(a_i) x^i.$$

Definiamo ora la mappa ϕ_R, lo studio del cui nucleo sarà l'argomento fondamentale di questa trattazione.

Definizione 1.1.5. *Dato un anello R, denotiamo con ϕ_R la mappa*

$$\phi_R : R[x] \to M(R, R)$$

che associa ad ogni polinomio in $R[x]$ la funzione che esso induce su R ovvero la mappa tale che

$$\phi_R : p(x) \mapsto (f : r \mapsto p(r)).$$

Questa mappa è ovviamente omomorfismo di anelli.

Se non ci saranno ambiguità ometteremo il pedice, scrivendo direttamente ϕ.
Questo ci permette finalmente di definire $\mathcal{Z}(R)$.

Definizione 1.1.6. *Dato un anello R definiamo $\mathcal{Z}(R) := \ker(\phi_R)$.*

Diamo ora una definizione più generale, quella di $\mathcal{Z}(S, J)$, tramite l'uso dei funtori definiti in precedenza. Siano $S \subseteq R$ un sottinsieme di R, $J \subseteq R$ un ideale. Denotiamo con $i_S : S \to R$ e $\pi_J : R \to R/J$ rispettivamente l'inclusione di S in R e la proiezione canonica di R su R/J. Poniamo

$$i_S^* := M(-, R)(i_S) : M(R, R) \to M(S, R)$$

e

$$\pi_{J*} := M(S, -)(\pi_J) : M(S, R) \to M(S, R/J).$$

Definiamo ora $\mathcal{Z}(S, J)$ come segue.

Definizione 1.1.7. *Dato un anello R, $S \subseteq R$ un suo sottoinsieme, $J \subseteq R$ un suo ideale, π_{J*}, i_S^* come sopra, definiamo*

$$\mathcal{Z}(S, J) := \phi_R^{-1}(\ker(\pi_{J*} \circ i_S^*)).$$

Denotiamo inoltre $\mathcal{Z}(S, 0)$ con $\mathcal{Z}(S)$.

L'insieme $\mathcal{Z}(S, J)$ è ovviamente un ideale di $R[x]$, in quanto controimmagine tramite l'omomorfismo ϕ_R del nucleo di un omomorfismo (tale a sua volta in quanto composizione di omomorfismi). Diamo subito una caratterizzazione più concreta di $\mathcal{Z}(S, J)$, che sarà cruciale nella nostra trattazione.

Lemma 1.1.8. *Siano R un anello ed S, J un sottoinsieme ed un ideale di R rispettivamente. Allora $\mathcal{Z}(S,J)$ è esattamente l'insieme dei polinomi che inducono (attraverso ϕ) funzioni f con $f(S) \subset J$. In particolare tale insieme è un ideale di $R[x]$.*

Dimostrazione. Basta osservare che

$$\begin{aligned} f(S) \subset J &\iff \pi_J \circ \phi(f)|_S = 0 \\ &\iff \pi_J \circ \phi(f) \circ i_S = \pi_{J*}(i_S^*(\phi(f))) = 0 \\ &\iff f \in \phi^{-1}(\ker(\pi_{J*} \circ i_S^*)). \end{aligned}$$ □

Enunciamo e dimostriamo ora alcuni semplici lemmi su $\mathcal{Z}(S,J)$ che verranno più volte utilizzati nel corso della trattazione. Il primo di questi concerne il comportamento rispetto all'unione e all'intersezione di sottoinsiemi ed ideali rispettivamente.

Lemma 1.1.9. *Sia $\{S_\alpha \subseteq R \mid \alpha \in \mathcal{I}\}$ un insieme di sottoinsiemi di un anello R e $\{J_\beta \subseteq R \text{ ideale} \mid \beta \in \mathcal{J}\}$ un insieme di ideali di R. Allora*

$$\mathcal{Z}(\bigcup_{\alpha\in\mathcal{I}} S_\alpha, \bigcap_{\beta\in\mathcal{J}} J_\beta) = \bigcap_{\alpha\in\mathcal{I}} \bigcap_{\beta\in\mathcal{J}} \mathcal{Z}(S_\alpha, J_\beta).$$

Dimostrazione. Basta osservare che

$$\begin{aligned} f \in \mathcal{Z}\left(\bigcup_{\alpha\in\mathcal{I}} S_\alpha, \bigcap_{\beta\in\mathcal{J}} J_\beta\right) &\iff f(s) \in \bigcap_{\beta\in\mathcal{J}} J_\beta \quad \forall s \in \bigcup_{\alpha\in\mathcal{I}} S_\alpha \\ &\iff \forall \alpha \in \mathcal{I}, \forall \beta \in \mathcal{J}, \forall s \in S_\alpha \text{ si ha } f(s) \in J_\beta \\ &\iff \forall \alpha \in \mathcal{I}, \forall \beta \in \mathcal{J}, f \in \mathcal{Z}(S_\alpha, J_\beta) \\ &\iff f \in \bigcap_{\alpha\in\mathcal{I}} \bigcap_{\beta\in\mathcal{J}} \mathcal{Z}(S_\alpha, J_\beta). \end{aligned}$$ □

Si ha allora, come d'altronde era immediato verificare utilizzando la fondamentale caratterizzazione mostrata nel Lemma 1.1.8, che per due insiemi $S \subseteq T$ ed un ideale J

$$\mathcal{Z}(T,J) = \mathcal{Z}(S \cup T, J) = \mathcal{Z}(S,J) \cap \mathcal{Z}(T,J) \subseteq \mathcal{Z}(S,J).$$

Analogamente, presi $I \subseteq J$ due ideali ed S un sottoinsieme,

$$\mathcal{Z}(S,I) = \mathcal{Z}(S, I \cap J) = \mathcal{Z}(S,J) \cap \mathcal{Z}(S,I) \subseteq \mathcal{Z}(S,J).$$

Il secondo lemma riguarda invece il comportamento di $\mathcal{Z}(S,J)$ rispetto all'operazione di passaggio al quoziente per un ideale I.

Lemma 1.1.10. *Siano $I, J \subset R$ due ideali, $\pi_I : R \to R/I$ e $\pi_{I[x]} : R[x] \to (R/I)[x]$ le proiezioni al quoziente e $S \subset R$ un sottoinsieme. Allora,*

$$\overline{\mathcal{Z}(S, J+I)} = \mathcal{Z}(\overline{S}, \overline{J}),$$

dove $\overline{\mathcal{Z}(S,J)} = \pi_{I[x]}(\mathcal{Z}(S,J)) \subset (R/I)[x]$ *e con* $\overline{S}, \overline{J}$ *denotiamo* $\pi_I(S), \pi_I(J)$ *rispettivamente. In particolare, se* $I \subseteq J$*, si ha che*

$$\overline{\mathcal{Z}(S,J+I)} = \overline{\mathcal{Z}(S,J)} = \mathcal{Z}(\overline{S},\overline{J})$$

ed in generale

$$\overline{\mathcal{Z}(S,J)} \subseteq \overline{\mathcal{Z}(S,J+I)} = \mathcal{Z}(\overline{S},\overline{J}).$$

Dimostrazione. Poniamo $\pi_{I[x]}(p) = \overline{p}$, $\pi_I(s) = \overline{s}$ e $\pi_I(p(s)) = \overline{p(s)}$. Allora si ha per definizione che $\overline{p} \in \mathcal{Z}(\overline{S},\overline{J}) \iff \forall \overline{s} \in \overline{S},\ \overline{p}(\overline{s}) \in \overline{J}$.

Quindi si ha che

$$\begin{aligned}
\overline{p} \in \mathcal{Z}(\overline{S},\overline{J}) &\iff \forall s \in S,\ \overline{p(s)} \in \overline{J} = \overline{J+I} \\
&\iff \forall s \in S,\ p(s) \in J+I \\
&\iff p \in \mathcal{Z}(S, J+I).
\end{aligned}$$

come voluto. □

Mostriamo un ulteriore lemma, che useremo più volte nel corso della trattazione. Si tratta di una generalizzazione al caso di un anello R del noto Teorema di Ruffini, che fornisce anche una descrizione di $\mathcal{Z}(S)$ per S insieme finito con una particolare proprietà. Denotiamo con $D(R)$ i divisori di zero dell'anello R.

Lemma 1.1.11. *Siano* R *un anello,* $f \in R[x]$ *un polinomio,* $c_1, \dots, c_n \in R$ *distinti tali che* $c_i - c_j \notin D(R)$ *per ogni* $i \neq j$ *e* $f(c_i) = 0$ *per ogni* i*. Allora* $g := \prod_{i=1}^{n}(x - c_i) \mid f$ *in* $R[x]$*. In particolare* $\mathcal{Z}(\{c_1, \dots, c_n\}) = (g)$*.*

Dimostrazione. Si procede per induzione su n.

`Caso base, n=1.` Sia $c := c_1$, $f = \sum_{i=0}^{k} a_i x^i$. Allora abbiamo che

$$\begin{aligned}
f(c) = 0 &\iff \sum_{i=0}^{k} a_i c^i = 0 \\
&\iff f = f - f(c) = \sum_{i=0}^{k} a_i (x^i - c^i) \\
&= \sum_{i=0}^{k} a_i (x-c) \left(\sum_{j=0}^{i-1} x^j c^{\,i-j-1} \right) = (x-c)\, q(x).
\end{aligned}$$

`Passo induttivo.` Dato che $c_1, \dots, c_{n-1}$ soddisfano le ipotesi del lemma, per ipotesi induttiva abbiamo

$$f = \Big(\prod_{i=1}^{n-1} (x - c_i) \Big) q(x).$$

Si ha allora

$$f(c_n) = 0 = \Big(\prod_{i=1}^{n-1} (c_n - c_i) \Big) q(c_n) = 0 \implies q(c_n) = 0,$$

essendo $c_n - c_i \notin D(R)\ \forall i < n$. Quindi, per quanto dimostrato nel caso base $n = 1$,

$$q(x) = (x - c_n)r(x) \implies f = \Big(\prod_{i=1}^{n}(x - c_i)\Big)r(x),$$

come voluto.

Questo mostra che $g \mid f$ per ogni $f \in \mathcal{Z}(\{c_1, \ldots, c_n\})$, cioè $\mathcal{Z}(\{c_1, \ldots, c_n\}) \subseteq (g)$. L'altra inclusione è banale. □

Applichiamo questo Lemma per dare subito una descrizione esplicità di $\mathcal{Z}(R)$ nel caso in cui R sia un campo finito.

Lemma 1.1.12. *Sia R un campo finito di cardinalità q, con elementi $r_1, \ldots, r_q$. Allora $x^q - x = \prod_{i=1}^{q}(x - r_i)$ e $\mathcal{Z}(R) = (x^q - x)$.*

Dimostrazione. Sia $R = \{r_1, \ldots, r_q\}$. Le ipotesi del Lemma 1.1.11 sono soddisfatte in quanto per ogni $i \neq j$ si ha $r_i - r_j \neq 0$ e quindi $r_i - r_j \notin D(R) = \{0\}$, essendo R un campo. Applicando quindi il lemma, si ha che

$$\mathcal{Z}(R) = \mathcal{Z}(\{r_1, \ldots, r_q\}) = (\prod_{i=1}^{q}(x - r_i)).$$

Inoltre per un noto corollario del Teorema di Lagrange sui gruppi, $r^q - r = 0$ per ogni $r \in R$ e, di conseguenza, sempre per il Lemma 1.1.11, $\prod_{i=1}^{q}(x - r_i) | x^q - x$. I due polinomi hanno però lo stesso grado e sono ambedue monici. Ne segue che $x^q - x = \prod_{i=1}^{q}(x - r_i)$. □

Concludiamo dando, per mezzo di quest'ultimo risultato ed il Lemma 1.1.10, una descrizione esplicita dell'ideale $\mathcal{Z}(R, \mathfrak{n})$ con $\mathfrak{n}$ ideale massimale di indice finito, che ci sarà utile in seguito.

Lemma 1.1.13. *Sia R un anello ed $\mathfrak{n}$ un suo ideale massimale di indice finito q. Allora $\mathcal{Z}(R, \mathfrak{n}) = (x^q - x, \mathfrak{n})$.*

Dimostrazione. Con le notazioni del Lemma 1.1.10, si ha, applicando quest'ultimo per $S = R$ e $I = J = \mathfrak{n}$, che $\overline{\mathcal{Z}(R, \mathfrak{n})} = \mathcal{Z}(R/\mathfrak{n}, \mathfrak{n}/\mathfrak{n}) = \mathcal{Z}(R/\mathfrak{n})$. Dato che $R/\mathfrak{n}$ è un campo finito di cardinalità q, per il Lemma 1.1.12 si ha $\mathcal{Z}(R/\mathfrak{n}) = (x^q - x)$. Quindi, come voluto,

$$\mathcal{Z}(R, \mathfrak{n}) = \pi^{-1}_{\mathfrak{n}[x]}(\overline{\mathcal{Z}(R, \mathfrak{n})}) = \pi^{-1}_{\mathfrak{n}[x]}((x^q - x)) = (x^q - x, \mathfrak{n}),$$

dove la prima eguaglianza segue dal fatto che, banalmente, $\mathfrak{n}[x] \subseteq \mathcal{Z}(R, \mathfrak{n})$. □

1.2 π-polinomi

Denotiamo in questa sezione con $(R, \mathfrak{m})$ un anello locale (ed il suo ideale massimale), con campo residuo $\overline{R} = R/\mathfrak{m}$ finito di cardinalità q. Introduciano in questo contesto il concetto di *π-polinomio.*

Definizione 1.2.1. *Siano $R, \mathfrak{m}, q$ come sopra, e $\pi : R \to R/\mathfrak{m}$ la proiezione al quoziente. Sia $C = \{c_1, \ldots, c_q\} \subseteq R$ tale che $\pi(C) = R/\mathfrak{m}$ (ossia C è un qualsiasi insieme di rappresentanti per le classi laterali di $\mathfrak{m}$ in R). Allora definiamo π-polinomi gli elementi di $R[x]$ della forma $\prod_{c_i \in C}(x - c_i)$, per un qualche insieme C come sopra.*

Esempio 1.2.2. *Per $R=\mathbb{Z}/p\mathbb{Z}$ e $\mathfrak{m}=(0)$, l'unico π-polinomio è $\prod_{0\leq i<p}(x-i)=x^p-x$. Infatti, essendo $\mathfrak{m}=0$, l'unico insieme di rappresentanti è R stesso.*

In generale, per R campo finito, l'unico π-polinomio è $\prod_{r\in R}(x-r)$, che per il Lemma 1.1.12 è $x^{|R|}-x$. Infatti, essendo $\mathfrak{m}=0$, l'unico insieme di rappresentanti è R stesso.

Esempio 1.2.3. *Per p primo dispari ed $n\geq 1$ possiamo considerare l'anello locale $R=\mathbb{Z}/p^n\mathbb{Z}$, che ha ideale massimale $\mathfrak{m}=p\mathbb{Z}/p^n\mathbb{Z}$. Un insieme di rappresentanti delle classi laterali di $\mathfrak{m}$ è $\{0,\pm 1,\dots,\pm\frac{p-1}{2}\}\subseteq R$. Si ha quindi che $x\prod_{i=1}^{\frac{p-1}{2}}(x-i)(x+i)=x\prod_{i=1}^{\frac{p-1}{2}}(x^2-i^2)$ è un π-polinomio in $R[x]$.*

Osserviamo subito una semplice ma importante proprietà dei π-polinomi.

Lemma 1.2.4. *Sia $f\in R[x]$ un π-polinomio. Allora $f\in\mathcal{Z}(R,\mathfrak{m})$.*

Dimostrazione. Mostriamo che $\forall r\in R$ si ha $f(r)\in\mathfrak{m}$. Fissato r, sia c_i il rappresentante tale che $\bar{r}=\overline{c_i}\in R/\mathfrak{m}$, ossia $r-c_i\in\mathfrak{m}$. Allora

$$f(r)=(\prod_{j\neq i}(r-c_j))(r-c_i)\in\mathfrak{m}$$

come voluto. □

Pertanto, per $f\in\mathcal{Z}(\mathfrak{m})$ e g un π-polinomio si ha $f\circ g\in\mathcal{Z}(R)$. Infatti $\forall r\in R$ si ha $f(g(r))\in f(\mathfrak{m})=0$.

Forniremo una caratterizzazione più precisa dei π-polinomi nei teoremi al termine della Sezione 2.1.

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

In questa sezione denotiamo con $(R,\mathfrak{m})$ un anello locale noetheriano (ed il suo ideale massimale $\mathfrak{m}$). Cominciamo intanto col dimostrare un'importante caratterizzazione degli R per i quali $\mathcal{Z}(R)$ e $\mathcal{Z}(\mathfrak{m})$ sono non nulli.

Denotiamo con $\mathcal{N}(R)$ l'ideale dei nilpotenti di R.

Mostriamo innanzitutto un lemma, conseguenza diretta del Lemma 1.1.11.

Lemma 1.3.1. *Siano $(R,\mathfrak{m})$ un anello locale e $f\in R[x]$ con $\deg(f)\leq n$. Inoltre sia $S\subseteq R$ tale che $|\pi_{\mathfrak{m}}(S)|>n$ e supponiamo $f\in\mathcal{Z}(S)$. Allora $f=0\in R[x]$.*

Dimostrazione. Per ipotesi $\exists\ s_1,\dots,s_{n+1}\in S$ tali che $\pi_{\mathfrak{m}}(s_i)\neq\pi_{\mathfrak{m}}(s_j)\ \forall i\neq j$. Allora per ogni $i\neq j$ abbiamo $\pi_{\mathfrak{m}}(s_i-s_j)\neq 0$ ossia $s_i-s_j\notin\mathfrak{m}\implies s_i-s_j\in R^*$. Si conclude quindi per il Lemma 1.1.11 che $g:=\prod_{i=1}^{n+1}(x-s_i)|f$. Dato che g è monico, se $f\neq 0$ allora $n\geq\deg(f)\geq\deg(g)=n+1$, che è assurdo. Quindi $f=0$ come voluto. □

Questo lemma ha un ovvio corollario

Lemma 1.3.2. *Siano $(R,\mathfrak{m})$ un anello locale, $T\subseteq R$ tale che $|\pi_{\mathfrak{m}}(T)|=\infty$ e $f\in\mathcal{Z}(T)$. Allora $f=0$.*

Dimostrazione. Si procede per assurdo, supponendo $f\neq 0$, e ponendo $n=\deg(f)$. Sia $Z=\{s_1,\dots,s_{n+1}\}$ un insieme di $n+1$ elementi di T tali che $|\pi_{\mathfrak{m}}(\{s_1,\dots,s_{n+1}\})|=n+1$. Applicando il Lemma 1.3.1 per $S=Z$ (ovviamente $f\in\mathcal{Z}(T)$ implica $f\in\mathcal{Z}(Z)$) si trova $f=0$. □

Ricordiamo che un elemento di un anello si dice *regolare* se è non divisore di zero.

Richiamiamo inoltre la definizione di profondità (depth) di un anello $(R, \mathfrak{m})$ locale noetheriano.

Definizione 1.3.3. *Sia R un anello. Una* sequenza regolare *è una sequenza $x_1, \dots, x_n$ di elementi $x_i \in R$ tali che $\pi_{(x_1,\dots,x_{i-1})}(x_i) = \overline{x_i} \in R/(x_1, \dots, x_{i-1})$ è un elemento regolare $\forall i \leq n$.*

Definizione 1.3.4. *Sia $(R, \mathfrak{m})$ un anello locale. La* profondità *di R, che denotiamo con* $\operatorname{depth}(R)$*, è la lunghezza della massima sequenza regolare composta da elementi di $\mathfrak{m}$.*

Dimostriamo infine un lemma che caratterizza gli anelli $(R, \mathfrak{m})$ locali noetheriani con $\operatorname{depth}(R) = 0$.

Per farlo richiamiamo un fatto noto sui primi associati di un modulo su un anello noetheriano, si veda ad esempio [3, Thm. 6.1 e 6.5].

Denotiamo con $\operatorname{Ass}(M) = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} = 0 : m,\ m \in M\}$ l'insieme dei primi associati dell'R-modulo M.

Lemma 1.3.5. *Siano R un anello noetheriano e M un R-modulo finitamente generato non nullo. Allora* $\operatorname{Ass}(M)$ *è finito e non vuoto. Inoltre*

$$D(R) = \bigcup_{\mathfrak{p} \in \operatorname{Ass}(R)} \mathfrak{p}.$$

Lemma 1.3.6. *Sia $(R, \mathfrak{m})$ un anello locale noetheriano. Allora*

$$\operatorname{depth}(R) = 0 \iff \exists r \in R \setminus \{0\} \text{ tale che } r\mathfrak{m} = 0.$$

Dimostrazione. Per la definizione data di profondità, abbiamo

$$\operatorname{depth}(R) = 0 \iff \mathfrak{m} \subseteq D(R).$$

Infatti abbiamo che, per definizione, se $\operatorname{depth}(R) = 0$ non esistono elementi regolari in $\mathfrak{m}$, e quindi $\mathfrak{m} \subseteq D(R)$.

Viceversa se $\mathfrak{m} \subseteq D(R)$ non possono chiaramente esistere sequenze regolari $x_1, \dots, x_n$ di lunghezza non nulla, proprio perché x_1 non sarebbe regolare in $\mathfrak{m}$, quindi $\operatorname{depth}(R) = 0$.

Abbiamo allora che

$$\operatorname{depth}(R) = 0 \iff \mathfrak{m} \subseteq \bigcup_{\mathfrak{p} \in \operatorname{Ass}(R)} \mathfrak{p}$$

per il Lemma 1.3.5. Per il lemma di scansamento questo vale se e solo se $\mathfrak{m} \subseteq \mathfrak{p} = 0 : r$ per qualche $r \in R \setminus \{0\}$. Infine

$$\mathfrak{m} \subseteq 0 : r \iff mr = 0 \text{ per ogni } m \in \mathfrak{m} \iff r\mathfrak{m} = 0$$

come voluto. □

Un'altra semplice osservazione che possiamo subito dimostrare è che un qualsiasi anello artiniano locale ha profondità nulla.

Corollario 1.3.7. *Sia $(R, \mathfrak{m})$ un anello artiniano locale. Allora* $\operatorname{depth}(R) = 0$.

Dimostrazione. Dato che R è artiniano (e quindi noetheriano) locale, si ha

$$\mathfrak{m} = \mathcal{N}(R) \subseteq D(R) = \bigcup_{\mathfrak{p} \in \operatorname{Ass}(R)} \mathfrak{p}.$$

Quindi, per quanto osservato nel Lemma 1.3.6, $\operatorname{depth}(R) = 0$. □

Possiamo ora enunciare e dimostrare la caratterizzazione cercata.

Teorema 1.3.8. *Sia $(R,\mathfrak{m})$ un anello locale noetheriano. Allora si ha:*

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

Dimostrazione. 1. Per il Lemma 1.3.6, si ha che $\operatorname{depth}(R) = 0 \iff \exists r$ tale che $r\mathfrak{m} = 0$. Quindi, in tal caso, $rx \in \mathcal{Z}(\mathfrak{m})$.

Viceversa $\operatorname{depth}(R) \neq 0 \iff \exists t \in \mathfrak{m}$ regolare. Supponiamo $g = \sum_{i=0}^{n} g_i x^i \in \mathcal{Z}(\mathfrak{m})$, allora, in particolare $g(t^k) = \sum_{i=0}^{n} g_i t^{ki} = 0$ per ogni $1 \leq k \leq n+1$. Possiamo scrivere questo insieme di equazioni in forma matriciale, ottenendo

$$\begin{pmatrix} 1 & t & t^2 & \cdots & t^n \\ 1 & t^2 & t^4 & \cdots & t^{2n} \\ 1 & t^3 & t^6 & \cdots & t^{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & t^{n+1} & t^{2(n+1)} & \cdots & t^{n(n+1)} \end{pmatrix} \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Il determinante della matrice di Vandermonde V di dimensione $n+1 \times n+1$ e $V_{ij} = (t^i)^{j-1}$, è

$$\begin{aligned} \det(V) &= \prod_{1 \leq k < l \leq n+1} (t^l - t^k) = \prod_{1 \leq k < l \leq n+1} t^k (t^{l-k} - 1) \\ &= t^{\sum_{1 \leq k < l \leq n+1} k} u = t^N u \end{aligned}$$

con $u \in R^*$. Infatti per ogni $b > 0$, $t^b - 1 \notin \mathfrak{m}$ ed è quindi invertibile, essendo $(R,\mathfrak{m})$ locale. In particolare si osserva che $\det(V)$ è regolare in quanto prodotto di elementi regolari. Moltiplicando a destra e sinistra per $\operatorname{Adj}(V)$ si ottiene

$$\begin{pmatrix} \det(V) & 0 & 0 & \cdots & 0 \\ 0 & \det(V) & 0 & \cdots & 0 \\ 0 & 0 & \det(V) & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \det(V) \end{pmatrix} \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

ossia $\det(V) g_i = 0$. Per la regolarità di $\det(V)$, ciò implica $g_i = 0$ per ogni i. Quindi $g = 0$, come voluto.

