Algebra Commutativa

Alessio Borzì

Indice

Capitolo 1

Anelli e Ideali

1.1 Introduzione

Gli anelli che verranno trattati nel seguito sono anelli commutativi unitari.
Assumeremo sempre che per ogni omomorfismo di anelli $f : A \to B$ valga $f(1_A) = 1_B$.
La scrittura $I \trianglelefteq A$ vuol dire che I è un ideale di A.
Dati due ideali I, J di A abbiamo che la loro intersezione $I \cap J$, la loro somma

$$I + J = \{i + j : i \in I, j \in J\}$$

e il loro prodotto

$$IJ = \left\{ \sum_{k=1}^{n} i_k j_k : i_k \in I, j_k \in J, n \geq 1 \right\}$$

sono ancora ideali di A. Inoltre si verifica facilmente che $IJ \subseteq I \cap J$.
Dato un ideale I di A possiamo considerare l'ideale quoziente A/I è formato dalle classi laterali di I. Per ogni ideale I di A esiste una corrispondenza biunivoca tra gli ideali di A contenenti I e gli ideali di A/I tramite $J \to \pi(J)$, dove $\pi : A \to A/I$ è la proiezione canonica.

Definizione 1.1.1. *Un elemento $a \in A$ si dice **nilpotente** se esiste un intero $n \geq 1$ tale che $a^n = 0$.*

Ovviamente ogni elemento nilpotente è anche un divisore dello zero, non vale invece il viceversa. Ad esempio in $k[x, y]/(xy)$, con k campo, l'elemento x è un divisore dello zero ma non è un elemento nilpotente.

Definizione 1.1.2. *Un anello A si dice **ridotto** se è privo di elementi nilpotenti non nulli.*

Definizione 1.1.3. *Un elemento $a \in A$ è **invertibile** se esiste $b \in A$ tale che $ab = 1$.*

Dall'ultima definizione segue che A è un campo se ogni elemento di $A \backslash \{0\}$ è invertibile.

Proposizione 1.1.4. *Per un anello A sono equivalenti*

1. *A è un campo.*

2. *Gli unici ideali di A sono (0) e $(1) = A$.*

3. *Ogni omomorfismo non nullo $f : A \to B$ è iniettivo.*

Dimostrazione.

$(1) \Rightarrow (2)$ Sia I un ideale di A. Se I contiene un elemento non nullo $i \in I$ allora, dato che i è invertibile, abbiamo che esiste $x \in A$ tale che $ix = 1 \in I$, da cui dalla legge di assorbimento $I = A$. Altrimenti $I = (0)$.

$(2) \Rightarrow (3)$ $\ker f$ è un ideale di A non nullo, petanto $\ker f = (0)$, cioè f è iniettivo.

$(3) \Rightarrow (1)$ Sia $x \in A$ un elemento non invertibile, consideriamo $\pi : A \to A/(x)$. π è un omomorfismo non nullo quindi è iniettivo, pertanto $\ker \pi = (x) = (0)$, cioè $x = 0$.

$\square$

Definizione 1.1.5. *Un ideale M di A è **massimale** se è massimale nell'insieme parzialmente ordinato degli ideali propri di A rispetto all'inclusione.*
*Un ideale P di A è **primo** se da $ab \in P$ segue $a \in P$ o $b \in P$.*

Proposizione 1.1.6.
M è massimale $\Leftrightarrow A/M$ è un campo.
P è primo $\Leftrightarrow A/P$ è un dominio.

Dalla precedente dimostrazione segue che ogni ideale massimale è anche primo, ma non vale il viceversa, infatti basta considerare l'ideale nullo in $\mathbb{Z}$, esso è primo in quanto $\mathbb{Z}$ è un dominio ma non è massimale.

Lemma 1.1.7. *Dato un ideale P di A, sono equivalenti*

- *P è primo*
- *$IJ \subseteq P \Rightarrow I \subseteq P$ oppure $J \subseteq P$ per ogni $I, J \trianglelefteq A$*

Dimostrazione.

$\Rightarrow$ Se $I \nsubseteq P$ sia $i \in I \setminus P$, per ogni $j \in J$ si ha $ij \in P$, $i \notin P \Rightarrow j \in P$, da cui $J \subseteq P$.

$\Leftarrow$ Se $ij \in P$ allora $(i)(j) \subseteq P$ da cui $i \in (i) \subseteq P$ oppure $j \in (j) \subseteq P$.

$\square$

Dato $f : A \to B$ un omomorfismo di anelli non è detto che l'immagine tramite f di un ideale di A sia un ideale di B, in generale esso sarà un ideale di $f(A)$.

Proposizione 1.1.8. *Dato $f : A \to B$ un omomorfismo di anelli se J è un ideale di B allora $f^{-1}(J)$ è un ideale di A. Inoltre se J è primo lo è anche $f^{-1}(J)$.*

Dimostrazione. Siano $x, y \in f^{-1}(J)$, allora $f(x - y) = f(x) - f(y) \in J$, da cui $x - y \in f^{-1}(J)$. Sia $a \in A$ allora $f(ax) = f(a)f(x) \in J$, da cui $ax \in f^{-1}(J)$.
Se J è primo supponiamo che $xy \in f^{-1}(J)$, allora $f(xy) = f(x)f(y) \in J$ da cui segue $f(x) \in J$ oppure $f(y) \in J$ cioè $x \in f^{-1}(J)$ opoure $y \in f^{-1}(J)$. $\square$

Osserviamo che la contro immagine di un ideale massimale non è in generale un ideale massimale. Ad esempio consideriamo l'immersione $\phi : \mathbb{Z} \to \mathbb{Q}$. L'ideale (0) è un ideale massimale di $\mathbb{Q}$ ma $\phi^{-1}((0)) = (0)$ non è massimale in $\mathbb{Z}$.

Lemma 1.1.9 (Lemma di Zorn)**.** *Sia $(\Sigma, \leq)$ un inseme p.o. con $\Sigma \neq \emptyset$. Se ogni catena ammette un maggiorante allora Σ ha elementi massimali.*

Definizione 1.1.10. *Sia A un anello. Un sottoinsieme $S \subseteq A$ si dice* ***parte moltiplicativa*** *se*

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

Lemma 1.1.11 (Krull)**.** *Siano S una parte moltiplicativa di A, J un ideale di A tale che $J \cap S = \emptyset$ e sia*

$$\Sigma = \{I \trianglelefteq A : J \subseteq I, I \cap S = \emptyset\}.$$

Allora esiste un ideale primo P massiamle in Σ rispetto all'inclusione.