2. Sia $\overline{R}$ finito e $\operatorname{depth}(R) = 0$. Esiste allora, per il Lemma 1.3.6, $r \in R \setminus \{0\}$ tale che $r\mathfrak{m} = 0$. Sia f un qualsiasi π-polinomio, allora per il Lemma 1.2.4 abbiamo che $\forall a \in R, rf(a) \in r\mathfrak{m} = 0$. Essendo i π-polinomi monici, abbiamo $rf \neq 0$ e quindi $\mathcal{Z}(R) \neq 0$.

Viceversa sia $f \in \mathcal{Z}(R)$ con $\overline{R}$ infinito o $\operatorname{depth}(R) \neq 0$. Nel primo caso si conclude immediatamente per il Lemma 1.3.2, posto $T = R$, che $f = 0$. Nell'altro caso supponiamo per assurdo $f \neq 0$, e sia $\deg(f) = n > 0$. Per definizione, $\operatorname{depth}(R) \neq 0 \iff \exists t \in \mathfrak{m} \setminus D(R)$, un elemento regolare. Consideriamo allora l'insieme di elementi regolari $T := \{t^k\}_{1 \leq k \leq n+1}$. Si ha che, per

$n+1 \geq a > b \geq 1$, $t^a - t^b = t^b(t^{a-b}-1)$ è elemento regolare in quanto prodotto di un'unità ($t^{a-b}-1$, per quanto già visto) ed un elemento regolare t^b. In particolare si ha che tale differenza non è nulla e quindi gli elementi di T sono distinti. Abbiamo quindi che per il Lemma 1.1.11, $g := \prod_{i=1}^{n+1}(x-t^i)|f$. Essendo g monico si ottiene quindi $n = \deg(f) \geq \deg(g) = n+1$, che è assurdo. Ne segue che in entrambi i casi $f = 0$, come voluto. □

Il prossimo risultato è una caratterizzazione degli anelli locali noetheriani con $\mathcal{Z}(R)$ e $\mathcal{Z}(\mathfrak{m})$ non solo non banali, ma contenenti elementi regolari.

Mostriamo innanzitutto il seguente lemma su $\mathcal{Z}(R)$ negli anelli locali noetheriani con dimensione di Krull positiva, insieme ad un lemma sugli anelli locali finiti che verrà usato nella dimostrazione della caratterizzazione.

Lemma 1.3.9. *Sia $(R,\mathfrak{m})$ un anello locale noetheriano con $\dim(R) > 0$. Allora $\mathcal{Z}(R) \subseteq \mathcal{Z}(\mathfrak{m}) \subseteq \mathcal{N}(R)[x]$. In particolare si ha $\mathcal{Z}(R) \subseteq \mathcal{Z}(\mathfrak{m}) \subseteq \mathcal{N}(R[x]) \subseteq D(R[x])$ e quindi $\mathcal{Z}(R)$ e $\mathcal{Z}(\mathfrak{m})$ non contengono elementi regolari.*

Dimostrazione. Se $(R,\mathfrak{m})$ è un anello locale noetheriano con $\dim(R) > 0$ si ha che $\mathfrak{m} \notin \mathrm{Min}(R)$ insieme dei primi minimali. Siano $\mathfrak{p} \in \mathrm{Min}(R)$ un qualsiasi primo minimale di R e $f \in \mathcal{Z}(\mathfrak{m})$. Applicando allora il Lemma 1.1.10 con $S = \mathfrak{m}$, $J = 0$ e $I = \mathfrak{p}$ si ha $\bar{f} = \pi_{\mathfrak{p}[x]}(f) \in \mathcal{Z}(\mathfrak{m}/\mathfrak{p})$. Si ha inoltre che $(R/\mathfrak{p}, \mathfrak{m}/\mathfrak{p})$ è un dominio locale noetheriano, nel quale, essendo $\mathfrak{p} \neq \mathfrak{m}$, esiste $t \in \mathfrak{m} \setminus \mathfrak{p}$ e quindi tale che $\bar{t} = \pi_{\mathfrak{p}}(t) \neq 0$. Quindi $\bar{t}$ è un elemento regolare in $\mathfrak{m}/\mathfrak{p}$, essendo non nullo nel dominio $R/\mathfrak{p}$. Ne segue che $\mathrm{depth}(R/\mathfrak{p}) \geq 1$, e quindi, per il Teorema 1.3.8, $\mathcal{Z}(\mathfrak{m}/\mathfrak{p}) = 0$. Quindi $\bar{f} = 0$, ossia $f \in \mathfrak{p}[x]$, $\forall \mathfrak{p} \in \mathrm{Min}(R)$. Ne segue allora che

$$f \in \bigcap_{\mathfrak{p}\in \mathrm{Min}(R)} \mathfrak{p}[x] = \Big(\bigcap_{\mathfrak{p}\in \mathrm{Min}(R)} \mathfrak{p}\Big)[x] = \mathcal{N}(R)[x]$$

come voluto. □

Lemma 1.3.10. *Sia $(R,\mathfrak{m})$ un anello locale. Allora R è finito se e solo se è artiniano e $\overline{R} := R/\mathfrak{m}$ è finito.*

Dimostrazione. Se R è finito è ovviamente artiniano e con $\overline{R}$ finito. Per dimostrare il viceversa si mostra, per induzione su n, che $R/\mathfrak{m}^n$ è finito $\forall n$. Questo basta per concludere, perché per artinianità esiste e tale che $\mathfrak{m}^e = 0$ e quindi $R/\mathfrak{m}^e = R$.
`Caso base, n=1.` Per $n = 1$ abbiamo $R/\mathfrak{m}^n = R/\mathfrak{m}$, finito per ipotesi.
`Passo induttivo.` Considero la successione esatta corta di $R/\mathfrak{m}$-moduli (e quindi $R/\mathfrak{m}$-spazi vettoriali)

$$0 \to \mathfrak{m}^n/\mathfrak{m}^{n+1} \to R/\mathfrak{m}^{n+1} \to R/\mathfrak{m}^n \to 0$$

dove le mappe sono l'inclusione e la proiezione canoniche. Si ha che $\mathfrak{m}^n$ è finitamente generato come R-modulo, per artinianità (e quindi noetherianità) di R. Da questo segue che $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ è finitamente generato come R-modulo, e quindi anche come $R/\mathfrak{m}$-modulo. Quindi, in particolare è finito essendo uno spazio vettoriale finitamente generato (ossia di dimensione finita) sul campo finito $R/\mathfrak{m}$. Inoltre $R/\mathfrak{m}^n$ è finito per ipotesi induttiva. Segue allora che anche il termine centrale della successione $R/\mathfrak{m}^{n+1}$ è finito. □

Possiamo ora finalmente enunciare e dimostrare la caratterizzazione cercata.

Teorema 1.3.11. *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.*

Dimostrazione. 1. L'anello locale noetheriano R è artiniano $\iff \exists e$ intero positivo tale che $\mathfrak{m}^e = 0$. Quindi $x^e \in \mathcal{Z}(\mathfrak{m})$. Osserviamo inoltre che x^e è regolare in $R[x]$, infatti non è divisore di zero in quanto, essendo monico, $\forall f \in R \setminus \{0\}$ si ha $\deg(x^e f) = e + \deg(f) \geq 1$ e quindi $x^e f \neq 0$.

Viceversa, se R non è artiniano, $\dim(R) > 0$ e quindi per il Lemma 1.3.9 $\mathcal{Z}(\mathfrak{m})$ non contiene elementi regolari.

2. Sia $(R, \mathfrak{m})$ un anello locale finito. In particolare si ha $|R/\mathfrak{m}| = q$ finito. Sia allora f un qualsiasi π-polinomio. Per il Lemma 1.2.4 si ha $f \in \mathcal{Z}(R, \mathfrak{m})$. Essendo R finito è anche artiniano e quindi $\exists e$ intero positivo tale che $\mathfrak{m}^e = 0$. Abbiamo allora che $\forall r \in R$, $f(r)^e \in \mathfrak{m}^e = 0$. Quindi $f^e \in \mathcal{Z}(R)$. Inoltre f^e è regolare: infatti non è divisore di zero in quanto, essendo monico, $\forall h \in R \setminus \{0\}$ si ha $\deg(f^e h) = eq + \deg(h) \geq 1$ e quindi $f^e h \neq 0$.

Viceversa, se R è infinito si ha per il Lemma 1.3.10 che o R non è artiniano o $R/\mathfrak{m}$ è infinito. In ogni caso $\mathcal{Z}(R)$ non contiene elementi regolari, nel primo caso per il Lemma 1.3.9, nel secondo caso dato che, per il Teorema 1.3.8, $\mathcal{Z}(R) = (0)$. □

1.4 Trivialità di $\mathcal{Z}(R)$ nel caso generale

Mostriamo in questa sezione una caraterizzazione degli anelli R con $\mathcal{Z}(R) \neq 0$ nel caso noetheriano ma non necessariamente locale.

Enunciamo e mostriamo preliminarmente un semplice lemma che descrive il comportamento di $\mathcal{Z}(R)$ rispetto alla localizzazione. Dati un anello R ed una sua parte moltiplicativa $T \subseteq R$ denotiamo con $i : R \to T^{-1}R$ la mappa canonica tale che $i(r) = \frac{r}{1}$. Denotiamo inoltre con i' la mappa

$$i' := (-[x])(i) : R[x] \to T^{-1}R[x]$$

indotta su $R[x]$ mediante il funtore $-[x]$: **Ring** $\to$ **Ring**. Dato un ideale $I \subseteq R$ denotiamo con $I^e = (i(I))$ la sua estensione rispetto alla mappa i, e analogamente dato un ideale $J \subseteq R[x]$ denotiamo con $J^e = (i'(J))$ la sua estensione rispetto alla mappa i'. Allo stesso modo denotiamo invece, per $I \subseteq T^{-1}R$ e $J \subseteq T^{-1}R[x]$, con I^c e J^c rispettivamente $i^{-1}(I)$ e $i'^{-1}(J)$, le contrazioni dei due ideali rispetto alle mappe i ed i'.

Lemma 1.4.1. *Siano R un anello, $S \subseteq R$ un suo sottoinsieme, $J \subset R$ un suo ideale e $T \subset R$ una sua parte moltiplicativa. Allora si ha, con le notazioni sopra definite, $\mathcal{Z}(S,J)^e \subseteq \mathcal{Z}(i(S), J^e) = \mathcal{Z}(S, J^{ec})^e$.*

Dimostrazione. Sia $f = \sum_{j=0}^{k} a_j x^j$ un generico elemento di $R[x]$. Allora, per ogni $s \in R$, si ha

$$i'(f)(i(s)) = \sum_{j=0}^{k} \left(\frac{a_j}{1}\right)\left(\frac{s}{1}\right)^j = \frac{\sum_{j=0}^{k} a_j s^j}{1} = i\left(\sum_{j=0}^{k} a_j s^j\right) = i(f(s)).$$

Questa semplice osservazione verrà usata più volte nella dimostrazione del lemma. Mostriamo ora l'inclusione e l'eguaglianza presenti nella tesi del lemma separatamente. Per la prima, basta osservare che $f \in \mathcal{Z}(S,J) \iff \forall s \in S\ f(s) \in J$, per definizione. Applicando la funzione i, otteniamo che

$i(f(s)) \in i(J) \subseteq J^e \ \forall s \in S$. Per l'osservazione fatta preliminarmente $i(f(s)) = i'(f)(i(s))$, quindi $i'(f)(s') \in J^e$ per ogni $s' \in i(S)$ ossia $i'(f) \in \mathcal{Z}(i(S), J^e)$. Dunque $i'(\mathcal{Z}(S,J)) \subseteq \mathcal{Z}(i(S), J^e)$, e di conseguenza $\mathcal{Z}(S,J)^e \subseteq \mathcal{Z}(i(S), J^e)$ come voluto.
Per la seconda osserviamo che, considerato un generico polinomio

$$f = \sum_{j=0}^{k} \frac{a_j}{t_j} x^j \in T^{-1}R[x]$$

sempre per definizione $f \in \mathcal{Z}(i(S), J^e) \iff f(i(s)) \in J^e$ per ogni $s \in S$. Posto allora $t := \prod_{j=0}^{k} t_j$ si ha che $tf = i'(f')$, dove f' è un polinomio in $R[x]$. Inoltre, dato che $i(f'(s)) = i'(f')(i(s)) = tf(i(s)) \in J^e$, abbiamo che $f'(s) \in J^{ec}$. Quindi $f' \in \mathcal{Z}(S, J^{ec})$, cioè $tf \in \mathcal{Z}(S, J^{ec})$ e, di conseguenza, $f \in \mathcal{Z}(S, J^{ec})^e$. Si conclude che $\mathcal{Z}(i(S), J^e) \subseteq \mathcal{Z}(S, J^{ec})^e$.

Infine osserviamo che $f \in \mathcal{Z}(S, J^{ec}) \iff f(s) \in J^{ec}$ per ogni $s \in S$, e quindi, applicando i, $i(f(s)) = i'(f)(i(s)) \in i(J^{ec}) \subseteq J^{ece} = J^e$ per ogni $s \in S$. Quindi $i'(f) \in \mathcal{Z}(i(S), J^e)$, e allora $i'(\mathcal{Z}(S, J^{ec})) \subseteq \mathcal{Z}(i(S), J^e)$, che implica $\mathcal{Z}(S, J^{ec})^e \subseteq \mathcal{Z}(i(S), J^e)$. Possiamo concludere che $\mathcal{Z}(i(S), J^e) = \mathcal{Z}(S, J^{ec})^e$, come voluto. □

Mostriamo ora che, in un certo senso, appartenere a $\mathcal{Z}(R)$ è una proprietà locale.

Siano R un anello noetheriano e $\mathfrak{p} \in \mathrm{Spec}(R)$, denotiamo con $i_\mathfrak{p} : R \to R_\mathfrak{p}$ la mappa canonica tale che $i_\mathfrak{p}(r) = \frac{r}{1}$. Per $f \in R[x]$ sia $f_\mathfrak{p} = (-)[x](i_\mathfrak{p})(f)$ l'immagine di f tramite la mappa $(-)[x](i_\mathfrak{p}) : R[x] \to R_\mathfrak{p}[x]$ indotta da $i_\mathfrak{p}$. Definiamo inoltre $j := \prod_{\mathfrak{p} \in \mathrm{Ass}(R)} i_\mathfrak{p} : R \to \prod_{\mathfrak{p} \in \mathrm{Ass}(R)} R_\mathfrak{p}$ la mappa canonica tale che $j(r) = (\frac{r}{1})_{\mathfrak{p} \in \mathrm{Ass}(R)}$. Mostriamo ora l'iniettività di j.

Lemma 1.4.2. *La mappa j è iniettiva.*

Dimostrazione. Supponiamo per assurdo che $r \in \mathrm{Ker}(j), r \neq 0$. Sia $\mathfrak{p}$ un primo in $\mathrm{Ass}((r))$. Allora $\mathfrak{p} = 0 : ar$ per qualche $a \in R \setminus \{0\}$. Dato che $j(r) = 0$, si ha $i_\mathfrak{p}(r) = \frac{r}{1} = 0$, cioè esiste $t \notin \mathfrak{p}$ tale che $tr = 0$. Quindi $tar = a(tr) = 0$ e dunque $t \in 0 : ar = \mathfrak{p}$, assurdo. □

Abbiamo ora tutto il necessario per dimostrare il seguente risultato:

Lemma 1.4.3. *Sia $S \subset R$ un sottoinsieme di un anello R. Allora*

$$f \in \mathcal{Z}(S) \iff f_\mathfrak{p} \in \mathcal{Z}(i_\mathfrak{p}(S)) \text{ per ogni } \mathfrak{p} \in \mathrm{Ass}(R).$$

Dimostrazione. Ricordiamo che, per ogni anello A, $\phi_A : A[x] \to M(A,A)$ è l'omomorfismo di anelli che associa ad ogni polinomio la funzione da esso indotta. Osserviamo innanzitutto che, per ogni $r \in R$, preso un polinomio generico $f = \sum_{i=0}^{k} a_i x^i \in R[x]$, si ha

$$\begin{aligned} j(\phi(f)(r)) = j(f(r)) &= j\left(\sum_{i=0}^{k} a_i r^i\right) \\ &= \left(\frac{\sum_{i=0}^{k} a_i r^i}{1}\right)_{\mathfrak{p} \in \mathrm{Ass}(R)} = \left(\sum_{i=0}^{k} \frac{a_i}{1} \frac{r}{1}^i\right)_{\mathfrak{p} \in \mathrm{Ass}(R)} \\ &= \big(f_\mathfrak{p}(i_\mathfrak{p}(r))\big)_{\mathfrak{p} \in \mathrm{Ass}(R)} = \big(\phi(f_\mathfrak{p})(i_\mathfrak{p}(r))\big)_{\mathfrak{p} \in \mathrm{Ass}(R)}. \end{aligned}$$

Quindi $j \circ \phi(f) = (\phi(f_\mathfrak{p}) \circ i_\mathfrak{p})_{\mathfrak{p} \in \mathrm{Ass}(R)}$.

Si ha inoltre che $f \in \mathcal{Z}(S)$ se e solo se $\phi(f)(S) = 0$, per definizione. Per l'iniettività di j, dimostrata nel Lemma 1.4.2, questo è vero se e solo se

$$(j \circ \phi(f))(S) = (\phi(f_{\mathfrak{p}} \circ i_{\mathfrak{p}})(S))_{\mathfrak{p} \in \mathrm{Ass}(R)} = 0.$$

Questo equivale a $\phi(f_{\mathfrak{p}})(i_{\mathfrak{p}}(S)) = 0$ per ogni $\mathfrak{p} \in \mathrm{Ass}(R)$, ossia a $f_{\mathfrak{p}} \in \mathcal{Z}(i_{\mathfrak{p}}(S))$ per ogni $\mathfrak{p} \in \mathrm{Ass}(R)$. □

Enunciamo e dimostriamo finalmente una caratterizzazione più generale per anelli noetheriani.

Teorema 1.4.4. *Sia un R anello noetheriano. Allora*

$$\mathcal{Z}(R) \neq (0) \iff \exists \mathfrak{p} \in \mathrm{Ass}(R) \text{ tale che } R/\mathfrak{p} \text{ è finito.}$$

Dimostrazione. Supponiamo che $\forall \mathfrak{p} \in \mathrm{Ass}(R)$ l'ideale $\mathfrak{p}$ abbia indice infinito e dimostriamo che $f \in \mathcal{Z}(R) \implies f = 0$. Fissiamo allora $\mathfrak{p}$ un qualunque primo di R. Sia $\psi : (R/\mathfrak{p})_{\pi_{\mathfrak{p}}(\mathfrak{p})} = Q(R/\mathfrak{p}) \to R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ l'isomorfismo canonico tale che $\psi(\frac{\overline{r}}{\overline{1}}) = \frac{\overline{r}}{1}$. Si ha allora

$$\psi \circ i_{\pi_{\mathfrak{p}}(\mathfrak{p})} \circ \pi_{\mathfrak{p}} = \pi_{\mathfrak{p}R_{\mathfrak{p}}} \circ i_{\mathfrak{p}}.$$

Di conseguenza, essendo ψ e $i_{\pi_{\mathfrak{p}}(\mathfrak{p})} : R/\mathfrak{p} \to Q(R/\mathfrak{p})$ entrambe iniettive, si ha

$$|\pi_{\mathfrak{p}R_{\mathfrak{p}}}(i_{\mathfrak{p}}(R))| = |\psi(i_{\pi_{\mathfrak{p}}(\mathfrak{p})}(\pi_{\mathfrak{p}}(R)))| = |\pi_{\mathfrak{p}}(R)| = |R/\mathfrak{p}| = \infty.$$

Abbiamo inoltre che, per il Lemma 1.4.3, $f \in \mathcal{Z}(R) \implies f_{\mathfrak{p}} \in \mathcal{Z}(i_{\mathfrak{p}}(R))$. Allora per il Lemma 1.3.2 applicato all'anello locale $(R_{\mathfrak{p}}, \mathfrak{p}R_{\mathfrak{p}})$, con $T = i_{\mathfrak{p}}(R)$, si conclude $f_{\mathfrak{p}} = 0$. A sua volta si ha, posto $f = \sum_{i=0}^{k} a_i x^i$,

$$\begin{aligned} f_{\mathfrak{p}} = 0 \text{ per ogni } \mathfrak{p} \in \mathrm{Ass}(R) &\iff \sum_{i=0}^{k} i_{\mathfrak{p}}(a_i)x^i = 0 \text{ per ogni } \mathfrak{p} \in \mathrm{Ass}(R) \\ &\iff i_{\mathfrak{p}}(a_i) = 0 \ \forall i \text{ e } \forall \mathfrak{p} \\ &\iff j(a_i) = 0 \ \forall i \\ &\iff a_i = 0 \ \forall i \\ &\iff f = 0, \end{aligned}$$

come voluto.

Viceversa sia $\mathfrak{p} \in \mathrm{Ass}(R)$ con indice finito. Sia allora $\{c_1, \ldots, c_q\}$ un insieme di rappresentanti delle classi laterali di $\mathfrak{p}$. Sia $t \in R$ tale che $\mathfrak{p} = 0 : t$. Allora posto $p = t\prod_{i=1}^{q}(x - c_i)$ si ha che per ogni $r \in R$ esiste j tale che $\pi_{\mathfrak{p}}(c_j) = \pi_{\mathfrak{p}}(r)$, ossia $r - c_j \in \mathfrak{p}$. Quindi $p(r) = t(r - c_j)\prod_{i \neq j}(r - c_i) \in t\mathfrak{p} = 0$. Abbiamo allora che $p \in \mathcal{Z}(R) \setminus \{0\}$. □

Capitolo 2

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

Nel corso di questo capitolo approfondiremo lo studio degli ideali $\mathcal{Z}(R)$ e $\mathcal{Z}(\mathfrak{m})$ nel caso di un anello R locale noetheriano. Nella prima sezione, dopo aver dato una decomposizione primaria minimale di $\mathcal{Z}(R)$ come intersezione di dei "traslati" $\mathcal{Z}(\mathfrak{m}+c_i)$ di $\mathcal{Z}(\mathfrak{m})$, mostreremo alcune fondamentali proprietà dei π-polinomi nel caso in cui R sia anche henseliano. In particolare mostreremo come una funzione indotta da un π-polinomio su qualunque classe laterale di $\mathfrak{m}$ sia surgettiva su $\mathfrak{m}$. Questo fatto sarà più volte cruciale nel seguito della nostra trattazione. Nella Sezione 2.2 daremo delle caratterizzazioni degli anelli $(R, \mathfrak{m})$ con $\mathcal{Z}(R)$ o $\mathcal{Z}(\mathfrak{m})$ principali o generati da un elemento regolare. Nell'ultima sezione del capitolo illustreremo infine un ulteriore legame, nel caso in cui R sia locale henseliano, fra $\mathcal{Z}(R)$ e $\mathcal{Z}(\mathfrak{m})$, dimostrando come un insieme di generatori del primo si possa ottenere semplicemente precomponendo un insieme di generatori del secondo con un qualsiasi π-polinomio. Questo fondamentale fatto, oltre a costituire in sé sicuramente un risultato degno di nota, sarà indispensabile nel capitolo successivo, permettendo di ridurci allo studio di $\mathcal{Z}(\mathfrak{m})$, per poi recuperare immediatamente un insieme di generatori d $\mathcal{Z}(R)$.

2.1 π-polinomi e decomposizione primaria

In tutta questa sezione, laddove non specificato, denotiamo con $(R, \mathfrak{m})$ un anello locale e $\overline{R} = R/\mathfrak{m}$. Dal Teorema 1.3.8 sappiamo che $|\overline{R}| = \infty \implies \mathcal{Z}(R) = 0$. Ci mettiamo quindi nel caso $|\overline{R}| = q$ intero positivo. Lo scopo della prima parte di questa sezione è fornire una dimostrazione del seguente teorema.

Teorema 2.1.1. *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 $\mathcal{Z}(R)$.*

Dimostrazione. Si ha, per il Lemma 1.1.9

$$\mathcal{Z}(R) = \mathcal{Z}(\bigcup_{1 \le i \le q} c_i + \mathfrak{m}) = \bigcap_{1 \le i \le q} \mathcal{Z}(c_i + \mathfrak{m}).$$

Mostriamo ora che $\mathcal{Z}(c_i + \mathfrak{m})$ è un ideale primario per ogni i. Per farlo basta mostrare che il suo radicale è massimale. Abbiamo

$$1 \notin \mathcal{Z}(c_i + \mathfrak{m}) \Longrightarrow 1 \notin \sqrt{\mathcal{Z}(c_i + \mathfrak{m})}$$

quindi è sufficiente mostrare che $\sqrt{\mathcal{Z}(c_i + \mathfrak{m})}$ contiene un ideale massimale per ottenere che $\sqrt{\mathcal{Z}(c_i + \mathfrak{m})}$ è esso stesso massimale.

Sia e tale che $\mathfrak{m}^e = 0$, la cui esistenza segue per finitezza e quindi artinianità di R. Per ogni $r \in c_i + \mathfrak{m}$ abbiamo $(r - c_i)^e \in \mathfrak{m}^e = 0$, e quindi $(x - c_i)^e \in \mathcal{Z}(c_i + \mathfrak{m})$. Da questo segue che $x - c_i \in \sqrt{\mathcal{Z}(c_i + \mathfrak{m})}$. Inoltre

$$\mathfrak{m}^e = 0 \implies \mathfrak{m} \subseteq \sqrt{0} \subseteq \sqrt{\mathcal{Z}(c_i + \mathfrak{m})}.$$

Quindi $(\mathfrak{m}, x - c_i) \subseteq \sqrt{\mathcal{Z}(c_i + \mathfrak{m})}$. Tale ideale è massimale dato che

$$R[x]/(\mathfrak{m}, x - c_i) \cong R/\mathfrak{m}$$

che è un campo.

Quindi $\mathcal{Z}(c_i + \mathfrak{m})$ è primario con primo associato $(x - c_i, \mathfrak{m})$, e quella del teorema è una decomposizione primaria.

Dimostriamo infine la sua minimalità, mostrando che per ogni j esiste un $f \in R[x]$ tale che $f \in \bigcap_{\substack{1 \le i \le q \\ i \neq j}} \mathcal{Z}(c_i + \mathfrak{m}) \setminus \mathcal{Z}(R)$. Consideriamo il polinomio

$$f = \prod_{\substack{1 \le i \le q \\ i \neq j}} (x - c_i)^e.$$

Per ogni $k \neq j$ si ha

$$r \in c_k + \mathfrak{m} \implies f(r) = (r - c_k)^e \prod_{\substack{1 \le i \le q \\ i \neq j \\ i \neq k}} (r - c_i)^e \in \mathfrak{m}^e = 0.$$

Quindi $f \in \mathcal{Z}(c_i + \mathfrak{m})$ per ogni $i \neq j$, ossia $f \in \bigcap_{\substack{1 \le i \le q \\ i \neq j}} \mathcal{Z}(c_i + \mathfrak{m})$. Si ha altresì che

$$f(c_j) = \prod_{\substack{1 \le i \le q \\ i \neq j}} (c_j - c_i)^e$$

con $c_j - c_i \notin \mathfrak{m}$ per ogni $i \neq j$, essendo $c_1, \ldots, c_q$ un insieme di rappresentanti delle classi laterali di $\mathfrak{m}$. Quindi $c_j - c_i \in R^*$ per ogni $i \neq j$ e di conseguenza $f(c_j) \in R^*$, in quanto prodotto di unità. In particolare $f(c_j) \neq 0$ e di conseguenza $f \notin \mathcal{Z}(R)$. □

Diamo ora un'altra caratterizzazione di $\mathcal{Z}(R)$ come intersezione, stavolta di ideali principali. In particolare questi ultimi sono gli (infiniti) ideali principali generati dai π-polinomi.

Teorema 2.1.2. *Sia $\mathcal{S}$ l'insieme dei π-polinomi in $R[x]$. Allora $\mathcal{Z}(R) = \bigcap_{f \in \mathcal{S}}(f)$.*

Dimostrazione. Sia $\mathcal{L}$ l'insieme degli insiemi di rappresentanti delle classi laterali di $\mathfrak{m}$, ossia $\mathcal{L} = \{S = \{c_1, \dots, c_q\} \subseteq R \text{ t.c. } \pi_{\mathfrak{m}}(S) = \overline{R}\}$. Allora si ha, per definizione di π-polinomio, che

$$\mathcal{S} = \{f \in R[x] \mid f = (x - c_1) \cdots (x - c_q), \{c_1, \dots, c_q\} \in \mathcal{L}\}.$$

Dato che è possibile estendere qualsiasi elemento $r \in R$ ad un insieme di rappresentanti delle classi laterali di $\mathfrak{m}$, abbiamo che $\bigcup_{S \in \mathcal{L}} S = R$. Quindi per il Lemma 1.1.9 ed il Lemma 1.1.11 si ha

$$\begin{aligned}
\mathcal{Z}(R) &= \mathcal{Z}\left(\bigcup_{S \in \mathcal{L}} S\right) \\
&= \bigcap_{\{c_1, \dots, c_q\} \in \mathcal{L}} \mathcal{Z}(\{c_1, \dots, c_q\}) \\
&= \bigcap_{\{c_1, \dots, c_q\} \in \mathcal{L}} \big((x - c_1) \cdots (x - c_q)\big) \\
&= \bigcap_{f \in \mathcal{S}} (f).
\end{aligned}$$

Si noti che abbiamo potuto applicare il Lemma 1.1.11 in quanto se $\{c_1, \dots, c_q\}$ è un insieme di rappresentanti delle classi laterali di $\mathfrak{m}$ allora $c_j - c_i \in R^*$ (e quindi in particolare non sono divisori di zero) per ogni $i \neq j$. □

Dimostriamo ora alcuni fatti sui π-polinomi.

Ricordiamo innanzitutto la definizione di *anello henseliano*. Dato un anello locale $(R, \mathfrak{m})$, un elemento $r \in R$ ed un polinomio $p(x) \in R[x]$, denotiamo $\pi_{\mathfrak{m}}(r)$ con $\overline{r}$ e $(-[x])(\pi_{\mathfrak{m}})(p(x)) = \pi_{\mathfrak{m}[x]}(p(x))$ con $\overline{p}(x)$.

Definizione 2.1.3. *Un anello $(R, \mathfrak{m})$ locale si dice henseliano se vale in tale anello il* Lemma di Hensel*, ossia se, dati un polinomio qualsiasi $f(x) \in R[x]$ e $\overline{a} \in \overline{R} = R/\mathfrak{m}$ una radice semplice di $\overline{f}(x)$ (cioè $\overline{f}(\overline{a}) = 0$ e $\overline{f}'(\overline{a}) \neq 0$ in $\overline{R}$), allora esiste $a' \in R$ con $f(a') = 0$ e $\overline{a'} = \overline{a}$.*

Si noti come esistano più definizioni equivalenti comunemente usate di *anello henseliano*, ad esempio:

Definizione 2.1.4. *Un anello $(R, \mathfrak{m})$ locale si dice henseliano se per ogni polinomio monico $f(x) \in R[x]$ tale che $\overline{f}(x)$ si fattorizza come*

$$\overline{f}(x) = g_1(x)h_1(x)$$

in $(R/\mathfrak{m})[x]$, con $g_1(x)$ e $h_1(x)$ monici e coprimi, allora esistono $g(x), h(x) \in R[x]$ monici tali che

$$f(x) = g(x)\, h(x), \quad e \quad \overline{g} = g_1, \quad \overline{h} = h_1.$$

Nelle dimostrazioni seguenti ci servirà solo poter sollevare radici, pertanto, per non appesantire la trattazione, abbiamo dato come definizione di anello henseliano la Definizione 2.1.3.

Enunciamo e dimostriamo ora il seguente teorema:

Teorema 2.1.5. *Sia $(R, \mathfrak{m})$ un anello locale con $R, \mathfrak{m}, q$ come sopra. Sia $p(x) \in R[x]$ qualsiasi. Se $p(x)$ è un π-polinomio, allora è monico e $\pi_{\mathfrak{m}[x]}(p(x)) = x^q - x \in \overline{R}[x]$. Se R è henseliano vale anche il viceversa.*

Dimostrazione. Sia f un qualsiasi π-polinomio in $R[x]$. Denotiamo con $\bar{f}$ il polinomio $\pi_{\mathfrak{m}[x]}(f) \in \overline{R}[x]$.

Per definizione $f = \prod_{i=1}^{q}(x - r_1)$, con $\{r_1, \dots, r_q\}$ un insieme di rappresentanti delle classi laterali di R. Quindi, usando Lemma 1.1.12, si ha che $\bar{f} = \prod_{i=1}^{q}(x - \overline{r_i}) = \prod_{\overline{r} \in \overline{R}}(x - \overline{r}) = x^q - x$, come voluto.

Per il viceversa, sia $f(x)$ un polinomio monico con $\bar{f}(x) = x^q - x \in \overline{R}[x]$. Si noti come questo implica che $\deg(f) = \deg(\bar{f}) = q$. Sia $\{d_1, \dots, d_q\}$ un qualsiasi insieme di rappresentanti delle classi laterali di $\mathfrak{m}$. Sia g il π-polinomio

$$g = \prod_{i=1}^{q}(x - d_i).$$

Allora, per quanto già visto nel corso di questa dimostrazione,

$$\bar{g} = \prod_{i=1}^{q}(x - \overline{d_i}) = x^q - x.$$

Quindi

$$\bar{f}(x) = x^q - x = \prod_{i=1}^{q}(x - \overline{d_i}) \in \overline{R}[x]$$

e $\bar{f}(\overline{d_i}) = 0$ per ogni i. Essendo i d_i distinti si ha inoltre che, per ogni i, $(x - d_i)^2 \nmid \overline{f}(x)$ in $\overline{R}[x]$ e quindi, per il criterio della derivata, $\bar{f}'(d_i) \neq 0$. Per henselianità si ha quindi che $\exists\{c_1, \dots, c_q\}$ tali che, per ogni i, $\overline{c_i} = \overline{d_i}$ e $f(c_i) = 0$. In particolare anche $\{c_1, \dots, c_q\}$ è un insieme di rappresentanti per le classi laterali di $\mathfrak{m}$, e dunque $c_i - c_j \in R \setminus \mathfrak{m} = R^*$ per ogni $i \neq j$. Definiamo il corrispettivo π-polinomio

$$h(x) = \prod_{i=1}^{q}(x - c_i)$$

ed applichiamo il Lemma 1.1.11 ad f: se ne desume che $h(x) \mid f(x)$. Essendo sia $h(x)$ che $f(x)$ monici di grado q si ha $h(x) = f(x)$ e quindi $f(x)$ è un π-polinomio. □

Mediante questo teorema è ora possibile mostrare il seguente importante risultato sulla surgettività su $\mathfrak{m}$ della funzione $\phi(f)$ indotta da un π-polinomio f nel caso di R henseliano.

Teorema 2.1.6. *Siano $(R, \mathfrak{m})$ henseliano e $f \in R[x]$ un π-polinomio. Allora $f(c + \mathfrak{m}) = \mathfrak{m}$ per ogni $c \in R$. In particolare $f(R) = \mathfrak{m}$.*

Dimostrazione. Dato $f \in R[x]$ un qualsiasi π-polinomio, si ha $f \in \mathcal{Z}(R, \mathfrak{m})$ per il Lemma 1.2.4, ossia $f(c + \mathfrak{m}) \subseteq f(R) \subseteq \mathfrak{m}$. Mostriamo ora il contenimento opposto. Sia $m \in \mathfrak{m}$ qualsiasi. Allora $\overline{f - m} = \overline{f} = x^q - x$. Quindi per il Teorema 2.1.5 $f - m$ è un π-polinomio. Possiamo allora scrivere $f - m = \prod_{i=1}^{q}(x - c_i)$ con $\{c_1, \dots, c_q\}$ un insieme di rappresentanti delle classi laterali di $\mathfrak{m}$. Essendo un insieme di rappresentanti si ha allora $c_j \in c + \mathfrak{m}$ per qualche j, e quindi che

$$(f - m)(c_j) = f(c_j) - m = (c_j - c_j) \prod_{\substack{1 \leq i \leq q \\ i \neq j}} (c_j - c_i) = 0 \implies f(c_j) = m.$$

Data l'arbitrarietà di m si ha allora che $f(c + \mathfrak{m}) = \mathfrak{m}$, come voluto. □

2.2 Casi in cui $\mathcal{Z}(R)$ e $\mathcal{Z}(\mathfrak{m})$ sono principali

Scopo di questa sezione è, usando i risultati mostrati nella sezione precedente, fornire ulteriori caratterizzazioni nello stile di quelle nella Sezione 1.3. Anche in questa sezione si assume, laddove non specificato diversamente, che $(R, \mathfrak{m})$ sia un anello locale noetheriano con il suo ideale massimale, e che il campo residuo $\overline{R} = R/\mathfrak{m}$ sia finito di cardinalità q.

Prima di enunciare la prima delle caratterizzazioni di questa sezione, enunciamo e dimostriamo un lemma sui polinomi regolari su anelli artiniani che sarà cruciale in seguito.

Lemma 2.2.1. *Siano $(R, \mathfrak{m})$ un anello locale artiniano e f un elemento regolare di $R[x]$. Allora esistono $v \in (R[x])^*$ e $f^* \in R[x]$ monico tali che $vf = f^*$.*

Dimostrazione. Nel corso di questa dimostrazione denoteremo, per un qualsiasi polinomio $p \in R[x]$, con $p[j]$ il coefficiente di grado j di p.

Si osserva innanzitutto che, posto $f = \sum_{i=0}^{d} \alpha_i x^i$, f regolare implica $f \notin \mathcal{N}(R[x]) = \mathcal{N}(R)[x] = \mathfrak{m}[x]$. Sia $k = \max\{k \text{ t.c. } \alpha_k \notin \mathfrak{m}\}$. Si noti che α_k è quindi invertibile. Dimostriamo per induzione su j che per ogni j esistono $g_j \in \mathfrak{m}[x], h_j \in \mathfrak{m}^j[x], f_j \in R[x]$ monico e $b_j \in R^*$ tali che

$$b_j f = f_j(1 + g_j) + h_j.$$

`Caso base, j=1.` Per $j = 1$ basta porre $g_1 = 0$, $h_1 = \alpha_k^{-1} \sum_{i=k+1}^{d} \alpha_i x^i \in \mathfrak{m}[x]$ per massimalità di k, $f_1 = \alpha_k^{-1} \sum_{i=0}^{k} \alpha_i x^i$, che è monico per costruzione e $b_1 = \alpha_k^{-1}$.

`Passo induttivo.` Per ipotesi induttiva possiamo scrivere

$$b_{j-1} f = f_{j-1}(1 + g_{j-1}) + h_{j-1}$$

con b_{j-1}, f_{j-1}, g_{j-1} e h_{j-1} con le proprietà sopra definite. Poniamo ora, eseguendo una divisione euclidea,

$$h_{j-1} = w f_{j-1} + r$$

con $w \in R[x]$ e $r \in R[x]$ con $\deg(r) < \deg(f_{j-1})$ (per convenzione $\deg(0) = -\infty$). Poniamo $b_j = b_{j-1}$, $f_j = f_{j-1} + r$ e $g_j = g_{j-1} + w$, e scriviamo $w = \sum_{i=0}^{s} w_i x^i$ e $f_{j-1} = \sum_{i=0}^{t} a_i x^i$.

Poniamo infine $h_j = b_j f - f_j(1 + g_j)$ di modo che $b_j f = f_j(1 + g_j) + h_j$ valga per costruzione.

Dato che f_{j-1} è monico e $\deg(r) < \deg(f_{j-1})$, anche f_j è monico. Rimane da verificare che $g_j \in \mathfrak{m}[x]$ e $h_j \in \mathfrak{m}^j[x]$.

Osserviamo che essendo $\deg(r) < \deg(f_{j-1}) := t$, si ha che $\forall\, k \geq t$

$$(f_{j-1} w)[k] = (h_{j-1} - r)[k] = h_{j-1}[k] \in \mathfrak{m}^{j-1}.$$

Mostriamo ora per induzione forte su l che per ogni $l \leq s$ si ha $w_{s-l} \in \mathfrak{m}^{j-1}$.

`Caso base, l=0.` Per $l = 0$ basta osservare che

$$(f_{j-1} w)[t + s] = w[s] = w_s$$

essendo f_{j-1} monico di grado t. Quindi $w_s \in \mathfrak{m}^{j-1}$ come voluto.

`Passo induttivo.` Si ha (ricordando $a_t = 1$ in quanto f_{j-1} è monico) che

$$(f_{j-1} w)[t + s - l] = \sum_{i=0}^{t} a_i w_{t+s-l-i} = (\sum_{i=0}^{t-1} a_i w_{t+s-l-i}) + w_{s-l}.$$

Si ha inoltre $(f_{j-1}w)[t+s-l] \in \mathfrak{m}^{j-1}$ e $w_{t+s-l-i} = w_{s-(l+i-t)} \in \mathfrak{m}^{j-1}$ per ogni $i \leq t-1$ per ipotesi induttiva. Allora anche $w_{s-l} \in \mathfrak{m}^{j-1}$, come voluto.

Dunque $w \in \mathfrak{m}^{j-1}[x]$ e quindi anche

$$r = h_{j-1} - wf_{j-1} \in \mathfrak{m}^{j-1}[x].$$

Si ha inoltre che

$$g_j = g_{j-1} + w \in \mathfrak{m}[x] + \mathfrak{m}^{j-1}[x] \subseteq \mathfrak{m}[x].$$

Infine

$$\begin{aligned} h_j &= b_j f - f_j(1+g_j) \\ &= b_j f - (f_{j-1}+r)(1+g_{j-1}+w) \\ &= b_j f - f_{j-1}(1+g_{j-1}) - f_{j-1}w - r(1+g_{j-1}+w) \\ &= b_j f - b_{j-1}f + h_{j-1} - h_{j-1} + r - r - rg_{j-1} - rw \\ &= rg_{j-1} - rw \in \mathfrak{m}^{j-1}[x]\mathfrak{m}[x] = \mathfrak{m}^j[x] \end{aligned}$$

e questo conclude la dimostrazione dell'esistenza di b_j, f_j, g_j e h_j che hanno le proprietà sopra definite.

Sia ora e tale che $\mathfrak{m}^e = 0$, che esiste per l'artinianità di R. Allora, posto $j = e$, si ha $h_e \in \mathfrak{m}^e[x] = 0$ e quindi

$$b_e f = (1+g_e)f_e$$

con f_e monico, $b_e \in R^*$ e $g_e \in \mathfrak{m}[x] = \mathcal{N}(R[x])$. Sia quindi N tale che $g_e^N = 0$. Allora

$$(1+g_e)(\sum_{i=0}^{N-1}(-1)^i g_e^i) = 1 + (-1)^{N-1}g_e^N = 1$$

e quindi $1+g_e \in (R[x])^*$. Si ha allora

$$b_e(1+g_e)^{-1}f = f_e.$$

Si conclude ponendo

$$v = b_e(1+g_e)^{-1}$$

che è un'unità in quanto prodotto di unità. □

Mostriamo inoltre due semplice lemmi generali: uno sugli ideali di un anello contenti elementi regolari, l'altro sul grado del generatore monico di un ideale principale in un anello di polinomi.

Lemma 2.2.2. *Siano R un anello e $I = (g)$ l'ideale principale generato da $g \in R$. Se esiste un elemento regolare $h \in I$ allora g è regolare.*

Dimostrazione. Si ha che $h = wg$ per qualche $w \in R$. Supponendo per assurdo $g \in D(R)$ e quindi $gt = 0$ per qualche $t \in R \setminus \{0\}$, avremmo quindi che $ht = w(gt) = 0$ e di conseguenza $h \in D(R)$, contrariamente a quanto supposto per ipotesi. Quindi g è regolare. □

Procediamo quindi ora ad enunciare e dimostrare la caratterizzazione cercata.

Teorema 2.2.3. *Siano $(R, \mathfrak{m})$ un anello locale finito ed $f \in R[x]$ un qualsiasi π-polinomio. Allora sono equivalenti:*

1. *R è un campo;*
2. *$\mathcal{Z}(R)$ è principale;*
3. *$\mathcal{Z}(R) = (f(x))$;*
4. *$\mathcal{Z}(\mathfrak{m})$ è principale;*
5. *$\mathcal{Z}(\mathfrak{m}) = (x)$.*

Dimostrazione. Osserviamo innanzitutto che R finito implica $\overline{R}$ finito, e quindi ha senso parlare di π-polinomi in $R[x]$.

Inoltre, per il Lemma 1.3.7, R finito (in particolare, artiniano) implica $\operatorname{depth}(R) = 0$ e quindi esiste $t \in R \setminus \{0\}$ tale che $t\mathfrak{m} = 0$, per il Lemma 1.3.6.

L'affermazione 1 implica la 2 in quanto se R è un campo $R[x]$ è un PID, e in particolare tutti i suoi ideali sono principali.

Mostriamo ora che la 2 implica la 3.

Per il Teorema 1.3.11, $\mathcal{Z}(R)$ contiene elementi regolari. Quindi se $\mathcal{Z}(R) = (g)$ per qualche $g \in R$, g deve essere regolare per il Lemma 2.2.2.

Per il Lemma 2.2.1 esiste $v \in (R[x])^*$ tale che $g_1 := vg$ è monico. Ovviamente $(g) = (g_1)$.

Inoltre per il Lemma 1.2.4, $f \in \mathcal{Z}(R, \mathfrak{m})$ e quindi per ogni $r \in R$ si ha $tf(r) \in t\mathfrak{m} = 0$. Quindi $0 \neq tf \in \mathcal{Z}(R) = (g_1)$, e allora, dato che f è monico, si conclude $\deg(tf) = \deg(f) = q \geq \deg(g_1)$.

Per il Teorema 2.1.2 si ha inoltre, denotando con $\mathcal{S}$ l'insieme dei π-polinomi in $R[x]$,

$$(g_1) = \mathcal{Z}(R) = \bigcap_{p \in \mathcal{S}} (p) \subseteq (f).$$

Quindi $f \mid g_1$ in $R[x]$, e g_1 è monico, come f, e di grado $\deg(g_1) \leq q = \deg(f)$.

Segue che $f = g_1$, e quindi $\mathcal{Z}(R) = (f)$ come voluto.

Mostriamo che a sua volta la 3 implica la 4.

Infatti, se $\mathcal{Z}(R) = (f)$ si ha per il Teorema 2.1.6 che $\mathfrak{m} = f(R) = 0$, essendo f sia π-polinomio che elemento di $\mathcal{Z}(R)$. Si noti che abbiamo potuto applicare il teorema in quanto R finito è anche completo, quindi henseliano. Dato che $\mathfrak{m} = 0$ si ha quindi $\mathcal{Z}(\mathfrak{m}) = \mathcal{Z}(\{0\}) = (x)$, per la dimostrazione del Lemma 1.1.11 nel caso $n = 1$. In particolare $\mathcal{Z}(\mathfrak{m})$ è principale, come voluto.

Mostriamo ora che la 4 implica la 5.

Per la 4, $\mathcal{Z}(\mathfrak{m}) = (g)$ per qualche polinomio $g \in R[x]$.

Sia e intero tale che $\mathfrak{m}^e = 0$, che esiste per artinianità. Si ha allora che per ogni $m \in \mathfrak{m}$, $m^e = 0$, quindi $x^e \in \mathcal{Z}(\mathfrak{m})$. Come già visto $x^e \in \mathcal{Z}(\mathfrak{m})$ è regolare, e quindi, per il Lemma 2.2.2, g è regolare.

Per il Lemma 2.2.1, esiste v unità in $(R[x])^*$ tale che $g_1 := vg$ è monico, e ovviamente $(g) = (g_1)$.