Dimostrazione. Osserviamo che $J \in \Sigma \neq \emptyset$. Sia $\{I_\lambda\}_{\lambda \in \Lambda}$ una catena in $(\Sigma, \subseteq)$. Proviamo che $I = \bigcup_{\lambda \in \Lambda} I_\lambda$ è un elemento di Σ. Siano $x, y \in I$, allora esistono $\alpha, \beta \in \Lambda$ tali che $x \in I_\alpha$, $y \in I_\beta$. Dato che $(I_\lambda)_{\lambda \in \Lambda}$ è un catena possiamo suppore $I_\alpha \subseteq I_\beta$, quindi $x, y \in I_\beta$ da cui $x - y \in I_\beta \subseteq I$. Sia adesso $a \in A$, allora $ax \in I_\alpha \subseteq I$. Ciò prova che I è un ideale di A. Inoltre $J \subseteq I_\lambda$ per ogni $\lambda \in \Lambda$, quindi $J \subseteq \bigcup_{\lambda \in \Lambda} I_\lambda = I$; per assurdo sia $s \in I \cap S = \bigcup_{\lambda \in \Lambda} I_\lambda \cap S$, quindi esiste $\alpha \in \Lambda$ tale che $s \in I_\alpha \cap S = \emptyset$, assurdo. Pertanto $I \cap S = \emptyset$. Ne segue che $I \in \Sigma$ ed è un maggiorante per la catena $(I_\lambda)_{\lambda \in \Lambda}$, da cui applicando il Lemma di Zorn sappiamo che Σ ha elementi massimali.
Sia P massimale in Σ e siano $a, b \notin P$, allora dalla massimalità di P si ha

$$J \subseteq P \subsetneq P + (a) \Rightarrow \exists s \in (P + (a)) \cap S$$

$$J \subseteq P \subsetneq P + (b) \Rightarrow \exists t \in (P + (b)) \cap S$$
$$\Rightarrow st \in (P + (ab)) \cap S,$$

da cui $ab \notin P$, altrimenti si avrebbe $st \in P \cap S = \emptyset$. Ciò prova che P è primo. □

Teorema 1.1.12 (Krull)**.** *Se A è un anello commutativo unitario allora*

1. *A possiede ideali massimali.*
2. *Ogni ideale I di A è contenuto in un ideale massimale.*
3. *Ogni elemento non invertibile $x \in A$ è contenuto in un ideale massimale.*

Dimostrazione.

1. Basta applicare il lemma precedente con $S = \{1\}$ e $J = (0)$.
2. Basta applicare il lemma precedente con $S = \{1\}$ e $J = I$.
3. Basta applicare il punto precedente con $I = (x)$.

$\square$

Definizione 1.1.13. *Un anello A è detto **locale** se ha un solo ideale massimale. É detto **semilocale** se ha un numero finito di ideali massimali.*

Proposizione 1.1.14. *Sia M un ideale proprio di A.*

1. *A è locale con ideale massimale $M \Leftrightarrow A \setminus M = U(A) = \{a \in A : a \text{ invertibile}\}$.*

2. *Se M è massimale con $1 + M \subseteq U(A)$ allora A è locale con ideale massimale M.*

Dimostrazione.

1. $\Rightarrow$ Sia $x \in A \setminus M$, se x fosse non invertibile allora (x) sarebbe un ideale proprio di A, quindi avremmo $(x) \subseteq M$ da cui $x \in M$, assurdo.

   $\Leftarrow$ Sia I un ideale proprio di A e $x \in I$. Dato che I è un ideale proprio x è non invertibile, quindi $x \in A \setminus U(A) = M$, da cui $I \subseteq M$.

2. Sia $x \in A \setminus M$. L'ideale $(x) + M$ contiene propriamente M quindi deve coincidere con A. Allora $1 \in A = (x) + M$ da cui $1 = \lambda x + m$ per qualche $m \in M$ e $\lambda \in A$. Ne segue che $\lambda x = 1 - m \in 1 + M \subseteq U(A)$, pertanto x è invertibile. Ciò prova che $A \setminus M \subseteq U(A)$, dato che l'altra inclusione è ovvia segue che $A \setminus M = U(A)$. Adesso basta applicare il punto 1.

$\square$

Definizione 1.1.15. *Sia I un ideale di A. Il **radicale** di I è l'insieme*

$$r(I) = \sqrt{I} = \{a \in A : a^n \in I, n \geq 1\}.$$

*Il **nilradicale** di A è il radicale dell'ideale nullo $N_A = \sqrt{(0)}$, cioè l'insieme formato da tutti gli elementi nilpotenti.*

Proposizione 1.1.16. *Il radicale di un ideale I è anch'esso un ideale.*

Dimostrazione. Siano $x, y \in \sqrt{I}$. Per ipotesi esistono $n, m \geq 1$ tali che $x^n, y^m \in I$. Si ha

$$(x-y)^{n+m-1} = \sum_{i=0}^{n+m-1} \binom{n+m-1}{i} x^i y^{n+m-1-i},$$

dato che non può verificarsi contemporaneamente $i < n, n+m-1-i < m \Leftrightarrow i > n-1$ allora ogni termine della precedente somma sta in I, da cui $x - y \in \sqrt{I}$. Infine per ogni $a \in A$ si ha $(ax)^n = a^n x^n \in I$ da cui $ax \in \sqrt{I}$. $\square$

Teorema 1.1.17. *Il nilradicale di A coincide con l'intersezione di tutti gli ideali primi di A*

$$N_A = \bigcap_{P \text{ primo}} P$$

Dimostrazione.

- $\subseteq$ Siano $x \in N_A$ e P un ideale primo di A. Per ipotesi esiste un $n \geq 1$ tale che $x^n = 0 \in P$ da cui segue facilmente $x \in P$.

- $\supseteq$ Sia $x \in A \setminus N_A$, proviamo che esiste un ideale primo P tale che $x \notin P$. Sia $S = \{x^n : n \in \mathbb{N}\} = \{1, x, x^2, \ldots\}$, S è una parte moltiplicativa di A, inoltre dato che $x \notin N_A$ allora $(0) \cap S = \emptyset$. Allora applicando il Lemma 1.1.11 con $J = (0)$ abbiamo che esiste un ideale primo P tale che $P \cap S = \emptyset$, in particolare $x \notin P$.