Inoltre si ha per ogni $m \in \mathfrak{m}$, $tm \in t\mathfrak{m} = 0$ e quindi $tx \in \mathcal{Z}(\mathfrak{m}) = (g_1)$. Dunque $\deg(tx) = 1 \geq \deg(g_1)$. Quindi g_1 è monico di grado ≤ 1, e non è 1 in quanto altrimenti si avrebbe $\mathcal{Z}(\mathfrak{m}) = (1) \implies 1(0) = 1 = 0$, assurdo. Dunque g_1 è della forma $x + x_0$ per qualche $x_0 \in R$. Per concludere osserviamo che, essendo $0 \in \mathfrak{m}$ e $g_1 \in \mathcal{Z}(\mathfrak{m})$, si ha $g_1(0) = x_0 = 0$, e quindi $g_1 = x$, e $\mathcal{Z}(\mathfrak{m}) = (x)$, come voluto.

Concludiamo mostrando che la 5 implica 1.

Infatti se $\mathcal{Z}(\mathfrak{m}) = (x)$, per ogni $m \in \mathfrak{m}$ vale che $x(m) = m = 0$. Segue che $\mathfrak{m} = 0$ e R è un campo. □

Concludiamo la sezione con un'ulteriore caratterizzazione, stavolta degli anelli con $\mathcal{Z}(R)$ e $\mathcal{Z}(\mathfrak{m})$ principali e generati da un elemento regolare.

Teorema 2.2.4. *Sia $(R, \mathfrak{m})$ un anello locale noetheriano. Allora:*

1. *$\mathcal{Z}(\mathfrak{m})$ è generato da un elemento regolare di $R[x] \iff R$ è un campo;*
2. *$\mathcal{Z}(R)$ è generato da un elemento regolare di $R[x] \iff R$ è un campo finito.*

Dimostrazione. Dimostriamo la prima affermazione.

Se R è campo, $\mathcal{Z}(\mathfrak{m}) = \mathcal{Z}(\{0\}) = (x)$ per il Lemma 1.1.11. Ovviamente x è regolare e quindi basta ora mostrare l'implicazione opposta.

Se $\mathcal{Z}(\mathfrak{m})$ è generato da un elemento regolare g, per il Teorema 1.3.11, R è artiniano. Allora, per il Lemma 1.3.7, $\operatorname{depth}(R) = 0$. Quindi per il Lemma 1.3.6 esiste $t \in R \setminus \{0\}$ tale che $t\mathfrak{m} = 0$, e dunque $tx \in \mathcal{Z}(\mathfrak{m})$. Esiste inoltre per il Lemma 2.2.1 v in $(R[x])^*$ tale che $g_1 := vg$ è monico, e $(g) = (g_1) = \mathcal{Z}(\mathfrak{m})$. Allora $\deg(g_1) \leq \deg(tx) = 1$. Quindi g_1 è nella forma $x + x_0$ per qualche $x_0 \in R$, e analogamente a quanto già mostrato nella dimostrazione del Teorema 2.2.3 se ne deduce che $(g_1) = \mathcal{Z}(\mathfrak{m}) = (x)$, dato che si deve avere $g_1(0) = x_0 = 0$. Quindi, per il Teorema 2.2.3, R è un campo, come voluto.

Mostriamo ora la seconda affermazione.

Se R è campo un finito, allora per il Teorema 2.2.3, $\mathcal{Z}(R) = (f)$ per f un qualsiasi π-polinomio in $R[x]$. Inoltre f è monico e dunque anche regolare. Quindi $\mathcal{Z}(R)$ è generato da un elemento regolare.

Viceversa se $\mathcal{Z}(R)$ è generato da un elemento regolare $f \in R[x]$, per il Teorema 1.3.11, R è finito, oltre che locale. Dato che $\mathcal{Z}(R)$ è principale, applicando il Teorema 2.2.3 abbiamo che R è un campo. Dunque R è un campo finito, come voluto. □

2.3 Da $\mathcal{Z}(\mathfrak{m})$ a $\mathcal{Z}(R)$

Anche in questa sezione, laddove non specificato diversamente, $(R, \mathfrak{m})$ è un anello locale con campo residuo $\overline{R}$ di cardinalità finita q.

Dato un qualsiasi π-polinomio $f \in R[x]$ ed un qualsiasi $g \in \mathcal{Z}(\mathfrak{m})$, si ha che per ogni $r \in R$, $g(f(r)) \in g(\mathfrak{m}) = 0$, dal momento che, per il Lemma 1.2.4, $f \in \mathcal{Z}(R, \mathfrak{m})$. Quindi $g \circ f \in \mathcal{Z}(R)$.

Lo scopo di questa sezione è arrivare a dimostrare il seguente teorema che in qualche modo fornisce un viceversa di questa facile osservazione: si mostra infatti come, sotto un'opportuna ipotesi di henselianità, esista un insieme di generatori di $\mathcal{Z}(R)$ dato dalla composizione di un insieme di generatori di $\mathcal{Z}(R, \mathfrak{m})$ con un π-polinomio $f(x) \in \mathcal{Z}(R, \mathfrak{m})$.

Teorema 2.3.1. *Siano $(R, \mathfrak{m})$ un anello locale henseliano con $|R/\mathfrak{m}| = q$ e $f(x) \in R[x]$ un qualsiasi π-polinomio. Allora se $\mathcal{Z}(\mathfrak{m}) = (F_1(x), \ldots, F_n(x))$, si ha che $\mathcal{Z}(R) = (F_1(f(x)), \ldots, F_n(f(x)))$.*

Si mostra prima un risultato più tecnico ma dal quale il Teorema 2.3.1 seguirà facilmente.

Teorema 2.3.2. *Siano $(R, \mathfrak{m})$ un anello locale henseliano con $|R/\mathfrak{m}| = q$, $f(x) \in R[x]$ un qualsiasi π-polinomio e $g(x) \in \mathcal{Z}(R)$. Allora esistono $r_0(x), \ldots, r_{q-1}(x)$ tali che $r_i(x) \in \mathcal{Z}(\mathfrak{m})$ per ogni $1 \leq i \leq q-1$ e*

$$g(x) = \sum_{i=0}^{q-1} x^i r_i(f(x)).$$

Dimostrazione. Identificando $g(x)$ e $f(x)$ con le loro immagini tramite l'immersione canonica $R[x] \to R[x, y]$, consideriamo il polinomio in due variabili $h(x, y) = f(x) - y \in R[x, y]$. Applicando l'algoritmo

di divisione euclidea su $R[x,y] = R[y][x]$, scriviamo

$$g(x) = w(x,y)h(x,y) + r(x,y)$$

con

$$\deg_x(r(x,y)) < \deg_x(h(x,y)) = \deg_x(f(x)) = q.$$

Sia allora

$$r(x,y) = \sum_{i=0}^{q-1} r_i(y)x^i \in R[x,y] = R[y][x]$$

con $r_1(y), \dots, r_{q-1}(y) \in R[y]$. Applicando l'omomorfismo di valutazione $\psi_{f(x)} : R[x,y] \to R[x]$ definito da $\psi_{f(x)} : p(x,y) \mapsto p(x, f(x))$, otteniamo

$$g(x) = w(x,f(x))h(x,f(x)) + r(x,f(x)) = r(x,f(x)) = \sum_{i=0}^{q-1} r_i(f(x))x^i.$$

Concludiamo ora mostrando che, per ogni i, $r_i(x) \in \mathcal{Z}(\mathfrak{m})$.

Posto $\{c_1, \dots, c_q\}$ un insieme di rappresentanti delle classi laterali di $\mathfrak{m}$, per il Lemma 2.1.6 abbiamo che $f(c_j + \mathfrak{m}) = \mathfrak{m}$. Quindi, fissato $m \in \mathfrak{m}$ qualunque, per ogni j troviamo $d_j \in c_j + \mathfrak{m}$ tale che $f(d_j) = m$.

Per ogni j, valutando $g(x) \in \mathcal{Z}(R)$ in d_j otteniamo allora

$$0 = g(d_j) = \sum_{i=0}^{q-1} r_i(m)d_j^i$$

ossia, posto

$$p_m(x) = \sum_{i=0}^{q-1} r_i(m)x^i,$$

si ha $p_m(x) \in \mathcal{Z}(\{d_1, \dots, d_q\})$.

Abbiamo che $\{d_1, \dots, d_q\}$ è, per costruzione, un insieme di rappresentanti delle classi laterali di $\mathfrak{m}$, ossia $|\pi_{\mathfrak{m}}(\{d_1, \dots, d_q\})| = q$, e che $\deg(p_m(x)) \leq q - 1 < q$. Si conclude per il Lemma 1.3.1 che $p_m(x) = 0$, ovvero che $r_i(m) = 0$ per ogni i.

Data l'arbitrarietà di m si ha allora che $r_i(x) \in \mathcal{Z}(\mathfrak{m})$ per ogni i, come voluto. □

Procediamo ora alla dimostrazione del Teorema 2.3.1.

Dimostrazione. Sia $g \in \mathcal{Z}(R)$. Allora per il Teorema 1.3.10 si ha $g = \sum_{i=0}^{q-1} r_i(f(x))x^i$ per dei polinomi $r_0(x), \dots, r_{q-1}(x) \in \mathcal{Z}(\mathfrak{m}) = (F_1(x), \dots, F_n(x))$. Poniamo, per ogni j

$$r_j(x) = \sum_{k=1}^{n} a_k^{(j)}(x)F_k(x)$$

con $a_k^{(j)}(x) \in R[x]$ per ogni j e k.

Abbiamo allora

$$\begin{aligned} g &= \sum_{i=0}^{q-1}\sum_{k=1}^{n} a_k^{(i)}(f(x))F_k(f(x))x^i \\ &= \sum_{k=1}^{n} F_k(f(x))\left(\sum_{i=0}^{q-1} a_k^{(i)}(x)x^i\right) \in (F_1(f(x)),\dots,F_n(f(x))). \end{aligned}$$

Quindi $\mathcal{Z}(R) \subseteq (F_1(f(x)),\dots,F_n(f(x)))$.

L'inclusione opposta è banale in quanto per ogni i e per ogni $r \in R$, per il Lemma 1.2.4, $F_i(f(r)) \in F_i(\mathfrak{m}) = 0$, dato che $F_i(x) \in \mathcal{Z}(\mathfrak{m})$. Quindi, per ogni i, $F_i(f(x)) \in \mathcal{Z}(R)$, e questo conclude. □

Capitolo 3

Il caso locale finito con ideale massimale principale

Nel corso di quest'ultimo capitolo ci concentreremo sul caso in cui R sia, oltre che locale, finito e con ideale massimale $\mathfrak{m} = (m)$ principale, con lo scopo di arrivare a dare una descrizione esplicita di $\mathcal{Z}(\mathfrak{m})$ in termini di generatori. A tale scopo, introdurremo nella prima sezione il concetto di q-espansione di un numero naturale n, grazie al quale sarà poi possibile definire le funzioni D ed E di cui dimostreremo alcune proprietà fondamentali. A loro volta quest'ultime saranno poi usate nella definizione dei polinomi L_n che forniscono insiemi di generatori per due famiglie di ideali A_n e B_n, nel contesto di un generico anello locale avente ideale massimale principale e di indice finito. La dimostrazione dell'uguaglianza $A_n = B_n$ sarà il risultato finale della Sezione 3.2. Nel corso della Sezione 3.3 mostreremo invece come, nel caso in cui R sia un DVR henseliano, A_n e B_n coincidano non solo fra di loro ma anche con l'ideale $\mathcal{Z}(\mathfrak{m}, \mathfrak{m}^n)$ dei polinomi che mandano l'ideale massimale nella sua n-esima potenza. La Sezione 3.4 combinerà il risultato su $\mathcal{Z}(\mathfrak{m}, \mathfrak{m}^{n+1})$ con il Teorema di Struttura di Cohen ed un suo raffinamento che ci permetterà di scrivere un qualsiasi anello locale finito avente ideale massimale principale come quoziente di un DVR completo. Concluderemo così che in tal caso $\mathcal{Z}(\mathfrak{m}) = A_n = B_n$. Trovato ciò le descrizioni di $\mathcal{Z}(R)$, sia in termini di generatori che di componenti primarie, saranno semplici corollari di quanto appena mostrato unito ai risultati del Capitolo 2.

3.1 q-espansioni e funzioni aritmetiche collegate

Definiamo in questa sezione il concetto di q-espansione di un numero naturale n ed alcune funzioni aritmetiche collegate, che saranno fondamentali nella costruzione di un insieme di generatori per $\mathcal{Z}(\mathfrak{m})$.

Definizione 3.1.1. *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.*

Esempio 3.1.2. *Per $q = 3$ si ha $Q_1 = 1$, $Q_2 = 4$, $Q_3 = 13$. Si ha quindi che ad esempio $3Q_2 + 2Q_3$ è una 3-espansione di 38.*

Esempio 3.1.3. *Per qualunque q (essendo $q = |R/\mathfrak{m}| \geq 2$), 0 ha q-espansione $0 = 0Q_1$, 1 ha q-espansione $1 = 1Q_1$ e 2 ha q-espansione $2Q_1$. Per $q > 2$, 3 ha q-espansione $3 = 3Q_1$, mentre per $q = 2$ ha espansione $3 = Q_2$.*

Diciamo che due q-espansioni $n = \sum_{i=1}^{k} \mu_i Q_i = \sum_{i=1}^{k'} \mu'_i Q_i$ con $k < k'$ coincidono se e solo se $\mu_i = \mu'_i$ per $0 \leq i \leq k$ e $\mu'_i = 0$ per ogni $i > k$. Tale relazione di coincidenza è ovviamente una relazione di equivalenza.

Osserviamo preliminarmente che

$$qQ_i = q\sum_{j=0}^{i-1} q^j = \sum_{j=1}^{i} q^j = Q_{i+1} - 1.$$

Dimostriamo ora un lemma che sarà cruciale nella dimostrazione dell'unicità delle q-espansioni.

Lemma 3.1.4. *Sia n un intero con q-espansione $\sum_{i=0}^{t} \mu_i Q_i$. Allora $n < Q_{t+1}$.*

Dimostrazione. Definiamo per $0 \leq j \leq t$

$$S_j = \{qQ_j + \sum_{t \geq i > j} \mu_i Q_i \mid 0 \leq \mu_i \leq q-1 \text{ per ogni } i\}.$$

Si osserva facilmente che per ogni $n_j \in S_j$

$$n_j \leq qQ_j + \sum_{t \geq i > j} (q-1)Q_i \in S_j$$

e che per ogni $0 \leq j \leq t$

$$\begin{aligned}
\max(S_j) &= qQ_j + \sum_{t \geq i > j} (q-1)Q_i = qQ_j + \sum_{t \geq i > j} (q^i - 1) \\
&= qQ_j - (t-j) + \sum_{i=0}^{t} q^i - \sum_{i=0}^{j} q^i = Q_{j+1} - 1 - (t-j) + Q_{t+1} - Q_{j+1} \\
&= Q_{t+1} - (t-j+1) < Q_{t+1}.
\end{aligned}$$

Posto allora $\mathcal{Q}_t$ l'insieme delle q-espansioni con coefficienti nulli per Q_s per ogni $s > t$, si ha

$$\begin{aligned}
\mathcal{Q}_t &= \left\{ \sum_{i=1}^{t} \nu_i Q_i \;\middle|\; \begin{array}{l} 0 \leq \nu_i \leq q, \\ \nu_i = 0 \text{ se } \nu_j = q \text{ per qualche } j > i \end{array} \right\} \\
&= \bigcup_{k=0}^{t} \left\{ \sum_{i=1}^{t} \nu_i Q_i \;\middle|\; \begin{array}{l} 0 \leq \nu_i \leq q, \\ \nu_i = 0 \text{ se } \nu_j = q \text{ per qualche } j > i, \\ \nu_k = q \end{array} \right\} \\
&= \bigcup_{k=0}^{t} \left\{ qQ_k + \sum_{t \geq i > k} \mu_i Q_i \;\middle|\; 0 \leq \mu_i \leq q-1 \right\} \\
&= \bigcup_{k=0}^{t} S_k
\end{aligned}$$

dove per convenzione si è posto $\nu_0 = q$ se $\nu_i \neq q$ per ogni $i \geq 1$.
Quindi

$$\begin{aligned}\max(\mathcal{Q}_t) &= \max\left(\{\max(S_k) \mid 0 \leq k \leq t\}\right) \\ &= \max\left(\{Q_{t+1} - (t-k+1) \mid 0 \leq k \leq t\}\right) \\ &= Q_{t+1} - 1 < Q_{t+1}\end{aligned}$$

che è esattamente quanto cercato. □

Lemma 3.1.5. *Ogni numero naturale n ammette una ed una sola q-espansione.*

Dimostrazione. Dimostro l'esistenza e l'unicità separatamente.

`Esistenza.` Dimostriamo per induzione su k che ogni $n < Q_{k+1}$ ammette una q-espansione dove compaiono coefficienti μ_i non nulli solo per $i \leq k$. Essendo $\lim_{k\to\infty} Q_k = \infty$ questo conclude.

Denotiamo con $\mathcal{H}_k = \{rQ_k \mid 0 \leq r \leq q\}$.

`Caso base, k=1.` Si ha $Q_2 = 1 + q$ e $Q_1 = 1$. Allora per $n < Q_2$, ossia $n \leq q$, si ha che $n = nQ_1$ è una q-espansione, come voluto.

`Passo induttivo` Sia $n < Q_{k+1}$. Sia $n' = \max(\mathcal{H}_k \cap \{i \mid i \leq n\})$ il massimo elemento di $\mathcal{H}_k$ minore o uguale di n.

Sia analogamente $n'' = \min(\mathcal{H}_k \cap \{i \mid i \geq n\})$ il minimo elemento di $\mathcal{H}_k$ maggiore o uguale di n. In particolare si ha che tale n'' esiste se e solo se $n \leq qQ_k = Q_{k+1} - 1$ ossia se e solo se $n < Q_{k+1}$, che è vero per ipotesi.

Se $n = tQ_k$ per qualche $t \leq q$ abbiamo concluso, dato che $n = tQ_k$ è una q-espansione valida.

Altrimenti si ha

$$n' = tQ_k < n < (t+1)Q_k = n''$$

per qualche $t \leq q - 1$.

Quindi $n = tQ_k + r$ con $0 < r = n - n' < n'' - n' = Q_k$. Allora, per ipotesi induttiva $r = \sum_{i=1}^{k-1} \nu_i Q_i$ con $0 \leq \nu_i \leq q$ per ogni i e $\nu_i = 0$ se $\nu_j = q$ per qualche $j > i$.

Abbiamo quindi che

$$n = \sum_{i=1}^{k} \mu_i Q_i$$

con $\mu_i = \nu_i$ per $i < k$ e $\mu_k = t$. Essendo $t \leq q - 1$ si ha che anche i μ_i soddisfano la proprietà che rende quella trovata una q-espansione.

`Unicità`

Supponiamo che $\sum_{i=1}^{k} \mu_i Q_i = n = \sum_{i=1}^{t} \nu_i Q_i$ siano due q-espansioni di un intero n e mostriamo che sono coincidenti.

Possiamo assumere senza perdita di generalità $k \geq t$ e $\nu_t \neq 0$. Se per assurdo $k > t$ e $\mu_j > 0$ per qualche $j > t$, si avrebbe $n \geq Q_j \geq Q_{t+1}$. Ma per il Lemma 3.1.4, essendo $\sum_{i=1}^{t} \nu_i Q_i$ una q-espansione di n, si avrebbe anche $n < Q_{t+1}$. Abbiamo quindi l'assurdo cercato e se ne conclude che $\mu_i = 0$ per ogni $i > t$. Possiamo quindi, a meno di sostituire la prima q-espansione con una coincidente, assumere $k = t$.

Concludiamo mostrando, per induzione su t, che se si ha l'eguaglianza fra due q-espansioni

$$\sum_{i=1}^{t} \mu_i Q_i = \sum_{i=1}^{t} \nu_i Q_i$$

queste coincidono, ossia $\mu_i = \nu_i$ per ogni i.

`Caso base, t=1.` Basta osservare che in tal caso $\mu_1 Q_1 = \mu_1 = \nu_1 = \nu_1 Q_1$.

`Passo induttivo.` Se $\mu_t = \nu_t$ si ha allora

$$\sum_{i=1}^{t-1} \mu_i Q_i = \sum_{i=1}^{t-1} \nu_i Q_i$$

che implica, per ipotesi induttiva, essendo le due ancora q-espansioni, $\mu_i = \nu_i$ per ogni i. Si conclude quindi in tal caso che anche le due q-espansioni originali coincidono, come voluto.

Per concludere è sufficiente quindi dimostrare che $\mu_t = \nu_t$: dimostriamolo per assurdo, supponendo invece $\mu_t \neq \nu_t$.

Sia j l'intero tale che $\mu_j = q$ se tale intero esiste (in tal caso è necessariamente unico per definizione di q-espansione), $j = 0$ altrimenti. Analogamente sia j' l'intero tale che $\nu_{j'} = q$ se tale intero esiste, $j' = 0$ altrimenti. Possiamo assumere senza perdita di generalità $j \geq j'$.

Con queste notazioni abbiamo quindi che

$$\left(\sum_{t \geq i > j} \mu_i Q_i \right) + q Q_j = \sum_{i=1}^{t} \mu_i Q_i = \sum_{i=1}^{t} \nu_i Q_i = \left(\sum_{t \geq i > j'} \nu_i Q_i \right) + q Q_{j'}.$$

Se avessimo $j = t$ (quindi $n = qQ_t$ nell'espansione a sinistra) e $j' < t$, si avrebbe allora

$$\begin{aligned}
Q_t &\leq (q - \nu_t) Q_t \\
&= q Q_{j'} + \sum_{t-1 \geq i > j'} \nu_i Q_i \\
&\leq q Q_{j'} + \sum_{t-1 \geq i > j'} (q-1) Q_i \\
&= Q_{j'+1} - 1 + \sum_{t-1 \geq i > j'} (q^i - 1) \\
&= Q_{j'+1} - 1 + (Q_t - Q_{j'+1}) - (t - 1 - j') \\
&= Q_t - (t - j') < Q_t
\end{aligned}$$

che è assurdo.

Quindi se $j = t$ si ha anche $j' = t$ e le due q-espansioni coincidono essendo entrambe qQ_t.

Rimane quindi solo da esaminare il caso $t > j \geq j'$.

In tal caso, se $\mu_t > \nu_t$ si avrebbe che

$$\begin{aligned}
Q_t &\leq (\mu_t - \nu_t)Q_t \\
&= qQ_{j'} - qQ_j + \sum_{t-1\geq i>j} (\nu_i - \mu_i)Q_i + \sum_{j\geq i>j'} \nu_i Q_i \\
&\leq (Q_{j'+1} - 1) - (Q_{j+1} - 1) + \sum_{t-1\geq i>j'} (q-1)Q_i \\
&= Q_{j'+1} - Q_{j+1} + \sum_{t-1\geq i>j'} (q^i - 1) \\
&= Q_{j'+1} - Q_{j+1} + (Q_t - Q_{j'+1}) - (t - 1 - j') \\
&= Q_t - Q_{j+1} - (t - 1 - j') \\
&< Q_t
\end{aligned}$$

che è assurdo.
Il caso $\mu_t < \nu_t$ è del tutto analogo, partendo dalla diseguaglianza $Q_t \geq (\nu_t - \mu_t)Q_t$.
Si ha allora necessariamente che $\mu_t = \nu_t$, e questo conclude. □

Possiamo finalmente definire il concetto di numero q-libero, assieme ad altre funzioni aritmetiche legate alle q-espansioni che saranno cruciali nel corso della trattazione.

Definizione 3.1.6. *Per ogni $i \geq 1$ definiamo $\mu_i : \mathbb{N} \to \mathbb{N}$ la funzione che associa ad ogni intero n il coefficiente di Q_i nella q-espansione di n. Poniamo $\mu_i(n) = 0$ se nella q-espansione il termine Q_i non compare.*

Osserviamo che, per definizione, $n = \sum_{i=1}^{\infty} \mu_i(n)Q_i$. Si noti come questa sommatoria ha senso in quanto $\mu_i(n) \neq 0$ solo per un numero finito di i.