$\square$

Corollario 1.1.18. *Il radicale di un ideale I coincide con l'intersezione di tutti gli ideali primi contenenti I*

$$\sqrt{I} = \bigcap_{\substack{P \text{ primo} \\ P \supseteq I}} P.$$

Dimostrazione. Sia $\pi : A \to A/I$. Proviamo che $\sqrt{I} = \pi^{-1}(N_{A/I})$. Sia $x \in \sqrt{I}$, allora esiste $n \geq 1$ tale che $x^n \in I$, da cui $\pi(x)^n = \pi(x^n) = x^n + I = I = 0_{A/I}$, quindi $\pi(x) \in N_{A/I} \Rightarrow x \in \pi^{-1}(N_{A/I})$. Viceversa sia $x \in \pi^{-1}(N_{A/I})$, quindi $\pi(x) = x+I \in N_{A/I}$, allora esiste $n \geq 1$ tale che $(x+I)^n = 0_{A/I}$, cioè $x^n \in I$, da cui $x \in \sqrt{I}$.
In base a quanto appena dimostrato si ha

$$\sqrt{I} = \pi^{-1}(N_{A/I}) = \pi^{-1}\left(\bigcap_{P \subseteq A/I \text{ primo}} P\right) = \bigcap_{P \subseteq A/I \text{ primo}} \pi^{-1}(P) = \bigcap_{\substack{P \subseteq A \text{ primo} \\ P \supseteq I}} P,$$

l'ultima uguaglianza segue dal fatto che la controimmagine tramite π di un ideale primo di A/I è un ideale primo di A contenente I. $\square$

Definizione 1.1.19. *Si dice **radicale di Jacobson** di A l'ideale*

$$\mathcal{J}(A) = \bigcap_{M \text{ massimale}} M.$$

Proposizione 1.1.20. *$x \in \mathcal{J} \Leftrightarrow 1 - xy$ è invertibile in A per ogni $y \in A$.*

Dimostrazione.

- $\Rightarrow$ Sia $x \in \mathcal{J}$, supponiamo per assurdo che $\exists y \in A$ tale che $1 - xy$ non è invertibile. Allora $1 - xy$ è contenuto in qualche ideale massimale M,inoltre $x \in \mathcal{J} \subseteq M$, da cui

  $$1 = (1 - xy) + xy \in M$$

  che è assurdo.

- $\Leftarrow$ Per assurdo supponiamo che esista un ideale massimale M tale che $x \notin M$. Allora dalla massimalità di M abbiamo $(x) + M = A$, da cui $1 \in A = (x) + M$, quindi esistono $m \in M$ e $y \in A$ tali che

  $$1 = m + xy \Rightarrow m = 1 - xy \in M$$

  che è una contraddizione in quanto M non può avere elementi invertibili.

$\square$

Proposizione 1.1.21. *Se I, J, L sono ideali di A allora*

1. $I(J+L) = IJ + IL$.
2. $(I \cap J) + (I \cap L) \subseteq I \cap (J+L)$.
3. $IJ \subseteq I \cap J$.
4. $(I+J)(I \cap J) \subseteq IJ$.
5. $IJ = I \cap J$ *se* $I + J = A$ *(cioè se I e J sono **coprimi**).*

Dimostrazione.

1. Sia $x \in I(J+L)$, allora esistono $i_k \in I, j_k \in J, l_k \in L$ tali che
$$x = \sum_{k=1}^{n} i_k(j_k + l_k) = \sum_{k=1}^{n} i_k j_k + \sum_{k=1}^{n} i_k l_k \in IJ + IL.$$
Viceversa osserviamo che
$$IJ + IL \subseteq I(J+L) + I(J+L) \subseteq I(J+L).$$
2. Basta osservare che
$$(I \cap J) + (I \cap L) \subseteq J + L$$
$$(I \cap J) + (I \cap L) \subseteq I.$$
Osserviamo che non vale il viversa, infatti siano $A = k[x,y]$, $I = (x+y)$, $J = (x)$, $L = (y)$. Allora $x + y \in I \cap (J+L) \setminus ((I \cap J) + (I \cap L))$.
3. Segue facilmente dalla proprietà di assorbimento degli ideali.
4. $(I+J)(I \cap J) \subseteq I(I \cap J) + J(I \cap J) \subseteq IJ + JI \subseteq IJ$.
5. Segue da 3 e 4.

$\square$

Se $A_1, A_2, \ldots, A_n$ sono anelli, possiamo dotare il loro prodotto cartesiano
$$A = \prod_{i=1}^{n} A_i$$
di struttura di anello effettuando la somma e il prodotto componente per componente. Sia A un anello e $I_1, I_2, \ldots, I_n$ ideali di A. Consideriamo l'applicazione
$$\varphi : A \to \prod_{i=1}^{n} A/I_i$$
con $\varphi(x) = (x + I_1, x + I_2, \ldots, x + I_n)$, allora si ha il seguente

Teorema 1.1.22 (Teorema cinese del resto)**.**

1. *Se* I_i, I_j *sono coprimi per ogni* $i \neq j$ *allora* $\prod_{i=1}^{n} I_i = \bigcap_{i=1}^{n} I_i$.
2. φ *è suriettiva* $\Leftrightarrow$ I_i, I_j *sono coprimi per ogni* $i \neq j$.
3. $\ker \varphi = \bigcap_{i=1}^{n} I_i$.
4. φ *è iniettiva* $\Leftrightarrow \bigcap_{i=1}^{n} I_i = (0)$.

Dimostrazione.

1. Procediamo per induzione su n. Il caso $n = 2$ segue dalla proposizione precedente. Supponiamo che il teorema si vero per $n-1$ e dimostriamolo per n. Dall'ipotesi induttiva abbiamo
$$J = \prod_{i=1}^{n-1} I_i = \bigcap_{i=1}^{n-1} I_i.$$
Dal momento che $I_i + I_n = A$ abbiamo n equazioni del tipo $x_i + y_i = 1$ con $x_i \in I_i$ e $y_i \in I_n$, allora
$$\prod_{i=1}^{n} x_i = \prod_{i=1}^{n} (1 - y_i) \equiv 1 \pmod{I_n}.$$
Pertanto $J + I_n = A$ e quindi
$$\prod_{i=1}^{n} I_i = JI_n = J \cap I_n = \bigcap_{i=1}^{n} I_i.$$

2. $\Rightarrow$ Senza perdita di generalità proviamo l'asserto per I_1 e I_2. Sia $(1, 0, \ldots, 0) \in \prod_{i=1}^{n} A/I_i$, dalla suriettività di φ abbiamo che esiste $x \in A$ tale che $x \in 1 + I_1$ e $x \in I_2$, quindi esiste $i_1 \in I_1$ tale che $x = 1 + i_1$ da cui $1 = -i_1 + x \in I_1 + I_2 = (1)$.