Definizione 3.1.7. *Definiamo la funzione $\iota : \mathbb{N} \to \mathbb{N}$ come segue:*

$$\iota(n) = \begin{cases} i & \text{se esiste } i > 0 \text{ tale che } \mu_i(n) = q, \\ 0 & \text{se } \mu_i(n) \neq q \text{ per ogni } i. \end{cases}$$

Definizione 3.1.8. *Un intero n si dice q-libero se $\iota(n) = 0$. Denotiamo con $\mathcal{F}_q = \{n \in \mathbb{N} \mid \iota(n) = 0\}$ l'insieme degli interi q-liberi.*

Definizione 3.1.9. *Definiamo $D = \sum_{i=1}^{\infty} q^{i-1}\mu_i : \mathbb{N} \to \mathbb{N}$.*

Si noti come la precedente definizione ha senso in quanto $\mu_i(n) \neq 0$ per un numero finito di valori i e per definizione, se $n \in \mathbb{N}$ ha q-espansione $\sum_{i=1}^{t_n} \mu_i(n)Q_i$,

$$D(n) = \sum_{i=1}^{\infty} q^{i-1}\mu_i(n) = \sum_{i=1}^{t_n} \mu_i(n)q^{i-1}.$$

Esempio 3.1.10. *Considerando quanto visto nell'Esempio 3.1.3, si ha che $D(0) = 0$, $D(1) = 1q^0 = 1$ e $D(2) = 2q^0 = 2$. In generale, $D(i) = iq^0 = i$ per ogni $i \leq q$, e $D(q+1) = 1q^1 = q$.*

Enunciamo e dimostriamo ora alcuni lemmi elementari su D e μ_i.

Lemma 3.1.11. *Per ogni intero $n \in \mathbb{N}$ si ha $\sum_{i=1}^{\infty} \mu_{i+1}(n)Q_i = n - D(n)$.*

Dimostrazione. Si osserva innanzitutto che l'espressione $\sum_{i=1}^{\infty} \mu_{i+1}(n)Q_i$ ha senso in quanto $\mu_{i+1}(n) \neq 0$ solo per un numero finito di i.

Si ha allora

$$\begin{aligned}
\sum_{i=1}^{\infty} \mu_{i+1}(n)Q_i &= \sum_{i=2}^{\infty} \mu_i(n)Q_{i-1} \\
&= \sum_{i=2}^{\infty} \mu_i(n)(Q_i - q^{i-1}) \\
&= \sum_{i=1}^{\infty} \mu_i(n)(Q_i - q^{i-1}) \\
&= \left(\sum_{i=1}^{\infty} \mu_i(n)Q_i\right) - \left(\sum_{i=1}^{\infty} \mu_i(n)q^{i-1}\right) \\
&= n - D(n),
\end{aligned}$$

dove abbiamo usato che $Q_1 - q^{1-1} = 1 - 1 = 0$ e che

$$Q_i = \sum_{j=0}^{i-1} q^j = \sum_{j=0}^{i-2} q^j + q^{i-1} = Q_{i-1} + q^{i-1}$$

per ogni $i \geq 2$. □

Lemma 3.1.12. *Per ogni $n \in \mathbb{N}$ ed ogni $i \geq 1$ si ha che*

$$\mu_i(n+1) = \begin{cases} 0 & \text{se } i \leq \iota(n), \\ \mu_i(n) + 1 & \text{se } i = \iota(n) + 1, \\ \mu_i(n) & \text{se } i > \iota(n) + 1. \end{cases}$$

Dimostrazione. Se n è q-libero, sia $\sum_{i=1}^{t_n} \mu_i(n)Q_i$ la sua q-espansione, con $\mu_i(n) < q$ per ogni i. Si ha quindi che $n + 1 = \sum_{i=1}^{t_n} \mu'_i(n+1)Q_i$, dove abbiamo posto

$$\mu'_i(n+1) = \begin{cases} \mu_i(n) + 1 & \text{se } i = 1, \\ \mu_i(n) & \text{altrimenti.} \end{cases}$$

Quest'ultima è una q-espansione, essendo $\mu_i(n) < q$ per ogni i e quindi $\mu_1(n+1) \leq q$, $\mu_i(n+1) < q$ per ogni $i > 1$, e quindi $\mu_i(n+1) = \mu'_i(n+1)$.

Altrimenti sia $j = \iota(n) > 0$. Si ha allora che n ha q-espansione $qQ_j + \sum_{i=j+1}^{\infty} \mu_i(n)Q_i$ con $\mu_i(n) < q$ per ogni i.

Quindi

$$n + 1 = 1 + qQ_j + \sum_{i=j+1}^{\infty} \mu'_i(n+1)Q_i = Q_{j+1} + \sum_{i=j+1}^{\infty} \mu'_i(n+1)Q_i = \sum_{i=1}^{\infty} \mu'_i(n+1)Q_i,$$

dove abbiamo posto

$$\mu'_i(n+1) = \begin{cases} 0 & \text{se } i \leq j, \\ \mu_i(n)+1 & \text{se } i = j+1, \\ \mu_i(n) & \text{altrimenti} \end{cases}$$

che è una q-espansione di $n+1$ dato che $\mu'_{j+1}(n+1) = \mu_j(n)+1 \leq q$, $\mu'_i(n+1) = 0$ per ogni $i < j+1$ e $\mu'_i(n+1) = \mu_i(n) < q$ per ogni $i > j+1$, e quindi $\mu_i(n+1) = \mu'_i(n+1)$.

In ambo i casi è quindi verificata la tesi del lemma. □

Corollario 3.1.13. *Per ogni $n \in \mathbb{N}$ si ha che $\iota(n+1) \in \{0, \iota(n)+1\}$.*

Dimostrazione. Per il Lemma 3.1.12 abbiamo che, per ogni $i < \iota(n)+1$, $\mu_i(n+1) = 0$. Inoltre $\mu_i(n) = \mu_i(n+1) < q$ per ogni $i > \iota(n)+1$. Inoltre $\mu_{\iota(n)+1}(n+1) = \mu_{\iota(n)+1}(n)+1$. Quindi $\iota(n+1) = \iota(n)+1$, se $\mu_{\iota(n)+1}(n) = q-1$, ed è 0 altrimenti. □

Lemma 3.1.14. *Per ogni intero n il numero $n+1-q^{\iota(n)}$ è q-libero.*

Dimostrazione. Per brevità sia $j = \iota(n)$.

Cominciamo con l'osservare che, per il Lemma 3.1.12,

$$n+1-q^j = Q_j - Q_{j+1} + \sum_{i=1}^{\infty} \mu_i(n+1)Q_i = Q_j - Q_{j+1} + Q_{j+1} + \sum_{i=j+1}^{\infty} \mu_i(n)Q_i = \sum_{i=0}^{\infty} \nu_i Q_i$$

con

$$\nu_i = \begin{cases} 0 & \text{se } i < j \\ 1 & \text{se } i = j \\ \mu_i(n) & \text{se } i > j. \end{cases}$$

In particolare $\nu_i < q$ per ogni i, e quindi $\sum_{i=0}^{\infty} \nu_i Q_i$ è una q-espansione di $n+1-q^j$ e quest'ultimo è q-libero, come voluto. □

Lemma 3.1.15. *Per ogni $n \in \mathbb{N}$ si ha*

$$D(n+1) = \begin{cases} D(n)+1 & \textit{se } n \textit{ è } q\textit{-libero}, \\ D(n) & \textit{altrimenti.} \end{cases}$$

In particolare, D è debolmente crescente.

Dimostrazione. Se n è q-libero si ha, applicando il Lemma 3.1.12

$$D(n+1) = \sum_{i=1}^{\infty} \mu_i(n+1)q^{i-1} = 1 + \sum_{i=1}^{\infty} \mu_i(n)q^{i-1} = 1 + D(n).$$

Se invece $\iota(n) = j > 0$ si ha, applicando sempre il Lemma 3.1.12, che

$$\begin{aligned} D(n+1) &= \sum_{i=1}^{\infty} \mu_i(n+1)q^{i-1} = q^j + \sum_{i=j+1}^{\infty} \mu_i(n)q^{i-1} \\ &= q^j + \left(\sum_{i=1}^{\infty} \mu_i(n)q^{i-1} \right) - \mu_j(n)q^{j-1} = q^j - qq^{j-1} + D(n) = D(n) \end{aligned}$$

come voluto. □

Lemma 3.1.16. *La funzione $D|_{\mathcal{F}_q} : S_q \to \mathbb{N}$, la restrizione di D ad $\mathcal{F}_q$, l'insieme degli interi q-liberi, è bigettiva e strettamente crescente.*

Dimostrazione. Dal Lemma 3.1.15 segue che per $s, z \in \mathcal{F}_q$ con $z > s$ si ha $D(s) < D(s+1) \leq D(z)$. Quindi $D|_{\mathcal{F}_q}$ è strettamente crescente, ed in particolare è iniettiva. Dimostriamo ora che ora che $D|_{\mathcal{F}_q}$ è suriettiva. Sia $n \in \mathbb{N}$ qualunque e sia $\sum_{i=0}^{d} a_i q^i$ la sua espansione in base q. Allora $s := \sum_{i=1}^{d+1} a_{i-1} Q_i \in \mathcal{F}_q$, dato che $a_i < q$ per ogni i e quindi $\sum_{i=1}^{d+1} a_{i-1} Q_i$ è una q-espansione per s e $\iota(s) = 0$. Si ha dunque che

$$D(s) = \sum_{i=1}^{d+1} a_{i-1} q^{i-1} = \sum_{i=0}^{d} a_i q^i = n.$$

Per l'arbitrarietà di n si conclude quidi che $D|_{\mathcal{F}_q}$ è suriettiva, come voluto. □

Possiamo ora definire la funzione E.

Definizione 3.1.17. *Denotiamo con E la funzione $D|_{\mathcal{F}_q}^{-1} : \mathbb{N} \to S$, l'inversa di $D|_{\mathcal{F}_q}$.*

Si ha quindi, dato che per definizione $E(n) \in S$ per ogni $n \in \mathbb{N}$,

$$D(E(n)) = D|_{\mathcal{F}_q}(E(n)) = (D|_{\mathcal{F}_q} \circ E)(n) = n$$

e che E è strettamente crescente essendo inversa di $D|_{\mathcal{F}_q}$ che è strettamente crescente per il Lemma 3.1.15.

Si osserva che, sempre per definizione, se n ha espansione in base q data da $n = \sum_{i=0}^{t} a_i q^i$, allora

$$E(n) = \sum_{i=1}^{t+1} a_{i-1} Q_i.$$

Si ha infatti $\sum_{i=1}^{t+1} a_{i-1} Q_i \in \mathcal{F}_q$ in quanto $a_i < q$ per ogni i e

$$D(\sum_{i=1}^{t+1} a_{i-1} Q_i) = \sum_{i=1}^{t+1} a_{i-1} q^{i-1} = \sum_{i=0}^{t} a_i q^i = n.$$

Esempio 3.1.18. *Per qualunque $q > 2$ usando quest'ultima osservazione deduciamo che $E(0) = E(0q^0) = 0Q_1 = 0$, $E(1) = E(1q^0) = 1Q_1 = 1$ ed $E(2) = E(2q^0) = 2Q_1 = 2$. Per $q = 2$ abbiamo invece $E(2) = E(0q^0 + 1q^1) = 0Q_1 + 1Q_2 = 1 + q = 3$.*

Sempre attraverso l'osservazione appena fatta sono di immediata dimostrazione due lemmi: il primo fornisce una proprietà ricorsiva di E, l'altro una caratterizzazione della quantità $\mu_1(E(n))$.

Lemma 3.1.19. *Per ogni intero $n \geq 0$ si ha che $E(n) = n + E(\lfloor \frac{n}{q} \rfloor)$.*

Dimostrazione. Sia $\sum_{i=0}^{t} a_i q^i$ un'espansione in base q di n, dove, a meno di aggiungere un termine $0q^1$, possiamo assumere $t \geq 1$. Allora

$$\begin{aligned} n + E\left(\left\lfloor \frac{n}{q} \right\rfloor\right) &= \sum_{i=0}^{t} a_i q^i + E\left(\left\lfloor \frac{a_0}{q} + \sum_{i=1}^{t} a_i q^{i-1} \right\rfloor\right) \\ &= \sum_{i=0}^{t} a_i q^i + E\left(\sum_{i=0}^{t-1} a_{i+1} q^i\right) \\ &= \sum_{i=0}^{t} a_i q^i + \sum_{i=1}^{t} a_i Q_i \\ &= \sum_{i=0}^{t} a_i Q_{i+1} = \sum_{i=1}^{t+1} a_{i-1} Q_i = E(n). \end{aligned}$$ □

Lemma 3.1.20. *Per ogni intero $n \geq 0$ si ha che $\mu_1(E(n)) = n - q\lfloor \frac{n}{q} \rfloor$.*

Dimostrazione. Sia $\sum_{i=0}^{t} a_i q^i$ un'espansione in base q di n, dove, a meno di aggiungere un termine $0q^1$, possiamo assumere $t \geq 1$. Allora basta osservare che

$$\begin{aligned} \mu_1(E(n)) = \mu_1\left(\sum_{i=1}^{t+1} a_{i-1} Q_i\right) &= a_0 = \sum_{i=0}^{t} a_i q^i - \sum_{i=1}^{t} a_i q^i \\ &= n - q \sum_{i=1}^{t} a_i q^{i-1} = n - q \left\lfloor \frac{a_0}{q} + \frac{1}{q} \sum_{i=1}^{t} a_i q^i \right\rfloor \\ &= n - q \left\lfloor \frac{n}{q} \right\rfloor. \end{aligned}$$ □

Dimostriamo ora un lemma che caratterizza $E(D(n))$.

Lemma 3.1.21. *Per ogni intero $n \geq 0$, $E(D(n)) = \inf\{k \geq n \text{ t.c. } k \in \mathcal{F}_q\}$, ossia $E(D(n))$ è il più piccolo intero q-libero maggiore o uguale ad n. In particolare $E(D(n)) \geq n$ ed $E(D(n)) = n$ se e solo se n è q-libero.*

Dimostrazione. Per il Lemma 3.1.16, esiste un unico $s \in \mathcal{F}_q$ tale che $D(s) = D(n)$. Per la monotonia debole di D (Lemma 3.1.15) questo implica $s \geq n$. Sempre per il Lemma 3.1.15 ed il Lemma 3.1.16, per qualsiasi $z \in \mathcal{F}_q$ che sia diverso da s e maggiore o uguale a n si ha $D(z) \geq D(n) = D(s)$. Dall'iniettività di $D_{|\mathcal{F}_q}$ si ottiene $D(z) > D(s)$ e quindi $z > s$.

Quindi $s = \inf\{k \geq n \text{ t.c. } k \in \mathcal{F}_q\}$. Mostriamo per concludere che $s = E(D(n))$.

Per farlo basta osservare che $D(E(D(n))) = (D \circ E)(D(n)) = D(n)$ e $E(D(n)) \in \mathrm{Im}(E) = \mathcal{F}_q$. Per l'unicità di s questo conclude. □

Diamo ora una simile caratterizzazione per $E(D(n) - 1)$.

Lemma 3.1.22. *Per ogni intero $n \geq 0$, $E(D(n) - 1) = \sup\{k < n \text{ t.c. } k \in \mathcal{F}_q\}$, ossia $E(D(n) - 1)$ è il più grande intero q-libero minore di n. In particolare $E(D(n) - 1) < n$.*

Dimostrazione. Per il Lemma 3.1.16, esiste un unico $s \in \mathcal{F}_q$ tale che $D(s) = D(n) - 1 < D(n)$. Per la monotonia debole di D (Lemma 3.1.15) questo implica $s < n$. Sempre per il Lemma 3.1.15 ed il Lemma 3.1.16, per qualsiasi $z \in \mathcal{F}_q$ che sia strettamente minore di n, si ha $D(z) < D(z)+1 = D(z+1) \leq D(n)$. Quindi $D(z) \leq D(n) - 1 = D(s)$, e per la monotonia di $D|_{\mathcal{F}_q}$ questo implica che $z \leq s$.

Quindi $s = \sup\{k < n \text{ t.c. } k \in \mathcal{F}_q\}$.

Mostriamo per concludere che $s = E(D(n) - 1)$. Per farlo basta osservare che $D(E(D(n) - 1)) = (D \circ E)(D(n) - 1) = D(n) - 1$ e $E(D(n) - 1) \in \mathrm{Im}(E) = \mathcal{F}_q$. Per l'unicità di s questo conclude. □

Mostriamo infine una semplice diseguaglianza che coinvolge le funzioni D ed E e che tornerà utile in seguito nella trattazione.

Lemma 3.1.23. *Per ogni coppia di interi n ed i tali che $n \geq 1$ e $0 \leq i \leq D(n) - 1$, si ha $E(i) - i \leq n - D(n)$.*

Dimostrazione. Poniamo $j = n-i$ e dimostriamo, per induzione su j, che $E(n-j)-(n-j) \leq n-D(n)$ per $n - D(n) + 1 \leq j \leq n$.

`Caso base,` $j = n - D(n) + 1$. Dobbiamo mostrare che

$$E(D(n) - 1) - D(n) + 1 \leq n - D(n),$$

ovvero che $E(D(n) - 1) + 1 \leq n$. Questo segue immediatamente dal Lemma 3.1.22.

`Passo induttivo.` Sia $n \geq j > n - D(n) + 1$, e quindi $0 \leq n - j \leq D(n) - 1$. Essendo E strettamente crescente si ha allora che $E(n - j) \leq E(n - (j - 1)) - 1$. Per ipotesi induttiva $E(n-(j-1))-(n-(j-1)) \leq D(n)-n$, e dunque $E(n-j) \leq D(n)-n+(n-(j-1))-1 = D(n)-n+(n-j)$.

Abbiamo quindi trovato che $E(n - j) - (n - j) \leq D(n) - n$, come voluto. □

3.2 I polinomi $L_n(x)$ e $\pi_n(x)$, gli ideali B_n e A_n

In questa sezione e quelle successive assumiamo che $(R, \mathfrak{m})$, laddove non specificato diversamente, sia un anello noetheriano locale con campo residuo $R/\mathfrak{m} = \overline{R}$ finito di cardinalità q, e $\mathfrak{m} = (m)$ ideale principale.

Cominciamo col definire alcune famiglie di polinomi ed ideali che saranno fondamentali nella trattazione. Scopo di questa sezione sarà, oltre a dare queste definizioni, dimostrare alcune elementari proprietà su questi ultimi.

Definizione 3.2.1. *Per ogni intero $n \geq 0$ definiamo $\pi_n(x) = x^q - m^{q^n-1}x \in R[x]$.*

Esempio 3.2.2. *Abbiamo $\pi_0(x) = x^q - m^{q^0-1}x = x^q - x$, $\pi_1(x) = x^q - m^{q-1}x$, $\pi_2(x) = x^q - m^{q^2-1}x$.*

Mostriamo subito un primo lemma che collega i polinomi π_n agli ideali oggetto della nostra trattazione.

Lemma 3.2.3. *Per ogni intero $n \geq 0$, $\pi_n(x) \in \mathcal{Z}(\mathfrak{m}^{Q_n}, \mathfrak{m}^{Q_{n+1}})$.*

Dimostrazione. Dal momento che $\mathfrak{m}^{Q_n} = (m^{Q_n})$, basta osservare che, per ogni $r \in R$,

$$\pi_n(rm^{Q_n}) = r^q m^{qQ_n} - rm^{q^n-1}m^{Q_n} = r^q m^{Q_{n+1}-1} - rm^{Q_{n+1}-1} = m^{Q_{n+1}-1}(r^q - r) \in \mathfrak{m}^{Q_{n+1}}$$

dove abbiamo usato il fatto che, per il Lemma 1.1.13, $r^q - r \in \mathfrak{m}$. □

Definizione 3.2.4. *Per ogni intero $n \geq 1$ definiamo ricorsivamente*

$$T_n(x) = \begin{cases} x & \text{se } n = 1, \\ \pi_{n-1}(T_{n-1}(x)) & \text{se } n > 1. \end{cases}$$

Esempio 3.2.5. *Per quanto visto nella Definizione 3.2.4 e nell'Esempio 3.2.2*

$$T_2(x) = \pi_1(T_1(x)) = \pi_1(x) = x^q - m^{q-1}x,$$

$$T_3(x) = \pi_2(T_2(x)) = (x^q - m^{q-1}x)^q - m^{q^2-1}(x^q - m^{q-1}x).$$

Dalla definizione ricorsiva dei polinomi $T_n(x)$ e dal Lemma 3.2.3 segue immediatamente il seguente risultato.

Lemma 3.2.6. *Per ogni intero $n \geq 1$, $T_n(x) \in \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^{Q_n})$.*

Dimostrazione. Procediamo per induzione su n.

`Caso base, n=1.` Si ha che $T_1 = x \in \mathcal{Z}(\mathfrak{m}, \mathfrak{m})$ banalmente.

`Passo induttivo.` Per $n > 1$ si ha, per ipotesi induttiva, $T_{n-1} \in \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^{Q_{n-1}})$.
Quindi $T_n(\mathfrak{m}) = \pi_{n-1}(T_{n-1}(\mathfrak{m})) \subseteq \pi_{n-1}(\mathfrak{m}^{Q_{n-1}})$. Inoltre, per il Lemma 3.2.3, $\pi_{n-1}(\mathfrak{m}^{Q_{n-1}}) \subseteq \mathfrak{m}^{Q_n}$.
Se ne conclude che $T_n(\mathfrak{m}) \subseteq \mathfrak{m}^{Q_n}$, come voluto. □

Osserviamo inoltre che per ogni n il polinomio $T_n(x)$ è monico.

Lemma 3.2.7. *Il polinomio $T_n(x) \in R[x]$ è monico di grado q^{n-1} per ogni intero $n \geq 1$.*

Dimostrazione. Procediamo per induzione su n.

`Caso base, n=1.` Abbiamo $T_1(x) = x$ e quindi la tesi è banalmente verificata.

`Passo induttivo.` Per definizione $T_n(x) = T_{n-1}(x)^q - m^{q^{n-1}-1}T_{n-1}(x)$. Applicando l'ipotesi induttiva osserviamo che

$$\begin{aligned} \deg(T_{n-1}(x)^q) &= q\deg(T_{n-1}(x)) = qq^{n-2} = q^{n-1} \\ &> q^{n-2} = \deg\left(m^{q^{n-1}-1}T_{n-1}(x)\right). \end{aligned}$$

Ne segue che $\deg(T_n(x)) = \deg(T_{n-1}(x)^q) = q^{n-1}$ e, sempre per ipotesi induttiva, che

$$T_n(x)[q^{n-1}] = (T_{n-1}(x)^q)[q^{n-1}] = (T_{n-1}(x)[q^{n-2}])^q = 1^q = 1$$

come voluto. □

Definizione 3.2.8. *Dato $n \geq 0$ definiamo $L_n = \prod_{i=1}^{\infty} T_i(x)^{\mu_i(n)} \in R[x]$.*

Si noti come la precedente definizione ha senso in quanto, per ogni n, $\mu_i(n) \neq 0$ per un numero finito di indici i.

Esempio 3.2.9. *Per quanto visto nell'Esempio 3.2.5 e nell'Esempio 3.1.3 abbiamo $L_0(x) = 1$, $L_1(x) = T_1(x) = x$, $L_2(x) = T_1(x)^2 = x^2$. Inoltre se $q > 2$ allora $L_3(x) = T_1(x)^3 = x^3$, mentre se $q = 2$ allora $L_3(x) = T_2(x) = x^2 - mx$.*

Dalla definizione dei polinomi L_n e dal Lemma 3.2.6 segue subito una cruciale proprietà di questi ultimi.

Lemma 3.2.10. *Per ogni intero $n \geq 1$, $L_n \in \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^n)$.*

Dimostrazione. Basta osservare che, per definizione di L_n e per il Lemma 3.2.6,

$$L_n(\mathfrak{m}) = \prod_{i=1}^{\infty} T_i(\mathfrak{m})^{\mu_i(n)} \subseteq \prod_{i=1}^{\infty} \mathfrak{m}^{Q_i \mu_i(n)} = \mathfrak{m}^{\sum_{i=1}^{\infty} \mu_i(n) Q_i} = \mathfrak{m}^n. \qquad \square$$

Dimostriamo ora un lemma sui polinomi L_n, che ne fornisce una definizione ricorsiva.

Lemma 3.2.11. *Per ogni $n \geq 1$ si ha, posto $j = \iota(n)$, che*

$$L_{n+1} = \begin{cases} xL_n & \text{se } j = 0 \\ L_n - m^{q^j - 1} L_{n+1-q^j} & \text{altrimenti.} \end{cases}$$

Dimostrazione. Abbiamo per il Lemma 3.1.12 che

$$\begin{aligned} L_{n+1} &= \prod_{i=1}^{\infty} T_i(x)^{\mu_i(n+1)} = T_{j+1}(x)^{\mu_{j+1}(n)+1} \prod_{i=j+2}^{\infty} T_i(x)^{\mu_i(n)} \\ &= T_{j+1}(x) \prod_{i=j+1}^{\infty} T_i(x)^{\mu_i(n)}. \end{aligned}$$

Se $j = 0$ si ha quindi

$$L_{n+1}(x) = T_1(x) \prod_{i=1}^{\infty} T_i(x)^{\mu_i(n)} = T_1(x) L_n(x) = x L_n(x).$$

Se invece $j > 0$, dato che $\mu_j(n) = q$ e $\mu_i(n) = 0$ per ogni $i < j$, si ottiene

$$T_j(x)^q L_{n+1} = T_{j+1}(x) \prod_{i=j}^{\infty} T_i(x)^{\mu_i(n)} = T_{j+1}(x) L_n(x) \qquad (*)$$

Inoltre si ha che

$$\begin{aligned} T_j(x) L_n(x) &= T_j(x) T_j(x)^q \prod_{i=j+1}^{\infty} T_i(x)^{\mu_i(n)} \\ &= T_j(x)^q L_{Q_j + \sum_{i=j+1}^{\infty} \mu_i(n) Q_i}(x) \\ &= T_j(x)^q L_{Q_j + n - q Q_j}(x) \\ &= T_j(x)^q L_{n+1-(Q_{j+1} - Q_j)}(x) \\ &= T_j(x)^q L_{n+1-q^j}(x). \qquad (**) \end{aligned}$$

Per definizione $T_{j+1}(x) = \pi_j(T_j(x)) = T_j(x)^q - m^{q^j - 1} T_j(x)$ e dunque

$$\begin{aligned} T_j(x)^q L_{n+1}(x) &= \left(T_j(x)^q - m^{q^j-1}T_j(x)\right) L_n(x) \\ &= T_j(x)^q L_n(x) - T_j(x)^q m^{q^j-1} L_{n+1-q^j}(x), \end{aligned}$$

dove abbiamo usato le identità (*) e (**) per la seconda eguaglianza.
Dato che, per il Lemma 3.2.7, $T_j(x)$ è monico, e quindi regolare in $R[x]$, questo implica

$$L_{n+1} = L_n - m^{q^j-1} L_{n+1-q^j}. \qquad \square$$

Definiamo degli ideali A_n e B_n in $R[x]$, dei quali mostreremo l'eguaglianza nel corso di questa sezione.

Definizione 3.2.12. *Per ogni intero $n \geq 1$ definiamo gli ideali di $R[x]$*

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

e

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

Esempio 3.2.13. *Per $n = 1$ abbiamo $D(1) - 1 = 0$ ed $E(D(1)) = E(1) = 1$, e quindi*

$$A_1 = (m^1 L_0, L_1) = (m, x) = B_1.$$

Per $n = 2$, $q > 2$ abbiamo $D(2) - 1 = 2 - 1 = 1$ ed $E(D(2)) = E(2) = 2$, e quindi

$$A_2 = (m^2 L_0, m^1 L_1, L_2) = (m^2, mx, x^2) = B_2.$$

Per $n = 2$, $q = 2$ abbiamo $D(2) - 1 = 2 - 1 = 1$ ma $E(D(2)) = E(2) = 3$, e quindi

$$A_2 = (m^2 L_0, m^1 L_1, L_3) = (m^2, mx, x^2 - mx) = (m^2, mx, x^2) = (m^2 L_0, m^1 L_1, L_2) = B_2.$$

Notiamo subito che, come conseguenza immediata del Lemma 3.2.10, $B_n \subseteq \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^n)$.

Lemma 3.2.14. *Per ogni intero $n \geq 1$, $B_n \subseteq \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^n)$.*

Dimostrazione. È sufficiente mostrare il contenimento per un insieme di generatori di B_n. Mostriamo quindi che per ogni $0 \leq i \leq n$ si ha $m^{n-i} L_i \in \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^n)$. Questo segue immediatamente dal Lemma 3.2.10, infatti $m^{n-i} L_i(\mathfrak{m}) \subseteq \mathfrak{m}^{n-i}\mathfrak{m}^i = \mathfrak{m}^n$. $\square$

Enunciamo e dimostriamo ora due lemmi analoghi che forniscono una definizione ricorsiva di A_n e B_n.

Lemma 3.2.15. *Per ogni $n \geq 2$, $B_n = (L_n) + \mathfrak{m} B_{n-1}$.*

Dimostrazione. Si osserva che per $n \geq 2$

$$\begin{aligned} B_n &= (m^n L_0,\, m^{n-1} L_1,\, \ldots,\, L_n) = (L_n) + (m)(m^{n-1} L_0,\, m^{n-2} L_1,\, \ldots,\, L_{n-1}) \\ &= (L_n) + \mathfrak{m} B_{n-1}. \end{aligned}$$

come voluto. $\square$

Lemma 3.2.16. *Per ogni $n \geq 2$, $A_n = (L_{E(D(n))}) + \mathfrak{m}^{n-E(D(n)-1)} A_{E(D(n)-1)}$.*

Dimostrazione. Si osserva che per ogni $n \geq 2$

$$\begin{aligned}
A_n &= (L_{E(D(n))}) + \left(\left\{ \mathfrak{m}^{n-E(i)} L_{E(i)} \,\middle|\, 0 \leq i \leq D(n)-1 \right\} \right) \\
&= (L_{E(D(n))}) + \left(\mathfrak{m}^{n-E(D(n)-1)} L_{E(D(n)-1)} \right) \\
&\quad + \left(\left\{ \mathfrak{m}^{n-E(i)} L_{E(i)} \,\middle|\, 0 \leq i \leq D(n)-2 \right\} \right) \\
&= (L_{E(D(n))}) + \mathfrak{m}^{n-E(D(n)-1)} \Bigg((L_{E(D(E(D(n)-1)))}) \\
&\qquad + \left(\left\{ \mathfrak{m}^{E(D(n)-1)-E(i)} L_{E(i)} \,\middle|\, 0 \leq i \leq D(E(D(n)-1))-1 \right\} \right) \Bigg) \\
&= (L_{E(D(n))}) + \mathfrak{m}^{n-E(D(n)-1)} A_{E(D(n)-1)}
\end{aligned}$$

dove nella terza eguaglianza abbiamo usato che, per definizione, $D(E(k)) = (D|_S \circ E)(k) = k$ per ogni $k \in \mathbb{N}$. □

Mostriamo alcuni ulteriori lemmi su A_n e B_n prima di poter finalmente dimostrare l'eguaglianza cercata.

Lemma 3.2.17. *Per ogni coppia di interi $n, k \geq 1$, $\mathfrak{m}^k B_n \subseteq B_{n+k}$.*

Dimostrazione. Procediamo per induzione forte su k.

`Caso base, k=1.` Si ha per il Lemma 3.2.15 che $B_{n+1} = (L_n) + \mathfrak{m} B_n \supseteq \mathfrak{m} B_n$, come voluto.

`Passo induttivo.` Applicando l'ipotesi induttiva prima per 1 e poi per $k-1$, otteniamo

$$\mathfrak{m}^k B_n = \mathfrak{m}^{k-1} \mathfrak{m} B_n \subseteq \mathfrak{m}^{k-1} B_{n+1} \subseteq B_{n+1+k-1} = B_{n+k}$$

come voluto. □

Lemma 3.2.18. *Per ogni intero $n \geq 1$ si ha che $\mathfrak{m} A_n \subseteq A_{n+1}$.*

Dimostrazione. Se n non è q-libero abbiamo che per il Lemma 3.1.15 $D(n) = D(n+1)$. Dunque per il Lemma 3.2.16 ed si ha che

$$\begin{aligned}
\mathfrak{m} A_n &= \left(m L_{E(D(n))} \right) + \mathfrak{m}^{n+1-E(D(n)-1)} A_{E(D(n)-1)} \\
&\subseteq \left(L_{E(D(n+1))} \right) + \mathfrak{m}^{n+1-E(D(n+1)-1)} A_{E(D(n+1)-1)} = A_{n+1}
\end{aligned}$$

come voluto.

Se invece n è q-libero si ha, sempre per il Lemma 3.1.15 ed il Lemma 3.1.21 che $E(D(n+1)-1) = E(D(n)+1-1) = E(D(n)) = n$.

Quindi, sempre per il Lemma 3.2.16, anche in tal caso

$$\begin{aligned}
A_{n+1} &= \left(L_{E(D(n+1))} \right) + \mathfrak{m}^{n+1-E(D(n+1)-1)} A_{E(D(n+1)-1)} \\
&= (L_{n+1}) + \mathfrak{m} A_n \supseteq \mathfrak{m} A_n.
\end{aligned}$$

come voluto. □

Lemma 3.2.19. *Per ogni intero k tale che $n \leq k \leq E(D(n))$ si ha $L_k \in B_n$.*

Dimostrazione. Procediamo per induzione forte su k.

`Caso base, k=n.` Abbiamo che $L_n \in B_n$ per definizione di B_n.

`Passo induttivo.` Essendo $E(D(n)) > k-1 \geq n$, per il Lemma 3.1.21, $k-1$ non è q-libero. Quindi per il Lemma 3.2.11 abbiamo che

$$L_k = L_{k-1} + m^{q^{\iota(k-1)}-1} L_{k-q^{\iota(k-1)}}.$$

Abbiamo che $L_{k-1} \in B_n$ per ipotesi induttiva, e lo stesso vale per $L_{k-q^{\iota(k-1)}}$ se $n \leq k - q^{\iota(k-1)}$. Se invece $k - q^{\iota(k-1)} < n$ si ha $m^{q^{\iota(k-1)}-1} L_{k-q^{\iota(k-1)}} \in B_n$ per definizione di B_n. Infatti, dato che $k-1 \geq n$, si ha che $m^{q^{\iota(k-1)}-1} L_{k-q^{\iota(k-1)}} = m^{k-n-1}(m^{n-k+q^{\iota(k-1)}} L_{k-q^{\iota(k)}}) \in B_n$. Si conclude in ambo i casi che $m^{q^{\iota(k-1)}-1} L_{k-q^{\iota(k-1)}} \in B_n$, e quindi $L_k \in B_n$. □

Lemma 3.2.20. *Per ogni intero $k \geq n \geq 1$ si ha $L_k \in A_n$.*

Dimostrazione. Dimostriamo prima il Lemma per $n \leq k \leq E(D(n))$, procedendo per induzione inversa su k.

`Caso base,` $k = E(D(n))$. Abbiamo $L_{E(D(n))} \in A_n$ per definizione di A_n.

`Passo induttivo.` Assumiamo che L_r sia in A_n per ogni $E(D(n)) \geq r > k$, e mostriamo che anche L_k vi appartiene, per $k \geq n$. Dato che $n \leq k < E(D(n))$ si ha che k non è q-libero per il Lemma 3.1.21. Infatti se lo fosse esso sarebbe maggiore o uguale del più piccolo numero q-libero maggiore o uguale ad n, che è $E(D(n))$.

Allora per il Lemma 3.2.11 $L_k = L_{k+1} + m^{q^{\iota(k)}-1} L_{k+1-q^{\iota(k)}}$.

Abbiamo che $L_{k+1} \in A_n$ per ipotesi induttiva.

Inoltre si ha che $k+1-q^{\iota(k)} \geq k < E(D(n))$, e che è q-libero per il Lemma 3.1.14. Quindi, per il Lemma 3.1.21, $k+1-q^{\iota(k)} < n$ (se fosse maggiore o uguale ad n sarebbe maggiore o uguale al più piccolo q-libero maggiore o uguale ad n, cioè ad $E(D(n))$), e sempre per lo stesso lemma $E(D(k+1-q^{\iota(k)})) = k+1-q^{\iota(k)}$.

Dunque

$$\begin{aligned} m^{q^{\iota(k)}-1} L_{k+1-q^{\iota(k)}} &= m^{k-n} m^{n-k-1+q^{\iota(k)}} L_{k+1-q^{\iota(k)}} \\ &= m^{k-n} m^{n-E(D(k+1-q^{\iota(k)}))} L_{E(D(k+1-q^{\iota(k)}))} \in A_n \end{aligned}$$

per definizione di A_n, dato che, per il Lemma 3.1.15, $k+1-q^{\iota(k)} < n \implies D(k+1-q^{\iota(k)}) < D(n)$.

Questo conclude la dimostrazione per il caso $k \leq E(D(n))$.

Mostriamo ora, per induzione forte su k, che il lemma vale anche per $k \geq E(D(n))$.

`Caso base,` $k = E(D(n))$. Come già osservato $L_{E(D(n))} \in A_n$ per definizione.

`Passo induttivo.` Sia $k > E(D(n))$. Se $k-1$ è q-libero, per il Lemma 3.2.11 si ha che $L_k = xL_{k-1} \in A_n$, per ipotesi induttiva.

Se invece $\iota(k-1) > 0$, per il Lemma 3.2.11 si ha che

$$L_k = L_{k-1} - m^{q^{\iota(k-1)}-1} L_{k-q^{\iota(k-1)}}.$$

Dato che $L_{k-1} \in A_n$ per ipotesi induttiva, per concludere è sufficiente mostrare che $m^{q^{\iota(k-1)}-1} L_{k-q^{\iota(k-1)}} \in A_n$. Procediamo ora per casi.

Se $n \leq k - q^{\iota(k-1)} \leq E(D(n))$ per quanto già dimostrato abbiamo che $L_{k-q^{\iota(k-1)}} \in A_n$ e quindi si conclude.

Anche se $k - q^{\iota(k-1)} > E(D(n))$ abbiamo, in questo caso per ipotesi induttiva forte, che $L_{k-q^{\iota(k-1)}} \in A_n$ e analogamente si conclude.

Rimane da esaminare solo il caso in cui $k - q^{\iota(k-1)} < n$. Osserviamo che $k - q^{\iota(k-1)} = (k-1) + 1 + q^{\iota(k-1)}$ è q-libero, per il Lemma 3.1.14, e che quindi per il Lemma 3.1.21 abbiamo che $E(D(k - q^{\iota(k-1)})) = k - q^{\iota(k-1)}$.

Quindi, in maniera del tutto analoga a quanto fatto nella dimostrazione del caso $k \leq E(D(n))$, abbiamo che

$$\begin{aligned} m^{q^{\iota(k-1)}-1} L_{k-q^{\iota(k-1)}} &= m^{k-1-n} m^{n-k+q^{\iota(k-1)}} L_{k-q^{\iota(k-1)}} \\ &= m^{k-1-n} m^{n-E(D(k-q^{\iota(k-1)}))} L_{E(D(k-q^{\iota(k-1)}))} \in A_n \end{aligned}$$

per definizione di A_n, dato che, per il Lemma 3.1.15, $k - q^{\iota(k-1)} < n$ implica $D(k - q^{\iota(k-1)}) < D(n)$. Questo conclude la dimostrazione del lemma. □

Possiamo ora finalmente dimostrare il principale risultato di questa sezione.

Teorema 3.2.21. *Per ogni intero $n \geq 1$ si ha $A_n = B_n$.*

Dimostrazione. Procediamo per induzione su n.

`Caso base, n=1.` Come visto nell'Esempio 3.2.13, $A_1 = B_1 = (x, m)$.

`Passo induttivo.` Dimostriamo per prima cosa che $A_n \subseteq B_n$.

Per il Lemma 3.2.16 si ha che $A_n = (L_{E(D(n))}) + \mathfrak{m}^{n-E(D(n)-1)} A_{E(D(n)-1)}$. Per ipotesi induttiva (che possiamo applicare essendo $E(D(n) - 1) < n$ per il Lemma 3.1.22), abbiamo allora che

$$A_n \subseteq (L_{E(D(n))}) + \mathfrak{m}^{n-E(D(n)-1)} B_{E(D(n)-1)} \subseteq (L_{E(D(n)}) + B_n$$

dove l'ultimo contenimento segue dal Lemma 3.2.17. Ma per il Lemma 3.2.19 anche $L_{E(D(n))} \in B_n$, quindi $A_n \subseteq B_n$.

Viceversa, per il Lemma 3.2.15, $B_n = (L_n) + \mathfrak{m}B_{n-1}$. Per ipotesi induttiva ed il Lemma 3.2.18, $\mathfrak{m}B_{n-1} = \mathfrak{m}A_{n-1} \subseteq A_n$. Inoltre, per il Lemma 3.2.20, $L_n \in A_n$, dunque si conclude che $B_n \subseteq A_n$.

Quindi $A_n = B_n$, come voluto. □

Concludiamo mostrando un lemma che segue dal teorema appena dimostrato e che ci permette di dare una struttura di $\overline{R}$-spazio vettoriale all'$R[x]$-modulo $A_n/(A_n \cap \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^{n+1}))$.

Lemma 3.2.22. *Per ogni intero $n \geq 1$, $(x, \mathfrak{m})A_n \subseteq A_{n+1}$.*

Dimostrazione. Abbiamo già che $\mathfrak{m}A_n \subseteq A_{n+1}$ per il Lemma 3.2.18.

Basta quindi dimostrare che

$$(x)A_n = (\{xm^{n-E(i)} L_{E(i)}, 0 \leq i \leq D(n) - 1\}) + (xL_{E(D(n))}) \subseteq A_{n+1}.$$

Se n è q-libero, per il Lemma 3.1.21, si ha $E(D(n)) = n$. Quindi, applicando i Lemmi 3.2.11 e 3.2.20, otteniamo $xL_{E(D(n))} = xL_n = L_{n+1} \in A_{n+1}$.

Se n non è q-libero, per il Lemma 3.1.15, $E(D(n+1)) = E(D(n))$ e quindi $xL_{E(D(n))} = xL_{E(D(n+1))} \in A_{n+1}$, per definizione.

Abbiamo quindi che $xL_{E(D(n))} \in A_{n+1}$ per ogni n. Basta ora mostrare che per qualsiasi i si ha $xm^{n-E(i)}L_{E(i)} \in A_{n+1}$. Dato che $E(i)$ è q-libero per ogni i per definizione di E, per il Lemma 3.2.11 si ha

$$xm^{n-E(i)}L_{E(i)} = m^{n-E(i)}L_{E(i)+1} \in B_{n+1} = A_{n+1},$$

dove abbiamo usato la definizione di B_{n+1} ed infine il Teorema 3.2.21 per l'ultima eguaglianza. □

Si ha quindi, per quanto appena dimostrato, il Teorema 3.2.21 ed il Lemma 3.2.14, che $(x, \mathfrak{m})A_n \subseteq A_n \cap A_{n+1} \subseteq A_n \cap \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^{n+1})$. Quindi $A_n/(A_n \cap \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^{n+1}))$ ammette una naturale struttura di $R/(x, \mathfrak{m}) \cong \overline{R}$-modulo, tale che, per ogni $r \in R$ ed ogni $f \in A_n$, $\overline{r}\overline{f} = \overline{rf}$.

3.3 Il caso DVR henseliano

In questa sezione assumiamo, laddove non specificato diversamente, che R sia un anello di valutazione discreta (DVR) henseliano con campo residuo finito.

Scopo della sezione sarà dimostrare che, sotto queste ipotesi su R, vale $A_n = B_n = \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^n)$.

Cominciamo col dimostrare un lemma tecnico che sarà di fondamentale importanza nelle dimostrazioni successive.

Lemma 3.3.1. *Sia $(R, \mathfrak{m})$ un DVR henseliano. Allora per ogni $r, b \in R$ esiste un $a \in R$ tale che per ogni $n \geq 1$, $T_{n+1}((r + am)m) = m^{q^n}T_n(bm)$.*

Dimostrazione. Dato che R è henseliano, per il Teorema 2.1.5, $x^q - x$ è un π-polinomio, e quindi, per il Teorema 2.1.6, induce una funzione surgettiva dalla classe laterale $r + \mathfrak{m} = r + (m)$ in $\mathfrak{m} = (m)$. Fissati r e b scegliamo allora a tale che $(r + am)^q - (r + am) = bm$ e dimostriamo che soddisfa la tesi.

Procediamo per induzione su n.

`Caso base, n=1` Osserviamo che per definizione

$$\begin{aligned} T_2((r + am)m) &= \pi_1(T_1((r + am)m)) = \pi_1((r + am)m) \\ &= (r + am)^q m^q - m^{q-1}(r + am)m \\ &= m^q\left((r + am)^q - (r + am)\right) = m^q bm = m^q T_1(bm). \end{aligned}$$

`Passo induttivo.` Per ipotesi induttiva si ha che per $n \geq 2$

$$\begin{aligned} T_{n+1}((r + am)m) &= \pi_n(T_n((r + am)m)) \\ &= \pi_n(m^{q^{n-1}}T_{n-1}(bm)) \\ &= \left(m^{q^{n-1}}T_{n-1}(bm)\right)^q - m^{q^n-1}m^{q^{n-1}}T_{n-1}(bm) \\ &= m^{q^n}\left(T_{n-1}(bm)^q - m^{q^{n-1}-1}T_{n-1}(bm)\right) \\ &= m^{q^n}\pi_{n-1}(T_{n-1}(bm)) = m^{q^n}T_n(bm). \end{aligned}$$

□

Possiamo ora dimostrare un lemma simile, che coinvolge però i polinomi L_n.

Lemma 3.3.2. *Sia $(R, \mathfrak{m})$ un DVR henseliano. Allora per ogni $r, b \in R$ esiste un $a \in R$ tale che per ogni $n \geq 0$, $L_n((r + am)m) = (r + am)^{\mu_1(n)}m^{D(n)}L_{n-D(n)}(bm)$.*

Dimostrazione. Per $n = 0$ la tesi del lemma è banalmente verificata, in quanto $L_0 = 1$ per definizione.

Per il Lemma 3.3.1, fissati b ed r, esiste un $a \in R$ tale che per ogni $n \geq 1$, $T_{n+1}((r + am)m) = m^{q^n} T_n(bm)$. Scelto tale a si ha quindi che per ogni $n \geq 1$,

$$\begin{aligned} L_n((r+am)m) &= \prod_{i=1}^{\infty} T_i((r+am)m)^{\mu_i(n)} \\ &= (r+am)^{\mu_1(n)} m^{\mu_1(n)} \prod_{i=2}^{\infty} (m^{q^{i-1}} T_{i-1}(bm))^{\mu_i(n)} \\ &= (r+am)^{\mu_1(n)} m^{\sum_{i=1}^{\infty} \mu_i(n) q^{i-1}} \prod_{i=1}^{\infty} T_i(bm)^{\mu_{i+1}(n)} \\ &= (r+am)^{\mu_1(n)} m^{D(n)} L_{\sum_{i=1}^{\infty} \mu_{i+1}(n) Q_i}(bm) \\ &= (r+am)^{\mu_1(n)} m^{D(n)} L_{n-D(n)}(bm) \end{aligned}$$

dove l'ultima eguaglianza segue dal Lemma 3.1.11. □

Siamo ora pronti per mostrare il principale risultato di questa sezione, dal quale l'uguaglianza cercata seguirà facilmente.

Teorema 3.3.3. *Per ogni intero $n \geq 1$, sia*

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

Allora $\overline{S_n} = \pi_{A_n \cap \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^{n+1})}(S_n)$, ossia l'immagine di S_n tramite la proiezione canonica di A_n su $A_n/(A_n \cap \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^{n+1}))$, è un sottoinsieme di $A_n/(A_n \cap \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^{n+1}))$ linearmente indipendente su $\overline{R}$.

Dimostrazione. Nella seguente dimostrazione poniamo $\overline{f} = \pi_{A_n \cap \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^{n+1})}(f)$ per qualsiasi $f \in R[x]$ e $\overline{r} = \pi_{\mathfrak{m}}(r)$ per qualsiasi $r \in R$.

Osserviamo che $S_n \subseteq A_n$ per ogni n, per definizione di A_n, e che quindi $\overline{S_n}$ è effettivamente un sottoinsieme di $A_n/(A_n \cap \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^{n+1}))$.

Osserviamo inoltre che ogni elemento di $\overline{R}$ si può scrivere come $\overline{r}$ con $r = 0$ o $r \in R \setminus \mathfrak{m} = R^*$.

Si procede ora per induzione forte su n.

`Caso base, n=1.` Abbiamo che $S_1 = \{x, m\}$. Per dimostrare la lineare indipendenza di $\overline{S_1}$, supponiamo che esistano a_1, a_2 tali che $\overline{a_1} \cdot \overline{x} + \overline{a_2} \cdot \overline{m} = \overline{0}$, dove possiamo assumere $a_1, a_2 \in R^* \cup \{0\}$, e mostriamo che $\overline{a_1} = \overline{a_2} = 0$. Si ha

$$\overline{a_1} \cdot \overline{x} + \overline{a_2} \cdot \overline{m} = \overline{0} \iff \overline{a_1 x + a_2 m} = \overline{0} \iff a_1 x + a_2 m \in \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^2).$$

In particolare $0 \in \mathfrak{m} \implies (a_1 x + a_2 m)(0) = a_2 m \in \mathfrak{m}^2$. Questo implica $a_2 = 0$, poiché se per assurdo avessimo $a_2 \in R^*$ ciò implicherebbe $m \in \mathfrak{m}^2$ e quindi $\mathfrak{m} = \mathfrak{m}^2$. Per Lemma di Nakayama questo a sua volta implicherebbe $\mathfrak{m} = 0$, ossia R campo. Ma ciò è assurdo dato che R è DVR (e quindi non un campo) per ipotesi.