   $\Leftarrow$ Dato che $(a_1, a_2, \ldots, a_n) = \sum_{i=1}^{n} a_i \underline{e}_i$ e φ è un omomorfismo, basta provare che per ogni $i \in \{1, \ldots, n\}$ esiste un elemento $x \in A$ tale che $\varphi(x) = \underline{e}_i$. Infatti, fissato $i \in \{1, \ldots, n\}$, per ogni $j \neq i$ abbiamo $1 \in A = I_j + I_i$ quindi esistono $x_j \in I_j$ e $y_j \in I_i$ tali che $x_j + y_j = 1$, da cui
$$x = \prod_{k \neq i} x_k = \prod_{k \neq i} (1 - y_k) \equiv 1 \pmod{I_i}$$
con $x \in \prod_{k \neq i} I_k = \bigcap_{k \neq i} I_k$. Pertanto $\varphi(x) = \underline{e}_i$.

3. $x \in \ker \varphi \Leftrightarrow \varphi(x) = \underline{0} \Leftrightarrow x \in I_i \quad \forall i \in \{1, \ldots, n\} \Leftrightarrow x \in \bigcap_{i=1}^{n} I_i$.

4. Segue dal punto precedente.

$\square$

Proposizione 1.1.23 (Prime avoidance lemma)**.**

1. *Siano $I_1, I_2, \dots, I_n$ ideali di A, e sia P un ideale primo.*
   Se $P \supseteq \bigcap_{i=1}^n I_i$ allora esiste $i \in \{1, \dots, n\}$ tale che $P \supseteq I_i$.
   Se $P = \bigcap_{i=1}^n I_i$ allora esiste $i \in \{1, \dots, n\}$ tale che $P = I_i$.

2. *Siano $P_1, P_2, \dots, P_n$ ideali primi di A e I un ideale quasiasi.*
   Se $I \subseteq \bigcup_{i=1}^n P_i$ allora esiste $i \in \{1, \dots, n\}$ tale che $I \subseteq P_i$.

Dimostrazione.

1. Nel primo caso, per assurdo $P \not\supseteq I_i$ per ogni $i \in \{1, \dots, n\}$ allora esistono $x_i \in I_i \setminus P$. Si ha
$$\prod_{i=1}^n x_i \in \prod_{i=1}^n I_i \subseteq \bigcap_{i=1}^n I_i \subseteq P,$$
ma P è primo, quindi esiste $i \in \{1, \dots, n\}$ tale che $x_i \in P$, assurdo.
Nel caso in cui si ha anche l'uguaglianza basta osservare che
$$I_i \subseteq P = \bigcap_{i=1}^n I_i \subseteq I_i.$$

2. Procediamo per induzione su n. Per $n = 1$ non c'è nulla da dimostrare. Supponiamo la tesi vera per $n-1$. Per assurdo $I \not\subseteq P_i$ per ogni $i \in \{1, \dots, n\}$. Allora dall'ipotesi induttiva segue che
$$I \not\subseteq \bigcup_{j \neq i} P_j \quad \forall i \in \{1, \dots, n\}.$$
Pertanto esistono $y_i \in I \setminus \bigcup_{j \neq i} P_j$. Se per qualche i abbiamo $y_i \notin P_i$ allora $I \not\subseteq \bigcup_{i=1}^n P_i$, contro l'ipotesi. Dunque $y_i \in P_i$ per ogni $i \in \{1, \dots n\}$. Adesso osserviamo che $\prod_{j \neq i} y_j \notin P_i$, altrimenti esisterebbe $j \neq i$ tale che $y_j \in P_i$, dato che P_i è primo. Inoltre ovviamente $\prod_{j \neq i} y_j \in P_k$ per ogn $k \neq i$. Consideriamo quindi
$$z = \sum_{i=1}^n \prod_{j \neq i} y_j \notin P_i \quad \forall i \in \{1, \dots, n\}$$
quindi $z \in I \setminus \bigcup_{i=1}^n P_i$, assurdo.

□

Definizione 1.1.24. *Siano I, J ideali di A. Si definisce*
$$(I : J) = \{x \in A : xJ \subseteq I\}.$$
Se I è l'ideale nullo allora poniamo
$$\mathrm{Ann}(J) = (0 : J).$$
Con queste definizioni abbiamo
$$Z(A) = \{\textit{divisori dello zero di } A\} = \bigcup_{x \in A} \mathrm{Ann}(x).$$

Definizione 1.1.25. *Se $f : A \to B$ è un omomorfismo di anelli e I è un ideale di A si definisce* ***estensione*** *dell'ideale I il più piccolo ideale di B contenente $f(I)$, cioè l'intersezione di tutti gli ideali di B che contengono $f(I)$, esplicitamente*

$$I^e = f(I)B = \left\{ \sum_{k=1}^{n} f(i_k)b_k : i_k \in I, b_k \in B \right\}.$$

Se invece J è un ideale di B di definisce ***contrazione*** *di J l'ideale $J^c = f^{-1}(J)$.*

Proposizione 1.1.26. *Per ogni ideale I di A e J di B abbiamo*

1. $I \subseteq I^{ec}$
2. $J \supseteq J^{ce}$
3. $I^e = I^{ece}$
4. $J^c = J^{cec}$

Dimostrazione.

1. $f(I) \subseteq I^e \Rightarrow I \subseteq f^{-1}(f(I)) \subseteq f^{-1}(I^e) = I^{ec}$.
2. $f(f^{-1}(J)) \subseteq J \Rightarrow J^{ce} = (f^{-1}(J))^e \subseteq J$.
3. Dal punto 1 si ha $I \subseteq I^{ec} \Rightarrow I^e \subseteq I^{ece}$. Dal punto 2 si ha $(I^e) \supseteq (I^e)^{ce}$.
4. Dal punto 1 si ha $J^c \subseteq (J^c)^{ec}$. Dal punto 2 si ha $J \supseteq J^{ce} \Rightarrow J^c \supseteq J^{cec}$.

□

Capitolo 2

Moduli

Definizione 2.0.1. *Sia A un anello. Un insieme M è un A-**modulo** se $(M,+)$ è un gruppo abeliano e esiste un'operazione $\cdot : A \times M \to M$ tale che $\forall a, b \in A$, $\forall m, n \in M$ si ha*

1. $a \cdot (m+n) = a \cdot m + a \cdot n$
2. $(a+b) \cdot m = a \cdot m + b \cdot m$
3. $a \cdot (b \cdot m) = (ab) \cdot m$
4. $1 \cdot m = m$

O in modo equivalente se esiste un omomorfismo di anelli $\varphi : A \to E(M)$ (dove $(E(M), +, \circ)$ è l'anello degli omomorfismi da M in M come gruppo abeliano). In questo caso l'oprea-zione è definita come $a \cdot m = (\varphi(a))(m)$.

Osserviamo che gli ideali di un anello, con l'operazione di moltiplicazione usuale, sono A-moduli.
Osserviamo che se k è un campo le due nozioni di k-spazio vettoriale e k-modulo coincidono.
Ogni gruppo abeliano $(G,+)$ con la seguente operazione

$$n \cdot g = \underbrace{g + g + \ldots + g}_{n \text{ volte}} \quad n \in \mathbb{Z}$$

è uno $\mathbb{Z}$-modulo.
Se $f : A \to B$ è un omomorfismo di anelli allora B è un A-modulo con l'operazione $a \cdot b = f(a)b$.

Definizione 2.0.2. *Sia M un A-modulo. Un sottoinsieme $N \subseteq M$ è un **sotto-A-modulo** se è un A-modulo con le stesse operazioni di M.*

Definizione 2.0.3. *Siano M e N due A-moduli, una funzione $f : M \to N$ è un omomorfismo di A-moduli se per ogni $x, y \in M$ e $a \in A$*

1. $f(x+y) = f(x) + f(y)$
2. $f(ax) = af(x)$

*Il **nucleo** di f è*
$$\ker f = \{x \in M : f(x) = 0_N\}.$$
Il nucleo di f è sempre un sottomodulo di M. Osserviamo inoltre che l'immagine $f(M)$ è un sottomodulo di N.

Dato che gli A-moduli sono gruppi abeliano, dati due A-moduli M e N possiamo sempre considerare il loro quoziente (come gruppi abeliani) M/N. Il quoziente è ancora un A-modulo con l'operazione $a(m+N) = am + N$. Pertanto anche per gli A-mouduli valgono i seguenti teoremi.

Teorema 2.0.4 (Teorema dell'omomorfismo)**.** *Siano M e N due A-moduli e $f : M \to N$ un omomorfismo di A-moduli, allora $M/\ker f \simeq f(M)$.*

Teorema 2.0.5 (Teorema dell'isomorfismo)**.** *Siano M, N, L tre A-moduli*

1. *Se $L \subseteq N \subseteq M$ allora N/L è un sottomodulo di M/L, inoltre*
$$\frac{(M/L)}{(N/L)} \simeq M/N.$$
2. *$N, L \subseteq M$, allora*
$$\frac{N+L}{N} \simeq \frac{L}{N \cap L}.$$

Dimostrazione.

1. Consideriamo $\varphi : M/L \to M/N$ con $\varphi(m+L) = m+N$. φ è un omomorfismo suriettivo inoltre $\ker \varphi = N/L$, quindi dal teorema dell'isomorfismo segue la tesi.
2. Consideriamo l'immersione canonica $i : L \to N + L$ e $\pi : N + L \to (N+L)/N$ la proiezione naturale e consideriamo la loro composizione $\varphi = \pi \circ i : L \to (N+L)/N$. Sotto queste ipotesi φ è un omomorfismo suriettivo, infatti per ogni $n + l + N \in (N+L)/N$ basta considerare $\varphi(l) = l + N = n + l + N$. Inoltre $\ker \varphi = L \cap N$, quindi dal teorema dell'isomorfismo segue la tesi.

□

Definizione 2.0.6. *Sia L un A-modulo e M, N due sottomoduli di L. Definiamo*
$$(M : N) = \{a \in A : aN \subseteq M\} \subseteq A$$
*(osserviamo che $(M : N)$ è un ideale di A). Definiamo l'**annullatore** di M come*
$$\mathrm{Ann}(M) = (0 : M).$$
*Se $\mathrm{Ann}(M) = (0)$ allora M si dice **fedele** su A.*

Osservazione 2.0.7. *Se M è un A-modulo e $I \subseteq \mathrm{Ann}(M)$ è un ideale di A allora M eredita in modo naturale la struttura di A/I-modulo nel seguente modo: $(a+I)m = am$. Proviamo che l'operazione appena introdotta è ben definita, infatti*
$$a + I = b + I \Rightarrow a - b \in I \subseteq \mathrm{Ann}(M) \Rightarrow (a-b)m = 0 \Rightarrow am = bm.$$
Inoltre è facile verificare che sono verificate tutte le proprietà degli A-moduli.

Definizione 2.0.8. *Se M è un A-modulo e $x \in M$ possiamo considerare il seguente sottomodulo*
$$Ax = \{ax \in M : a \in A\} \subseteq M.$$
*M si dice **finitamente generato** (o **tipo finito** o **finito**) se $\exists x_1, x_2, \dots, x_n \in M$ tali che*
$$M = Ax_1 + Ax_2 + \ldots + Ax_n.$$
*Un ideale I di A è detto **finitamente generato** se lo è come A-modulo. In questo caso introduciamo la seguente notazione*
$$I = Ax_1 + Ax_2 + \ldots + Ax_n = (x_1, x_2, \dots, x_n).$$

Definizione 2.0.9. *Siano $M_i \subseteq M$ con $i \in \Omega$ sotto-A-moduli di M, definiamo **somma diretta** come*
$$\bigoplus_{i\in\Omega} M_i = \{(m_i)_{i\in\Omega} : m_i \in M_i, m_i = 0 \text{ tranne un numero finito}\}.$$
*Mentre il **prodotto diretto** sarà*
$$\prod_{i\in\Omega} M_i = \{(m_i)_{i\in\Omega} : m_i \in M_i\}.$$
Somma e prodotto diretto sono ancora A-moduli definendo l'opreazione di somma e prodotto componente per componente

- $(m_i) + (m_i') = (m_i + m_i')$
- $a(m_i) = (am_i)$

Osserviamo che nel caso in cui Ω sia un insieme finito somma e prodotto diretto coincidono.

Definizione 2.0.10. *Un A-modulo M è **libero** se è somma diretta di copie di A*
$$M = \bigoplus_{i\in\Omega} A.$$

Proposizione 2.0.11. *Ogni A-modulo M di tipo finito è isomorfo a un quoziente di un modulo libero di tipo finito.*

Dimostrazione. Se $M = Ax_1 + Ax_2 + \ldots + Ax_n$ allora possiamo considerare l'omomorfismo
$$\varphi : \bigoplus_{i=1}^{n} A \to M \quad \varphi(a_1, a_2, \dots, a_n) = a_1x_1 + a_2x_2 + \ldots + a_nx_n.$$
φ è suriettivo quindi dal teorema dell'omomorfismo abbiamo che $M \simeq \bigoplus_{i=1}^n A/\ker\varphi$. □

In generale $\ker\varphi \neq \{0\}$, cioè esistono moduli finitamente generati che non sono liberi. Ad esempio se consideriamo $M = \mathbb{Z}/n\mathbb{Z}$ come $\mathbb{Z}$-modulo, esso è finitamente generato da $1 + n\mathbb{Z}$, ma non è un modulo libero, infatti in questo caso $\ker\varphi = n\mathbb{Z}$.
È per questo motivo che non esiste una nozione analoga a quella di base per gli spazi vettoriali negli A-moduli.