Dunque $(a_1 x + a_2 m)(\mathfrak{m}) \in \mathfrak{m}^2 \iff a_1 \mathfrak{m} \in \mathfrak{m}^2$. Si conclude allora come sopra, per Nakayama, che anche $a_1 = 0$, e che quindi $\overline{S_1}$ è un sottoinsieme linearmente indipendente dell'$\overline{R}$-spazio vettoriale $A_1/(A_1 \cap \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^2))$.

`Passo induttivo.` Definiamo

$$D' = |S_n| = \begin{cases} D(n) & \text{se } \iota(n) = 0, \\ D(n) - 1 & \text{altrimenti .} \end{cases}$$

Analogamente a quanto fatto nel caso $n = 1$, per mostrare che $\overline{S_n}$ è linearmente indipendente, supponiamo $\sum_{i=0}^{D'} \overline{a_i} \cdot \overline{m^{n-E(i)} L_{E(i)}(x)} = \overline{0}$ con $a_i \in R^* \cup \{0\}$ per ogni i.

Sempre in maniera analoga a quanto fatto nel caso base, osserviamo che

$$\sum_{i=0}^{D'} \overline{a_i} \cdot \overline{m^{n-E(i)} L_{E(i)}(x)} = \overline{0} \iff \sum_{i=0}^{D'} a_i m^{n-E(i)} L_{E(i)}(x) \in \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^{n+1}).$$

Sia $f = \sum_{i=0}^{D'} a_i m^{n-E(i)} L_{E(i)}(x) \in R[x]$, e siano $r, b \in R$ due elementi di R qualsiasi. Allora, per il Lemma 3.3.2, esiste $a \in R$ tale che per ogni $n \geq 0$, $L_n((r+am)m) = (r+am)^{\mu_1(n)} m^{D(n)} L_{n-D(n)}(bm)$.

Dunque abbiamo che

$$\begin{aligned} f((r+am)m) &= \sum_{i=0}^{D'} a_i m^{n-E(i)} L_{E(i)}((r+am)m) \\ &= \sum_{i=0}^{D'} a_i (r+am)^{\mu_1(E(i))} m^{n-E(i)} m^{D(E(i))} L_{E(i)-D(E(i))}(bm) \\ &= \sum_{i=0}^{D'} a_i (r+am)^{\mu_1(E(i))} m^{n-(E(i)-i)} L_{E(i)-i}(bm), \end{aligned}$$

dove per l'ultima eguaglianza abbiamo usato che $D(E(i)) = (D|_S \circ E)(i) = i$ per ogni i.

Dato che $f \in \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^{n+1})$, si ha dunque

$$f((r+am)m) = \sum_{i=0}^{D'} a_i (r+am)^{\mu_1(E(i))} m^{n-(E(i)-i)} L_{E(i)-i}(bm) \in \mathfrak{m}^{n+1}.$$

Inoltre, per ogni k, $(r+am)^k \equiv r^k \mod \mathfrak{m}$, e quindi per ogni i esiste $m_i \in \mathfrak{m}$ tale che $(r + am)^{\mu_1(E(i))} = r^{\mu_1(E(i))} + m_i$.

Inoltre per ogni i abbiamo, per definizione di B_n, che $m^{n-(E(i)-i)} L_{E(i)-i} \in B_n$. Allora, per il Lemma 3.2.14, $m^{n-(E(i)-i)} L_{E(i)-i} \in \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^n)$.

Quindi $m^{n-(E(i)-i)} L_{E(i)-i}(bm) \in \mathfrak{m}^n$.

Allora si ha che

$$\begin{aligned} &\sum_{i=0}^{D'} a_i (r+am)^{\mu_1(E(i))} m^{n-(E(i)-i)} L_{E(i)-i}(bm) = \\ &\sum_{i=0}^{D'} a_i r^{\mu_1(E(i))} m^{n-(E(i)-i)} L_{E(i)-i}(bm) + \sum_{i=0}^{D'} m_i m^{n-(E(i)-i)} L_{E(i)-i}(bm) \in \mathfrak{m}^{n+1} \end{aligned}$$

e dato che per ogni i

$$m_i m^{n-(E(i)-i)} L_{E(i)-i}(bm) \in \mathfrak{m}\mathfrak{m}^{\mathfrak{n}} = \mathfrak{m}^{n+1}$$

otteniamo

$$\sum_{i=0}^{D'} a_i r^{\mu_1(E(i))} m^{n-(E(i)-i)} L_{E(i)-i}(bm) \in \mathfrak{m}^{n+1}.$$

Scrivendolo nella forma

$$m^{D(n)} \sum_{i=0}^{D'} a_i r^{\mu_1(E(i))} m^{(n-D(n))-(E(i)-i)} L_{E(i)-i}(bm)$$

otteniamo

$$\sum_{i=0}^{D'} a_i r^{\mu_1(E(i))} m^{(n-D(n))-(E(i)-i)} L_{E(i)-i}(bm) \in \mathfrak{m}^{n-D(n)+1}$$

dove abbiamo usato il fatto che, per il Lemma 3.1.23, $n - D(n) \geq E(i) - i$ per ogni $0 \leq i \leq D'$.

Dato che questo vale per ogni $b \in R$, e che ogni elemento di $\mathfrak{m}$ si scrive come bm per qualche $b \in R$, si ha quindi che

$$\sum_{i=0}^{D'} a_i r^{\mu_1(E(i))} m^{(n-D(n))-(E(i)-i)} L_{E(i)-i}(x) \in \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^{n-D(n)+1}).$$

Spezzando la sommatoria in $\left\lfloor \frac{D'}{q} \right\rfloor + 1$ parti, ognuna corrispondente agli indici $kq \leq i \leq kq + q - 1$ per $0 \leq k \leq \left\lfloor \frac{D'}{q} \right\rfloor$, e definendo $a_j = 0$ per $j > D'$, si ha che

$$\begin{aligned}
&\sum_{i=0}^{D'} a_i \, r^{\mu_1(E(i))} \, m^{(n-D(n))-(E(i)-i)} \, L_{E(i)-i}(x) \\
&= \sum_{i=0}^{q\left\lfloor \frac{D'}{q} \right\rfloor + q - 1} a_i \, r^{\mu_1(E(i))} \, m^{(n-D(n))-(E(i)-i)} \, L_{E(i)-i}(x) \\
&= \sum_{k=0}^{\left\lfloor \frac{D'}{q} \right\rfloor} \sum_{i=kq}^{kq+q-1} a_i \, r^{\mu_1(E(i))} \, m^{(n-D(n))-(E(i)-i)} \, L_{E(i)-i}(x).
\end{aligned}$$

Si noti che abbiamo usato il fatto che $q \left\lfloor \frac{D'}{q} \right\rfloor + q - 1 > q(\frac{D'}{q} - 1) + q - 1 = D' - 1$ e che quindi $q \left\lfloor \frac{D'}{q} \right\rfloor + q - 1 \geq D'$.

Per il Lemma 3.1.19, per ogni $kq \leq i < qk + q$, $E(i) - i = E(\left\lfloor \frac{i}{q} \right\rfloor) = E(k)$. Inoltre, sempre per $kq \leq i < kq + q$, per il Lemma 3.1.20 si ha che $\mu_1(E(i)) = i - q \left\lfloor \frac{i}{q} \right\rfloor = i - kq$. Si ha allora che

$$\begin{aligned}
&\sum_{k=0}^{\left\lfloor \frac{D'}{q} \right\rfloor} \sum_{i=kq}^{kq+q-1} a_i\, r^{\mu_1(E(i))}\, m^{(n-D(n))-(E(i)-i)}\, L_{E(i)-i}(x) \\
&\quad = \sum_{k=0}^{\left\lfloor \frac{D'}{q} \right\rfloor} \sum_{i=kq}^{kq+q-1} a_i r^{i-qk} m^{n-D(n)-E(k)} L_{E(k)}(x) \\
&\quad = \sum_{k=0}^{\left\lfloor \frac{D'}{q} \right\rfloor} \sum_{i=0}^{q-1} a_{i+qk} r^i m^{n-D(n)-E(k)} L_{E(k)}(x).
\end{aligned}$$

Denotiamo, per $0 \leq k \leq \left\lfloor \frac{D'}{q} \right\rfloor$, con $g_k(x)$ i polinomi $\sum_{i=0}^{q-1} a_{i+qk} x^i \in R[x]$. Abbiamo allora che

$$\begin{aligned}
&\sum_{k=0}^{\left\lfloor \frac{D'}{q} \right\rfloor} \left(\sum_{i=0}^{q-1} a_{i+qk} r^i \right) m^{n-D(n)-E(k)} L_{E(k)}(x) \\
&= \sum_{k=0}^{\left\lfloor \frac{D'}{q} \right\rfloor} g_k(r) m^{n-D(n)-E(k)} L_{E(k)}(x) \in \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^{n-D(n)+1})
\end{aligned}$$

per ogni $r \in R$. Notiamo inoltre che, per ogni k, $m^{n-D(n)-E(k)} L_{E(k)}(x) \in B_{n-D(n)} = A_{n-D(n)}$, per la definizione degli ideali B_m ed il Teorema 3.2.21. Si ha quindi, passando al quoziente, che, usando le notazioni fissate ad inizio dimostrazione,

$$\sum_{k=0}^{\left\lfloor \frac{D'}{q} \right\rfloor} \overline{g_k(r)} \cdot \overline{m^{n-D(n)-E(k)} L_{E(k)}(x)} = \overline{0} \in A_{n-D(n)}/(A_{n-D(n)} \cap \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^{n-D(n)+1})).$$

Mostriamo ora, procedendo per casi, che, per $0 \leq k \leq \left\lfloor \frac{D'}{q} \right\rfloor$, si ha

$$m^{n-D(n)-E(k)} L_{E(k)}(x) \in S_{n-D(n)}.$$

Poniamo $j = \iota(n)$.

Se $j = 0$, per definizione $\mu_i(n) < q$ per ogni i. Per il Lemma 3.1.11, $n - D(n)$ ha q-espansione $\sum_{i=0}^{t} \mu_{i+1}(n) Q_i$ per qualche $t \geq 0$. Pertanto anche $n - D(n)$ è q-libero, essendo i coefficienti della sua q-espansione strettamente minori di q.

Allora per il Lemma 3.1.19 ed il Lemma 3.1.21 si ha che

$$E\left(\left\lfloor \frac{D'}{q} \right\rfloor \right) = E(D') - D' = E(D(n)) - D(n) = n - D(n) = E(D(n - D(n))).$$

Se invece $j > 0$, si ha $D' = D(n) - 1$. Si ha inoltre che, per il Lemma 3.1.11, $n - D(n)$ ha q-espansione $\sum_{i=1}^{t} \mu_{i+1}(n) Q_i$ per qualche $t > j > 0$.

In particolare, se $j = 1$, $n - D(n) = \sum_{i=1}^{t} \mu_{i+1}(n)Q_i$ è q-libero, dato che $\mu_i(n) < q$ per ogni $i > j = 1$. Inoltre anche $n-1$ è q-libero: se infatti si avesse $\iota(n-1) > 0$, ne seguirebbe per il Lemma 3.1.13 che $1 = j \in \{0, 1 + \iota(n-1)\}$, che è chiaramente assurdo. Ne segue che $E(D(n)-1)$, che per il Lemma 3.1.22 è il massimo dei numeri q-liberi minori di n, è proprio $n-1$.

Si ha dunque che, applicando il Lemma 3.1.19, nel caso $j = 1$,

$$E\left(\left\lfloor \frac{D'}{q} \right\rfloor\right) = E(D') - D' = E(D(n)-1) - D(n) + 1 = n - D(n) = E(D(n - D(n))),$$

dove per l'ultima eguaglianza abbiamo di nuovo usato il Lemma 3.1.21.

Dunque per $j = 0, 1$ abbiamo che $n - D(n)$ è q-libero e inoltre, per la monotonia di E, si ha $k \leq D(n - D(n))$ per ogni $k \in \{0, \dots, \left\lfloor \frac{D'}{q} \right\rfloor\}$.

Allora, in questi due casi si ha

$$m^{n-D(n)-E(k)} L_{E(k)}(x) \in \{m^{n-D(n)-E(i)} L_{E(i)} \mid 0 \leq i \leq D(n - D(n))\} = S_{n-D(n)}$$

per ogni $0 \leq k \leq \left\lfloor \frac{D'}{q} \right\rfloor$.

Se $j > 1$ si ha, vista la q-espansione di $n - D(n)$ nel caso $j > 0$, che $\mu_{(j-1)}(n - D(n)) = q$, e pertanto nemmeno $n - D(n)$ è q-libero.

Applicando il Lemma 3.1.19 ed il Lemma 3.1.23 si ha inoltre che

$$E\left(\left\lfloor \frac{D'}{q} \right\rfloor\right) = E(D') - D' = E(D(n)-1) - (D(n)-1) \leq n - D(n).$$

Dato che $\mathrm{Im}(E) = \mathcal{F}_q$, $E\left(\left\lfloor \frac{D'}{q} \right\rfloor\right)$ è q-libero, quindi minore stretto di $n - D(n)$. Allora si ha $E\left(\left\lfloor \frac{D'}{q} \right\rfloor\right) \leq E(D(n - D(n)) - 1)$, che per il Lemma 3.1.22 è il più grande intero q-libero minore di $n - D(n)$.

Dunque per $j > 1$ abbiamo che $n - D(n)$ non è q-libero e inoltre, per la monotonia di E, si ha $k \leq D(n - D(n)) - 1$ per ogni $k \in \{0, \dots, \left\lfloor \frac{D'}{q} \right\rfloor\}$.

Allora anche nel caso $j > 1$ si ha

$$m^{n-D(n)-E(k)} L_{E(k)}(x) \in \{m^{n-D(n)-E(i)} L_{E(i)} \mid 0 \leq i \leq D(n - D(n)) - 1\} = S_{n-D(n)}$$

per ogni $0 \leq k \leq \left\lfloor \frac{D'}{q} \right\rfloor$.

Si ha allora che $\sum_{k=0}^{\left\lfloor \frac{D'}{q} \right\rfloor} \overline{g_k(r)} \cdot \overline{m^{n-D(n)-E(k)} L_{E(k)}(x)}$ è una combinazione lineare nulla di elementi di $\overline{S_{n-D(n)}}$. Per ipotesi induttiva forte si ha quindi che, per ogni k, $\overline{g_k(r)} = \overline{g_k}(\overline{r}) = \overline{0} \in R/\mathfrak{m}$ per ogni $r \in R$. Quindi $\overline{g_k} \in \mathcal{Z}(\overline{R})$, che per il Lemma 1.1.12 è $(x^q - x)$. Ne segue che $x^q - x | g_k(x)$, e, dato che $\deg(\overline{g_k}) \leq \deg(g_k) \leq q - 1$, questo implica $\overline{g_k} = 0$ per ogni k.

Dunque i coefficienti di $\overline{g_k}$, ossia $\overline{a_{kq+i}} \in \overline{R}$ per $0 \leq i \leq q-1$, sono nulli per ogni $0 \leq k \leq \left\lfloor \frac{D'}{q} \right\rfloor$, ossia $\overline{a_s} = \overline{0} \in \overline{R}$ per $0 \leq s \leq D'$.

Abbiamo quindi dimostrato che $\overline{S_n}$ è un insieme linearmente indipendente, come voluto. □

Concludiamo ora la sezione, mostrando che $A_n = B_n = \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^n)$ nel caso in cui R sia un DVR henseliano.

Teorema 3.3.4. *Per ogni $n \geq 1$, $A_n = \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^n)$.*

Dimostrazione. Procediamo per induzione su n.

`Caso base, n=1.` Per il Lemma 1.1.10 applicato per $S = \mathfrak{m} = J$, si ha $\overline{\mathcal{Z}(\mathfrak{m}, \mathfrak{m})} = \mathcal{Z}(\overline{\mathfrak{m}}, \overline{\mathfrak{m}}) = \mathcal{Z}(\{\overline{0}\}) \in \overline{R}[x]$. Per il caso base della dimostrazione del Lemma 1.1.11, si ha che $\mathcal{Z}(\{\overline{0}\}) = (x)$. Quindi, dato che ovviamente $\mathfrak{m}[x] \subseteq \mathcal{Z}(\mathfrak{m}, \mathfrak{m})$, si ha

$$\mathcal{Z}(\mathfrak{m}, \mathfrak{m}) = \pi^{-1}_{\mathfrak{m}[x]}(\overline{\mathcal{Z}(\mathfrak{m}, \mathfrak{m})}) = \pi_{\mathfrak{m}[x]}(x) = (x, \mathfrak{m}) = A_1,$$

come visto nell'Esempio 3.2.13.

`Passo induttivo.` Sia $n > 1$. Poniamo

$$D' = |S_{n-1}| = \begin{cases} D(n-1) & \text{se } \iota(n-1) = 0, \\ D(n-1) - 1 & \text{altrimenti .} \end{cases}$$

Per il Lemma 3.2.14 ed il Teorema 3.2.21, sappiamo già che $A_n \subseteq \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^n)$. Dimostriamo ora che $\mathcal{Z}(\mathfrak{m}, \mathfrak{m}^n) \subseteq A_n$.

Sia $f \in \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^n)$. Ovviamente si ha anche $f \in \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^{n-1}) = A_{n-1}$, dove l'ultima eguaglianza vale per ipotesi induttiva. Allora, per definizione di A_{n-1}, si ha che

$$f = a_{D(n-1)} L_{E(D(n-1))} + \sum_{i=0}^{D(n-1)-1} a_i m^{n-1-E(i)} L_{E(i)},$$

con $a_i \in R[x]$ per ogni i.

Poniamo $f_1 = \sum_{i=0}^{D'} a_i m^{n-1-E(i)} L_{E(i)}$.

Abbiamo che, se $n-1$ non è q-libero, $E(D(n-1)) = E(D(n))$, per il Lemma 3.1.15. Inoltre, per definizione, $D' = D(n-1) - 1$. Quindi in tal caso $a_{D(n-1)} L_{E(D(n-1))} = a_{D(n-1)} L_{E(D(n))} \in A_n$ e di conseguenza

$$f \in A_n \iff f_1 = f - a_{D(n-1)} L_{E(D(n-1))} \in A_n.$$

Inoltre dato che $f \in \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^n)$ per ipotesi e che, per il Lemma 3.2.14, $a_{D(n-1)} L_{E(D(n-1))} \in A_n \subseteq \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^n)$, si ha $f_1 \in \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^n)$. Osserviamo anche che $f_1 \in A_{n-1}$, dato che $f \in A_{n-1}$ e $a_{D(n-1)} L_{E(D(n-1))} \in A_{n-1}$.

Altrimenti, se $n-1$ è q-libero, si ha $D' = D(n-1)$ e quindi

$$f = \sum_{i=0}^{D'} a_i m^{n-1-E(i)} L_{E(i)} = f_1.$$

In ambo i casi basta dunque dimostrare che $f_1 \in A_n$ per concludere, e sappiamo che $f_1 \in A_{n-1} \cap \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^n)$.

Applicando la mappa di proiezione $\pi_{A_{n-1} \cap \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^n)} : A_{n-1} \to A_{n-1}/(A_{n-1} \cap \mathcal{Z}(\mathfrak{m}, \mathfrak{m}^n))$ otteniamo, usando le stesse notazioni del Teorema 3.3.3,

$$\overline{f_1} = \overline{0} = \sum_{i=0}^{D'} \overline{a_i}\, \overline{m^{n-1-E(i)} L_{E(i)}}.$$

Applicando il Teorema 3.3.3 a questa combinazione lineare a coefficienti in $\overline{R}$ di elementi di $\overline{S_{n-1}}$, concludiamo $\pi_{(x,\mathfrak{m})}(a_i) = \overline{0} \in \overline{R}$, e quindi $a_i \in (x, \mathfrak{m})$ per ogni i.

Osserviamo che per ogni i, $a_i m^{n-1-E(i)} L_{E(i)} \in A_{n-1}$, per definizione di A_{n-1}. Si ha quindi, applicando il Lemma 3.2.22, che

$$a_i m^{n-1-E(i)} L_{E(i)} \in (x, \mathfrak{m}) A_{n-1} \subseteq A_n$$

per ogni i. Ne segue che $f_1 \in A_n$ e questo, come già osservato, conclude. □

3.4 Da DVR al caso locale ad ideali principali

Scopo di quest'ultima sezione è estendere i risultati della precedente al caso di un anello locale finito R con ideale massimale principale $\mathfrak{m} = (m)$.

Ricordiamo innanzitutto la definizione di *caratteristica* di un anello R.

Definizione 3.4.1. *Dati R un anello ed $n \in \mathbb{N}$ un intero, definiamo n_R l'elemento $\underbrace{1+1+\cdots+1}_{n \text{ volte}}$. Diciamo che R* ha caratteristica *m, con $m > 0$, se $m_R = 0$ e $n_R \neq 0$ per ogni intero $0 < n < m$.*

Ricordiamo ora alcuni fatti di base sulla caratteristica di anelli finiti e locali.

Lemma 3.4.2. *Sia R anello finito, allora* $\mathrm{char}(R) > 0$.

Lemma 3.4.3. *Sia R un campo con* $\mathrm{char}(R) > 0$. *Allora* $\mathrm{char}(R) = p$ *con $p \in \mathbb{N}$ primo.*

Lemma 3.4.4. *Sia $(R, \mathfrak{m})$ anello locale con* $\mathrm{char}(R) > 0$, *e sia $p = \mathrm{char}(R/\mathfrak{m})$. Allora* $\mathrm{char}(R) = p^k$ *per $k \geq 1$.*

Introduciamo ora il concetto di v-anello, che sarà cruciale in questa sezione.

Definizione 3.4.5. *Un anello D si dice v-anello se è un dominio locale noetheriano completo e di caratteristica zero, con ideale massimale (p_D) e campo residuo $D/(p_D)$ di caratteristica p, per qualche $p \in \mathbb{N}$ primo.*

In particolare si ha quindi che un v-anello è un campo od un DVR.

Dimostriamo ora due semplici lemmi sugli anelli locali noetheriani con ideale massimale principale.

Lemma 3.4.6. *Sia R un anello locale noetheriano con ideale massimale principale $\mathfrak{m} = (m)$. Allora per ogni $r \in R \setminus \{0\}$ esiste $u \in R^*$ e $k \in \mathbb{N}$ tali che $r = um^k$.*

Dimostrazione. Fissato un qualunque elemento $r \in R$, supponiamo per assurdo di non poterlo scrivere in nessun modo come um^k, per $u \in R^*$ e $k \in \mathbb{N}$. Chiaramente tale r non potrebbe essere un'unità, e sarebbe dunque in (m).

Costruiamo allora una successione $(r_k)_{k \in \mathbb{N}} \subseteq R$ ponendo $r_0 = r$ ed r_{k+1} tale che $r_k = r_{k+1} m$ per ogni $k \geq 0$.

Fare ciò è possibile: sia per assurdo k il minimo intero tale che r_k non si scrive come $r_{k+1} m$ per qualche $r_{k+1} \in R$. Avremmo allora

$$r_0 = r_1 m = r_2 m m = r_2 m^2 = \cdots = r_k m^k,$$

con $r_k \in R \setminus (m) = R^*$, contraddicendo la supposta impossibilità di scrivere r in tale forma.

Consideriamo allora la catena ascendente di ideali

$$(r_0) \subseteq (r_1) \subseteq (r_2) \dots (r_m) \subseteq (r_{m+1}) \dots$$

Ogni contenimento è stretto in quanto se fosse $r_k = ur_{k+1}$ per qualche $u \in R^*$ e qualche intero k, ne seguirebbe $ur_{k+1} = r_{k+1}m$, ossia $r_{k+1}(m-u) = 0$. Dato che $m-u$ è invertibile in R^*, si avrebbe quindi $r_{k+1} = 0$. Ma questo implicherebbe

$$r = r_{k+1}m^{k+1} = 0,$$

che contraddice le ipotesi.

L'esistenza di tale catena però contraddice la noetherianità di R. □

Lemma 3.4.7. *Sia R un anello locale noetheriano con ideale massimale principale $\mathfrak{m} = (m)$. Allora ogni ideale $I \subseteq R$ è della forma $I = (m^k)$ per qualche $k \geq 0$.*

Dimostrazione. Per noetherianità possiamo scrivere $I = (r_1, \dots, r_n)$ per qualche $r_1, \dots, r_n \in R$. Applicando il Lemma 3.4.6 a ciascuno degli r_i si ha allora che

$$I = (u_1 m^{k_1}, \dots, u_n m^{k_n}) = (m^{k_1}, \dots, m^{k_n}) = (m^{\min_i k_i}),$$

dove $u_1, \dots, u_n \in R^*$ e $k_1, \dots, k_n \in \mathbb{N}$, e questo conclude. □

Richiamiamo infine due semplici lemmi sull'anello delle serie formali $R[[x]]$. Per una loro dimostrazione si veda ad esempio [8, Cap. 7].

Lemma 3.4.8. *Se R è noetheriano anche l'anello delle serie formali $R[[x]]$ lo è.*

Lemma 3.4.9. *Sia $R[[x]]$ l'anello delle serie formali con coefficienti in R. Allora la serie formale $\sum_{i=0}^{\infty} r_i x^i$ è invertibile in $R[[x]]$ se e solo se r_0 è invertibile, e quindi è irriducibile se r_0 è irriducibile.*

Come immediato corollario abbiamo il seguente lemma.

Lemma 3.4.10. *Se R è un anello locale con ideale massimale $\mathfrak{m}$, l'anello delle serie formali $R[[x]]$ è un anello locale con ideale massimale $(x, \mathfrak{m})$.*

Concludiamo i richiami sugli anelli di serie formali ricordando un ulteriore lemma sulle serie formali a coefficienti in un DVR. Per una sua dimostrazione si veda ad esempio [2, Pag. 13, Es. B].

Lemma 3.4.11. *Se R è un campo DVR, il suo anello delle serie formali $R[[x]]$ è un UFD.*

Ricordiamo inoltre un noto fatto sui moduli finitamente generati su anelli I-adicamente completi, del quale ci serviremo in seguito. Per una sua dimostrazione si veda ad esempio [7, Lemma 10.96.11].

Lemma 3.4.12. *Sia R un anello ed I un suo ideale. Allora, se R è I-adicamente completo, ed M è un R-modulo finitamente generato tale che $\bigcap_{i=0}^{\infty} I^i M = (0)$, anche M è I-adicamente completo.*

Richiamiamo infine due teoremi classici, il Teorema di Intersezione di Krull ed il Teorema di Struttura di Cohen, quest'ultimo nel caso di caratteristica finita. Per delle loro dimostrazioni si vedano rispettivamente [4, Thm. 14.2] e [1, Thm. 12].

Teorema 3.4.13. *Se R è un anello noetheriano locale con ideale massimale $\mathfrak{m}$ e M è un R-modulo finitamente generato, allora $\bigcap_{n=0}^{\infty} \mathfrak{m}^n M = 0$.*

Teorema 3.4.14. *Sia R un anello completo locale con ideale massimale $\mathfrak{m} = (m_1, \dots, m_n)$ finitamente generato da n elementi e campo residuo $R/\mathfrak{m}$ di caratteristica $p > 0$. Allora esistono un v-anello D, un ideale $I \subseteq D[[t_1, \dots, t_n]]$ ed un isomorfismo $\xi : D[[t_1, \dots, t_n]]/I \to R$ tale che $\xi(\overline{t_i}) = m_i$ per ogni i. Inoltre D ha campo residuo isomorfo ad $R/\mathfrak{m}$.*

Possiamo ora finalmente dimostrare il Lemma chiave di questa sezione.

Lemma 3.4.15. *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 $\psi : T/(t^n) \to R$ tale che $\psi(\bar{t}) = m$.*

Dimostrazione. Sia $p > 0$ la caratteristica di $R/\mathfrak{m}$.

Applicando il Teorema 3.4.14 (un anello finito è infatti banalmente completo) per $n = 1$, si ha che esiste un v-anello D con ideale massimale (p_D), un ideale $I \in D[[t]]$, ed un isomorfismo $\xi : D[[t]]/I \to R$ tale che $\xi(\bar{t}) = m$. Sia $\pi_I : D[[t]] \to D[[t]]/I$ la proiezione al quoziente.

Allora $\tau = \xi \circ \pi_I : D[[t]] \to R$ è una mappa surgettiva tale che $\tau(t) = m$. Essendo un omomorfismo di anelli si ha inoltre che

$$\tau(p_D) = \tau(\underbrace{1 + 1 + \cdots + 1}_{p \text{ volte}}) = \underbrace{1 + 1 + \cdots + 1}_{p \text{ volte}} = p_R.$$

Se $p_D = 0$, D è un campo e quindi $D[[t]]$ è un DVR con ideale massimale (t), ed è ovviamente (t)-adicamente completo (quindi completo come anello locale). Inoltre $D[[t]]/(t) \cong D \cong D/(p_D) \cong R/\mathfrak{m}$, e quindi il campo residuo di $D[[t]]$ ha cardinalità q.

Mostriamo ora che, in questo caso, $\ker(\tau) = (t^n)$.

Per il Lemma 3.4.7 esiste l tale che $\ker(\tau) = (t^l)$. Si ha che $\tau(t^n) = \tau(t^n) = m^n = 0$, e quindi $(t^n) \subseteq \ker(\tau) = (t^l)$. D'altra parte $\tau(t^{n-1}) = \tau(t^{n-1}) = m^{n-1} \neq 0$, per definizione di indice di nilpotenza, e quindi $(t^{n-1}) \nsubseteq \ker(\tau) = (t^l)$. Ne segue che $\ker(\tau) = (t^n)$, come voluto.

Allora, per primo teorema di omomorfismo, esiste un isormofismo di anelli $\psi : D[[t]]/(t^n) \to R$ tale che $\psi(\bar{t}) = \tau(\bar{t}) = m$. Abbiamo quindi trovato, nel caso $p_D = 0$, un anello ed un morfismo che soddisfano le ipotesi del lemma.

Consideriamo ora il caso $p_D \neq 0$. In tal caso il v-anello D non è un campo, ed è quindi un DVR.

Per il Lemma 3.4.6, se $p_R \neq 0$ esistono $v \in R^*$ e $j \in \mathbb{N}$ tali che $p_R = vm^j$. Se $p_R = 0$ tali v e j esistono comunque: prendiamo infatti in tal caso $v = 1$ e $j = n$. Per surgettività di τ esiste un elemento $u \in D[[t]]$ tale che $\tau(u) = v$.

Per il Lemma 3.4.4, $\mathrm{char}(R) = p^k$ per qualche $k \geq 1$. Allora $(p^k)_R = p_R^k = 0$, quindi $p_R \in \mathcal{N}(R)$ ed in particolare $p_R \notin R^*$. Da ciò segue che $j \geq 1$.

Per definizione di ξ si ha inoltre che $\tau(ut^j - p_D) = vm^j - p_R = 0$. Quindi $(ut^j - p_D) \subseteq \ker(\tau)$, e dunque, per primo teorema di omomorfismo, esiste un omomorfismo $\lambda : D[[t]]/(ut^j - p_D) \to R$ tale che $\lambda \circ \pi_{(ut^j - p)} = \tau$, dove con $\pi_{(ut^j - p_D)} : D[[t]] \to D[[t]]/(ut^j - p_D)$ denotiamo la proiezione canonica.

Poniamo $T = D[[t]]/(ut^j - p_D)$ e mostriamo che T è un DVR completo. Osserviamo subito che per il Lemma 3.4.10, $D[[t]]$ è un anello locale con ideale massimale (p_D, t). Ne segue che il suo quoziente T è anch'esso anello locale, con ideale massimale $(\overline{p_D}, \bar{t}) = (\overline{ut^j}, \bar{t}) = (\bar{t})$. Inoltre T è noetheriano, essendo quoziente di $D[[t]]$ che è noetheriano per il Lemma 3.4.8.

Ovviamente $D[[t]]$ è (t)-adicamente completo. Inoltre $\bigcap_{i=0}^{\infty}(t)^n T = \bigcap_{i=0}^{\infty}(\bar{t})^n$. Dato che T è noetheriano, essendo quoziente di noetheriano, questa intersezione è 0 per il Teorema 3.4.13. Per il Lemma 3.4.12 questo implica che T, che è banalmente finitamente generato come $D[[t]]$-modulo, è (t)-adicamete

completo come $D[[t]]$-modulo. Questo implica che è anche $(\bar{t})$-adicamente completo dato che, per ogni n, $t^n T = (\bar{t})^n T$. Quindi T è anche completo come anello locale.

Non rimane che mostrare che T è un dominio, e per fare ciò basta mostrare che $(ut^j - p_D)$ è primo in $D[[t]]$. Per il Lemma 3.4.11 $D[[t]]$ è UFD, e quindi la primalità di $(ut^j - p_D)$ equivale alla irriducibilità di $ut^j - p_D$ in $D[[t]]$. Per il Lemma 3.4.9 questa è implicata a sua volta alla irriducibilità di p_D in D. Supponiamo allora di avere due elementi non nulli in D, d_1 e d_2, tali che $d_1 d_2 = p_D$. Denotando con ν_D la valutazione discreta associata all'ideale massimale (p_D), si ha quindi $\nu_D(d_1) + \nu_D(d_2) = \nu_D(p_D) = 1$, che implica che uno fra $\nu_D(d_1)$ e $\nu_D(d_2)$ sia nullo, e che quindi uno fra d_1 e d_2 sia invertibile. Quindi p_D è irriducibile e T è un dominio, come voluto.

Inoltre, per terzo teorema d'omomorfismo,

$$\begin{aligned} T/(\bar{t}) = T/(\bar{t}, \overline{p_D}) &= \big(D[[t]]/(ut^j - p_D)\big)\big/\big((t, p_D)/(ut^j - p_D)\big) \\ &\cong D[[t]]/(t, p_D) \cong (D[[t]]/t)\big/\big((p_D, t)/(t)\big) \cong D/p_D \cong R/\mathfrak{m}. \end{aligned}$$

In particolare allora $|T/(\bar{t})| = |R/\mathfrak{m}| = q$.

Mostriamo ora che $\ker(\lambda) = (\bar{t}^n)$.

Per il Lemma 3.4.7 esiste l tale che $\ker(\lambda) = (\bar{t}^l)$. Si ha che $\lambda(\bar{t}^n) = \tau(t^n) = m^n = 0$, e quindi $(\bar{t}^n) \subseteq \ker(\lambda) = (\bar{t}^l)$. D'altra parte $\lambda(\bar{t}^{n-1}) = \tau(t^{n-1}) = m^{n-1} \neq 0$, per definizione di indice di nilpotenza, e quindi $(\bar{t}^{n-1}) \nsubseteq \ker(\lambda) = (\bar{t}^l)$. Ne segue che $\bar{t}^l \mid \bar{t}^n$, e che quindi $l \leq n$, ma che $\bar{t}^l \nmid \bar{t}^{n-1}$, e quindi $l > n - 1$. Dunque $l = n$, e $\ker(\lambda) = (\bar{t}^n)$, come voluto.

Allora, per primo teorema di omomorfismo, esiste un isomorfismo di anelli $\psi : T/(\bar{t}^n) \to R$ tale che $\psi(\bar{t} + (\bar{t}^n)) = \lambda(\bar{t}) = m$.

Abbiamo quindi trovato, anche nel caso $p_D \neq 0$, un anello T ed un morfismo ψ che soddisfano la tesi del lemma. □

D'ora in poi, per ogni noetheriano locale Z con ideale massimale principale e campo residuo finito, denotiamo con L_n^Z ed A_n^Z rispettivamente gli elementi e gli ideali di $Z[x]$ ottenuti applicando le costruzioni della Sezione 3.2 nell'anello Z.

Enunciamo e dimostriamo ora due semplici lemmi, che saranno poi usati per passare, mediante il lemma appena dimostrato ed il Lemma 1.1.10, dai risultati visti sui DVR ad una descrizione generale di $\mathcal{Z}(R)$ per un generico anello R locale finito con ideale principale massimale.

Lemma 3.4.16. *Siano T ed R due anelli locali con ideali massimali principali $(t) \subseteq T$ ed $(m) \subseteq R$, e con campi residui $R/(m)$ ed $T/(t)$ finiti e della stessa cardinalità q. Sia inoltre $\psi : T \to R$ un omomorfismo di anelli tale che $\psi(t) = m$, e sia $\delta = (-)[x](\psi) : T[x] \to R[x]$ la mappa indotta da ψ tramite il funtore $(-)[x]$. Si ha allora che, per ogni $n \geq 0$, $\delta(L_n^T) = L_n^R$, e quindi $\delta(A_n^T) = A_n^R$.*

Dimostrazione. Procediamo per induzione su n.

`Caso base, n=0.` Abbiamo $L_0^T = 1 = L_0^R$ per l'Esempio 3.2.9.

`Passo induttivo.` Se n è q-libero, per il Lemma 3.2.11 abbiamo che (per qualunque anello) $L_{n+1} = xL_n$, e quindi, usando l'ipotesi induttiva, che

$$\delta(L_{n+1}^T) = \delta(xL_n^T) = x\delta(L_n^T) = xL_n^R = L_{n+1}^R.$$

Altrimenti abbiamo, sempre per il Lemma 3.2.11 e l'ipotesi induttiva, che

$$\delta(L_{n+1}^T) = \delta(L_n^T - t^{q^{\iota(n)}-1} L_{n+1-q^{\iota(n)}}) = L_n^R - m^{q^{\iota(n)}-1} L_{n+1-q^{\iota(n)}}^R = L_{n+1}^R.$$

In ambo i casi questo conclude la dimostrazione del passo induttivo, e quindi del lemma. □

Lemma 3.4.17. *Siano T e R due anelli, sia $\psi : T \to R$ un isomorfismo, e sia $\delta = (-)[x](\psi) : T[x] \to R[x]$ la mappa indotta da ψ tramite il funtore $(-)[x]$.*

Allora per ogni sottoinsieme $S \subseteq T$ ed ogni ideale $J \subseteq T$, si ha che $\delta(\mathcal{Z}(S, J)) = \mathcal{Z}(\psi(S), \psi(J))$.

Dimostrazione. Sia f un generico polinomio di $R[x]$, con $f(x) = \sum_{i=0}^{d} f_i x^i$.

Basta osservare che per definizione

$$f \in \mathcal{Z}(\psi(S), \psi(J)) \iff \sum_{i=0}^{d} f_i \psi(s)^i = \psi(\sum_{i=0}^{d} \psi^{-1}(f_i) s^i) \in \psi(J) \text{ per ogni } s \in S.$$

Essendo ψ un isomorfismo questo è vero se e solo se $\sum_{i=0}^{d} \psi^{-1}(f_i) s^i \in J$ per ogni $s \in S$, ovvero se e solo se $\sum_{i=0}^{d} \psi^{-1}(f_i) x^i \in \mathcal{Z}(S, J)$.

Anche δ, essendo indotta da un isomorfismo, è un isomorfismo, e quindi abbiamo che

$$\begin{aligned} f \in \mathcal{Z}(\psi(S), \psi(J)) &\iff \sum_{i=0}^{d} \psi^{-1}(f_i) x^i \in \mathcal{Z}(S, J) \\ &\iff \delta\left(\sum_{i=0}^{d} \psi^{-1}(f_i) x^i\right) = \sum_{i=0}^{d} f_i x^i = f \in \delta(\mathcal{Z}(S, J)) \end{aligned}$$

ed abbiamo quindi concluso. □

Possiamo ora finalmente dare una descrizione esplicita di $\mathcal{Z}(\mathfrak{m})$ nel caso in cui R sia un generico anello locale finito con ideale principale. Si noti che questo è ad esempio il caso di $R = \mathbb{Z}/p^n\mathbb{Z}$, per p primo ed $n \geq 1$.

Teorema 3.4.18. *Sia R un anello locale finito con ideale massimale principale $\mathfrak{m} = (m)$ avente indice di nilpotenza n. Allora $\mathcal{Z}(\mathfrak{m}) = A_n$.*

Dimostrazione. Siano T e ψ come nel Lemma 3.4.15.

Poniamo $\delta = (-)[x](\psi) : (T/(t^n))[x] \to R[x]$ la funzione indotta da ψ tramite il funtore $(-)[x]$. Denotiamo con $\bar{t}$ l'immagine di t, generatore dell'ideale massimale di T, tramite la proiezione $T \to T/(t^n)$.

Allora per il Lemma 3.4.17,

$$\delta(\mathcal{Z}((\bar{t})) = \mathcal{Z}(\psi((\bar{t}))) = \mathcal{Z}((m)) = \mathcal{Z}(\mathfrak{m}).$$

Per il Lemma 1.1.10 si ha $\overline{\mathcal{Z}((t), (t^n))} = \mathcal{Z}((\bar{t}))$.

Quindi, mettendo insieme questi due fatti, ed applicando il Teorema 3.3.4 al DVR completo (e quindi henseliano) T, si ha che

$$\mathcal{Z}(\mathfrak{m}) = \delta(\overline{\mathcal{Z}((t), (t^n))}) = \delta(\pi_{(t^n)[x]}(A_n^T)).$$

Osserviamo che la mappa $\pi_{(t^n)[x]}$ è la mappa indotta tramite il funtore $(-)[x]$ dalla mappa $\pi_{(t^n)} : T \to T/(t^n)$. Dato che quest'ultima manda (t) in $(\bar{t})$, e che per il terzo teorema d'omomorfismo $(T/(t^n))/(\bar{t}) \cong T/(t)$ e quindi i campi residui di T e $T/(t^n)$ hanno la medesima cardinalità q, possiamo applicare il Lemma 3.4.16 per concludere che $\pi_{(t^n)[x]}(A_n^T) = A_n^{T/(t^n)}$.

Applicando di nuovo il Lemma 3.4.16, stavolta con la mappa $\psi : T/(t^n) \to R$, che ne soddisfa le ipotesi per costruzione, si ottiene

$$\mathcal{Z}(\mathfrak{m}) = \delta(A_n^{T/(t^n)}) = A_n^R. \qquad \square$$

Possiamo combinare questo risultato, valido per gli anelli locali finiti con ideale massimale principale, col Teorema 2.3.1 ed il Teorema 3.2.21, ottenendo immediatamente una caratterizzazione in termini di generatori di $\mathcal{Z}(R)$.

Corollario 3.4.19. *Sia $(R, \mathfrak{m})$ un anello locale finito con ideale massimale principale $\mathfrak{m} = (m)$ avente indice di nilpotenza n, e sia $f(x) \in R[x]$ un qualsiasi π-polinomio. Allora*

$$\mathcal{Z}(R) = (\{m^{n-E(i)} L_{E(i)}(f(x)) \mid 0 \leq i \leq D(n)-1\}) + (L_{E(D(n))}(f(x))) = (\{m^{n-i} L_i(f(x)) \mid 0 \leq i \leq n\}).$$

Con una semplice osservazione aggiuntiva, possiamo fare lo stesso per il Teorema 2.1.1, ottenendo invece una descrizione esplicita della decomposizione primaria minimale di $\mathcal{Z}(R)$.

Corollario 3.4.20. *Siano $(R, \mathfrak{m})$ un anello locale finito con ideale massimale principale $\mathfrak{m} = (m)$ avente indice di nilpotenza n, e sia $\{c_1, \ldots, c_q\}$ un insieme di rappresentanti per le classi laterali di $\mathfrak{m}$. Per ogni i sia $\psi_i : R[x] \to R[x]$ l'automorfismo di anelli tale che $\psi_i(x) = x - c_i$. Allora $\bigcap_{i=1}^q \psi_i(A_n)$ è una decomposizione primaria minimale di $\mathcal{Z}(R)$.*

Dimostrazione. Osserviamo che, per ogni $1 \leq i \leq q$ e per ogni polinomio $f(x) \in R[x]$, si ha

$$\begin{aligned} f(x) \in \mathcal{Z}(c_i + \mathfrak{m}) &\iff f(c_i + m) = 0 \quad \text{per ogni } m \in \mathfrak{m} \\ &\iff f(x + c_i) \in \mathcal{Z}(\mathfrak{m}) \\ &\iff \psi_i(f(x + c_i)) = f(x) \in \psi_i(\mathcal{Z}(\mathfrak{m})) \end{aligned}$$

dove l'ultima doppia implicazione vale perché ϕ_i è un automorfismo.

Quindi $\mathcal{Z}(c_i + \mathfrak{m}) = \psi_i(\mathcal{Z}(\mathfrak{m}))$, ed il corollario segue immediatamente combinando i Teoremi 2.1.1 e 3.4.18. $\square$

Concludiamo la trattazione con un semplice esempio che ci permette di illustrare come ora ci è effettivamente possibile calcolare in maniera esplicita gli ideali $\mathcal{Z}(R)$ e $\mathcal{Z}(\mathfrak{m})$ nel caso in cui R sia locale finito con ideale massimale principale.

Esempio 3.4.21. *Sia $R = \mathbb{Z}/p^n\mathbb{Z}$, con $p \geq n$ primo.*

La cardinalità q del campo residuo $R/pR \cong \mathbb{Z}/p\mathbb{Z}$ è p, mentre l'indice di nilpotenza dell'ideale massimale pR è n.

Dato che $p \geq n$, ogni intero i tale che $0 \leq i \leq n$ ha come q-espansione semplicemente iQ_1. Quindi per ogni $0 \leq i \leq n$ si ha, per definizione degli L_i, che $L_i = (T_1(x))^i = x^i$.

Quindi $\mathcal{Z}(\mathfrak{m})$ (che coincide con A_n per il Teorema 3.2.21) è in questo caso

$$(\{p^{n-i}x^i, 0 \leq i \leq n\}) = (p, x)^n.$$

Scegliendo un qualsiasi π-polinomio f si conclude allora, per il Teorema 2.3.1, che

$$\mathcal{Z}(R) = (\{p^{n-i}f^i, 0 \leq i \leq n\}) = (p, f)^n.$$

Se invece n è, ad esempio, fra $p+1$ e $2p+1$, estremi inclusi, si ha che ogni $p+1 \leq i \leq n$ ha q-espansione $i = (i-p-1)Q_1 + Q_2$. In tal caso abbiamo quindi due tipi di generatori $p^{n-i}L_i$ dell'ideale $B_n = \mathcal{Z}(\mathfrak{m})$: quelli della forma $p^{n-i}x^i$, come prima, per gli indici i minori o uguali a p, e quelli invece della forma

$$p^{n-i}(T_1(x))^{i-p-1}T_2(x) = p^{n-i}x^{i-p-1}(x^p - p^{p-1}x)$$

per $p+1 \leq i \leq n$.

In maniera del tutto analoga si può, computando q-espansioni di n, ottenere forme esplicite (progressivamente più complesse) per i generatori degli ideali $\mathcal{Z}(\mathfrak{m})$ per ogni n. Precomponendoli poi con un qualsiasi π-polinomio f questi forniscono un insieme di generatori per $\mathcal{Z}(R)$.

Bibliografia

[1] I. S. Cohen. On the structure and ideal theory of complete local rings. *Trans. Am. Math. Soc.*, 59:54–106, 1946.

[2] Wolfgang Krull. Über die Zerlegung der Hauptideale in allgemeinen Ringen. *Math. Ann.*, 105:1–14, 1931.

[3] Hideyuki Matsumura. *Commutative ring theory. Transl. from the Japanese by M. Reid.*, volume 8 of *Camb. Stud. Adv. Math.* Cambridge etc.: Cambridge University Press, paperback ed. edition, 1989.

[4] Masayoshi Nagata. *Local rings. Corr. reprint of the orig. ed. 1962.* 1975.

[5] Mark W. Rogers and Cameron Wickham. Polynomials inducing the zero function on local rings. *Int. Electron. J. Algebra*, 22:170–186, 2017.

[6] Mark W. Rogers and Cameron Wickham. Polynomials inducing the zero function on chain rings. *J. Algebra Appl.*, 17(8):16, 2018. Id/No 1850160.

[7] The Stacks Project Authors. *Stacks Project.* `https://stacks.math.columbia.edu`, 2018.

[8] Oscar Zariski and Pierre Samuel. *Commutative algebra. Vol. II. Reprint of the 1958-1960 Van Nostrand edition*, volume 29 of *Grad. Texts Math.* Springer, Cham, 1976.