2.1 Lemma di Nakayama

Lemma 2.1.1 (Lemma di Nakayama). *Sia M un A-modulo di finitamente generato, $I \subseteq \mathcal{J}(A)$ un ideale di A e supponiamo che $IM = M$, allora $M = \{0\}$.*

Dimostrazione. Per ipotesi $M = Ax_1 + \ldots + Ax_n$. Allora si ha anche

$$IM = Ix_1 + Ix_2 + \ldots + Ix_n.$$

Dato che $x_i \in M = IM$ per ogni $i \in \{1, \ldots, n\}$ allora abbiamo n equazioni del tipo

$$\begin{cases} x_1 = a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \\ x_2 = a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n \\ \vdots \\ x_n = a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n \end{cases}$$

dove $a_{ij} \in I$. Ponendo $A = (a_{ij})$, $\underline{x} = (x_1, \ldots, x_n)$, $I_n = (\delta_{ij})$ abbiamo

$$\underline{x} = A\underline{x}$$
$$(I_n - A)\underline{x} = \underline{0}$$

da cui ponendo $B = I_n - A$ moltiplicando ambo i membri dell'ultima uguagliaza per la trasposta dell'aggiunta di B otteniamo

$$\det(B)\underline{x} = \underline{0}$$

cioè $\det(B)x_i = 0$ per ogni $i \in \{1, \ldots, n\}$. Adesso $\det(B)$ è della forma $1 + i$ con $i \in I \subseteq \mathcal{J}(A)$, per cui $1 + i$ è un elemento invertibile di A, pertanto $x_i = 0$ per ogni $i \in \{1, \ldots, n\}$, cioè $M = \{0\}$. $\square$

Corollario 2.1.2. *Siano M un A-modulo fintamente generato, $N \subseteq M$ un suo sottmodulo e $I \subseteq \mathcal{J}(A)$ un ideale di A. Se $M = N + IM$ allora $M = N$.*

Dimostrazione. Osserviamo che

$$I(M/N) = \frac{IM + N}{N} = M/N$$

infatti per ogni $m \in M$, $n \in N$ e $i \in I$ si ha

$$i(m + N) = im + N = (im + n) + N.$$

Pertanto applicando il lemma di Nakayama a M/N abbiamo $M/N = 0$, cioè $M = N$. $\square$

Osserviamo che se $(A, \underline{m})$ è un anello locale e M è un A-modulo allora

$$\underline{m}(M/\underline{m}M) = \{0\}$$

quindi $M/\underline{m}M$ è un $A/\underline{m}$-modulo, cioè un $k = A/\underline{m}$-spazio vettoriale. Inoltre, se M è finitamente generato e $\{x_1, \ldots, x_n\}$ è un sistema di generatori minimale di M allora, avendo posto $\overline{x_i} = x_i + \underline{m}M$, $B = \{\overline{x_1}, \ldots, \overline{x_n}\}$ è una base di $M/\underline{m}M$. Infatti è facile verificare che B è un insieme di generatori di $M/\underline{m}M$. Supponiamo che

$$\overline{a_1}\,\overline{x_1} + \ldots + \overline{a_n}\,\overline{x_n} = \overline{0}$$
$$\Rightarrow a_1x_1 + \ldots + a_nx_n = m_1x_1 + \ldots + m_nx_n \in \underline{m}M,$$

dove $m_i \in \underline{m}$. Adesso se fosse $\overline{a_i} \neq \overline{0}$, cioè se $a_i \notin \underline{m}$, per qualche $i \in \{1, \ldots, n\}$ allora a_i sarebbe invertibile, quindi lo sarebbe anche $a_i - m_i$, da cui si avrebbe

$$x_i = (a_i - m_i)^{-1}\Big((m_1 - a_1)x_1 + \ldots + (m_i - a_i)\hat{x}_i + \ldots (m_n - a_n)x_n\Big)$$

contro la minimalità di $\{x_1, \ldots, x_n\}$. Dunque B è una base di $M/\underline{m}M$. Il lemma di Nakayama ci assicura che vale anche il viceversa.

Corollario 2.1.3. *Sia $(A, \underline{m})$ un anello locale e M un A-modulo finitamente generato. Se $\{\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n}\}$ è una base di $M/\underline{m}M$ e $N = Ax_1 + Ax_2 + \ldots + Ax_n$ allora $M = N$.*

Dimostrazione. Consideriamo l'immersione canonica $i : N \to M$ e la proiezione naturale $\pi : M \to M/\underline{m}M$. La composizione

$$\varphi = \pi \circ i : N \to M/\underline{m}M$$

è suriettiva, infatti $\varphi(x_i) = \overline{x_i}$ per ogni $i \in \{1, \ldots, n\}$ e $\{\overline{x_1}, \ldots, \overline{x_n}\}$ è una base di $M/\underline{m}M$. Dunque $N + \underline{m}M = M$, quindi applicando il corollario precedente abbiamo $M = N$. $\square$

Corollario 2.1.4. *Se A è un anello locale, gli insiemi di generatori minimali di un A-modulo finitamente generato hanno la stessa cardinalità.*

Definizione 2.1.5. *Se M e N sono due A-moduli allora*

$$\mathrm{Hom}_A(M, N) = \{f : M \to N : f \textit{ omomorfismo}\}$$

è un A-modulo con le operazioni definite nel modo seguente: per ogni $f, g \in \mathrm{Hom}_A(M, N)$, $m \in M$ e $a \in A$

- $(f + g)(m) = f(m) + g(m)$
- $(af)(m) = af(m)$

Osservazione 2.1.6. *Osserviamo che $\mathrm{Hom}(A, M) \simeq M$ tramite $\varphi : \mathrm{Hom}(A, M) \to M$ con $\varphi(f) = f(1)$. Verifichiamo che φ è un isomorfismo.*

- *φ è un omomorfismo, infatti*

$$\varphi(f + g) = (f + g)(1) = f(1) + g(1) = \varphi(f) + \varphi(g)$$
$$\varphi(af) = (af)(1) = af(1) = a\varphi(f)$$

- *φ è iniettiva, infatti*

$$\varphi(f) = \varphi(g) \Rightarrow f(1) = g(1) \Rightarrow af(1) = ag(1) \Rightarrow f(a) = g(a) \Rightarrow f = g.$$

- *φ è suriettiva, infatti per ogni $m \in M$ consideriamo $f_m : A \to M$ tale che $f_m(a) = am$. Risulta $f_m \in \mathrm{Hom}(A, M)$ e $\varphi(f_m) = m$.*

Definizione 2.1.7. *Supponiamo di avere tre A-moduli M, N e L. Dato un omomorfismo $f : M \to N$ esso induce due omomorfismi: il primo $f^* : \mathrm{Hom}(N, L) \to \mathrm{Hom}(M, L)$ definito nel seguente modo*

$$f^*(g) = g \circ f;$$

il secondo $f_* : \mathrm{Hom}(L, M) \to \mathrm{Hom}(L, N)$ definito nel seguente modo

$$f_*(g) = f \circ g.$$

2.2 Successioni esatte

Definizione 2.2.1. *Una successione di A-moduli e omomorfismi di moduli del tipo*

$$\ldots \to M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \to \ldots$$

*è detto **complesso** se*

$$\mathrm{Im}\, f_i \subseteq \ker f_{i+1},$$

*mentre è detta **esatta** se*

$$\mathrm{Im}\, f_i = \ker f_{i+1}.$$

Definizione 2.2.2. *Una successione esatta del tipo*

$$0 \to M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0 \tag{2.1}$$

*si dice successione **esatta corta**.*
Osserviamo che in queste ipotesi, l'immagine del primo omomorfismo è nulla e coincide con il nucleo di u, da cui u è iniettiva. Allo stesso modo, il nucleo dell'ultimo omomorfismo dev'essere tutto M'' e deve coincidere con l'immagine di v, pertanto v è suriettiva. Riassumendo si ha

1. *u è iniettiva.*

2. *v è suriettiva.*

3. *$\mathrm{Im}\, u = \ker v$.*

Data una successione esatta

$$\ldots \to M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \to \ldots$$

tenendo conto che $\mathrm{Im}\, f_i = \ker f_{i+1}$, essa si può decomporre in successioni esatte corte nel seguente modo

$$0 \to \mathrm{Im}\, f_i = \ker f_{i+1} \to M_i \xrightarrow{f_{i+1}} \mathrm{Im}\, f_{i+1} \to 0.$$

Definizione 2.2.3. *Sia $\mathcal{C}$ una famiglia di A-moduli. Un'applicazione $\lambda : \mathcal{C} \to \mathbb{Z}$ tale che per ogni successione esatta corta del tipo 2.1 (con $M, M', M'' \in \mathcal{C}$) risulti*

$$\lambda(M) = \lambda(M') + \lambda(M'')$$

si dice ***additiva****.*

Proposizione 2.2.4.

1. *Sia*
$$M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$$
una successione di A-moduli e omomorfismi. La precedente è esatta se e solo se per ogni A-modulo N la successione
$$0 \to \mathrm{Hom}(M', N) \xrightarrow{u^*} \mathrm{Hom}(M, N) \xrightarrow{v^*} \mathrm{Hom}(M'', N)$$
è esatta.

2. *Sia*
$$0 \to M' \xrightarrow{u} M \xrightarrow{v} M''$$
una successione di A-moduli e omomorfismi. La precedente è esatta se e solo se per ogni A-modulo N la successione
$$0 \to \mathrm{Hom}(N, M') \xrightarrow{u_*} \mathrm{Hom}(N, M) \xrightarrow{v_*} \mathrm{Hom}(N, M'')$$
è esatta.

Dimostrazione.

1.

2. $\Rightarrow$ Dobbiamo provare che u_* è iniettiva e che $\mathrm{Im}\, u_* = \ker v_*$.
Sia $f \in \mathrm{Hom}(N, M')$ tale che $u_*(f) = \underline{0}$. Allora per ogni $n \in N$ si ha $u_*(f)(n) = (u \circ f)(n) = u(f(n)) = 0$, dall'iniettività di u abbiamo $f(n) = 0$, cioè $f = \underline{0}$. Ciò prova che u_* è iniettiva.
Sia $g \in \mathrm{Im}\, u_*$, allora esiste $f \in \mathrm{Hom}(N, M')$ tale che $g = u_*(f) = u \circ f$. Adesso $v_*(g) = v \circ g = v \circ (u \circ f) = (v \circ u) \circ f = \underline{0}$, quindi $g \in \ker v_*$.
Viceversa sia $g \in \ker v_*$, allora $v_*(g) = \underline{0}$, cioè per ogni $n \in N$ si ha $v_*(g)(n) = (v \circ g)(n) = v(g(n)) = 0$, cioè $g(n) \in \ker v = \mathrm{Im}\, u$ per ogni $n \in N$. Quindi esiste un unico $m_n \in M$ tale che $u(m_n) = g(n)$ (l'unicità segue dall'iniettività di u). Pertanto possiamo definire $f : N \to M$ tale che $f(n) = m_n$. Si verifica facilmente che $f \in \mathrm{Hom}(N, M)$. Così per ogni $n \in N$ risulta $u_*(f)(n) = (u \circ f)(n) = u(f(n)) = u(m_n) = g(n)$ da cui $g = u_*(f) \in \mathrm{Im}\, u_*$.

   $\Leftarrow$ Dobbiamo dimostrare che u è iniettiva e che $\mathrm{Im}\, u = \ker v$.
Sia $x \in M'$ tale che $u(x) = 0$. Poniamo $N = Ax \subseteq M'$ e consideriamo l'inclusione canonica $i : N \to M' \in \mathrm{Hom}(N, M')$, per ogni $ax \in N$ risulta $u_*(i)(ax) = (u \circ i)(ax) = u(i(ax)) = u(ax) = au(x) = 0$, cioè $u_*(i) = \underline{0}$, pertanto dall'iniettività di u_* segue che $i = \underline{0}$ ovvero $Ax = 0$, da cui deve

aversi $x = 0$. Ciò prova l'iniettività di u.
Sia $x \in \operatorname{Im} u$, allora esiste $y \in M'$ tale che $x = u(y)$. Poniamo $N = Ay \subseteq M'$ e consideriamo l'inclusione canonica $i : N \to M' \in \operatorname{Hom}(N, M')$, per ipotesi $v_* \circ u_*$ è nulla, quindi $(v_* \circ u_*)(i) = v_*(u_*(i)) = v_*(u \circ i) = v \circ (u \circ i) = (v \circ u) \circ i = \underline{0}$, da cui dato che $y \in N$ si ha $((v \circ u) \circ i)(y) = (v \circ u)(y) = v(u(y)) = 0$ in altri termini $v(x) = 0$, ovvero $x \in \ker v$.
Viceversa sia $x \in \ker v \subseteq M$, poniamo $N = Ax$ e consideriamo l'immersione canonica $i : N \to M$, allora per ogni $ax \in N$ si ha $v_*(i)(ax) = (v \circ i)(ax) = v(ax) = av(x) = 0$. Pertanto $v_*(i) = \underline{0}$, da cui $i \in \ker v_* = \operatorname{Im} u_*$ quindi deve esistere $f \in \operatorname{Hom}(N, M')$ tale che $i = u_*(f) = u \circ f$, da cui otteniamo $x = i(x) = u(f(x)) \in \operatorname{Im} u$.

□

2.3 A-algebre

Definizione 2.3.1. *Sia $f : A \to B$ un omomorfismo di anelli . In questo modo B è un A-modulo con $a \cdot b = f(a)b$. B viene detta A-**algebra**.*

Nel caso in cui $A = k$ sia un campo se f è non nullo allora è iniettivo (è un'immersione di k in B), quindi B contiene una copia isomorfa a k. Pertanto quando parleremo di k-algebre possiamo sempre intendere un anello che contiene k.

Definizione 2.3.2. *Una A-algebra B è **finitamente generata** se esistono $b_1, b_2, \ldots, b_n \in B$ tali che*
$$B = f(A)[b_1, b_2, \ldots, b_n].$$

Definizione 2.3.3. *Una A-algebra B è detta **finita** se B è finito come A-modulo, cioè se esistono $b_1, b_2, \ldots, b_n \in B$ tali che*

$$B = Ab_1 + Ab_2 + \ldots + Ab_n.$$

2.4 Anelli e moduli di frazioni

Sia A un anello e $S \subseteq A$ una parte moltiplicativa. Su $A \times S$ definiamo la seguente relazione
$$(a, s) \sim (b, t) \Leftrightarrow \exists u \in S : (at - bs)u = 0.$$

Verifichiamo che $\sim$ è una relazione di equivalenza. La proprietà riflessiva e simmetrica seguono banalmente. Verifichiamo la poprietà transitiva. Supponiamo che

$$(a, s) \sim (b, t),\ (b, t) \sim (c, r)$$

allora esistono $u, v \in S$ tali che

$$u(at - bs) = uat - ubs = 0$$
$$v(br - ct) = vbr - vct = 0,$$

da cui moltiplicando ambo i membri della prima per vr e la seconda per us si ha

$$\begin{aligned} vruat - vrubs &= 0 \\ usvbr - usvct &= 0, \end{aligned}$$

infine sommando membro a membro otteniamo

$$vruat - usvct = uvt(ar - cs) = 0$$

e dato che $uvt \in S$ allora risulta $(a, s) \sim (c, r)$.

Definizione 2.4.1. *Sia A un anello e $S \subseteq A$ una parte moltiplicativa. Definiamo*

$$S^{-1}A = A \times S/ \sim$$

e indichiamo $[(a, s)] = \frac{a}{s}$. $S^{-1}A$ con le operazioni

$$\begin{aligned} \frac{a}{s} + \frac{b}{t} &= \frac{at + bs}{st} \\ \frac{a}{s} \cdot \frac{b}{t} &= \frac{ab}{st}. \end{aligned}$$

è un anello commutativa unitario.

Osserviamo che abbiamo l'omomorfismo canonico

$$\varphi : A \to S^{-1}A \quad \text{con } \varphi(a) = \frac{a}{1}$$

e risulta

$$\ker \varphi = \left\{ a \in A : \frac{a}{1} = \frac{0}{1} \right\} = \{a \in A : \exists u \in S : au = 0\}.$$

Pertanto se ad esempio S non ha divisori dello zero allora φ è un'immersione.

Proposizione 2.4.2. *Sia $f : A \to B$ un omomorfismo di anelli e S una parte moltiplicativa di A. Supponiamo che $f(s)$ sia invertibile in B per ogni $s \in S$, allora esiste un unico omomorfismo $g : S^{-1}A \to B$ tale che $g(\frac{a}{1}) = f(a)$ (in altri termini $f = g \circ \varphi$).*

Dimostrazione. Dimostriamo prima l'unicità. Supponiamo che esista un tale g. Per ipotesi $g(\frac{a}{1}) = f(a)$ e per ogni $s \in S$ abbiamo che $f(s)$ è invertibile, quindi

$$(f(s))^{-1} = \left(g\left(\frac{s}{1}\right) \right)^{-1} = g\left(\left(\frac{s}{1}\right)^{-1} \right) = g\left(\frac{1}{s}\right)$$

pertanto

$$g\left(\frac{a}{s}\right) = g\left(\frac{a}{1}\right) g\left(\frac{1}{s}\right) = f(a)f(s)^{-1}.$$

Dunque se un siffatto g esiste dev'essere tale che $g\left(\frac{a}{s}\right) = f(a)f(s)^{-1}$. Questo prova l'unicità. Per provare l'esistenza ci basta verificare che tale g è ben definito ed è un omomorfismo. Siano $\frac{a}{s} = \frac{b}{t}$, allora esiste $u \in S$ tale che $u(at - bs) = 0$ da cui

$$f(u(at - bs)) = 0 \Rightarrow f(u)(f(a)f(t) - f(b)f(s)) = 0$$

dato che $f(u)$ è invertibile per ipotesi, si ha che

$$f(a)f(t) - f(b)f(s) = 0 \Rightarrow f(a)f(s)^{-1} = f(b)f(t)^{-1} \Rightarrow g\left(\frac{a}{s}\right) = g\left(\frac{b}{t}\right).$$

Si verifica facilmente che g è un omomorfismo. $\square$

Siano M un A-modulo e $S \subseteq A$ una parte moltiplicativa. In modo anologo a quanto fatto prima, su $M \times S$ definiamo la seguente relazione (di equivalenza)

$$(m, s) \sim (n, t) \Leftrightarrow \exists u \in S : \ u(mt - ns) = 0.$$

Definizione 2.4.3. *Siano M un A-modulo e $S \subseteq A$ una parte motliplicativa. Definiamo*

$$S^{-1}M = M \times S/ \sim .$$

Indichiamo con $[(m, s)] = \frac{m}{s}$. $S^{-1}M$ con le operazioni

$$\frac{m}{s} + \frac{n}{t} = \frac{mt + ns}{st}$$
$$\frac{a}{s} \cdot \frac{m}{t} = \frac{am}{st}$$

è un $S^{-1}A$-modulo.

Se $f : M \to N$ è un omomorfismo di A-moduli e $S \subseteq A$ è una parte moltiplicativa, allora definiamo $S^{-1}f : S^{-1}M \to S^{-1}N$ con $S^{-1}f\left(\frac{m}{s}\right) = \frac{f(m)}{s}$. $S^{-1}f$ è un omomorfismo di $S^{-1}A$-moduli.

Proposizione 2.4.4. *Se $S \subseteq A$ è una parte moltiplicativa e*

$$\ldots \to M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \to \ldots$$

è una successione esatta allora la successione

$$\ldots \to S^{-1}M_{i-1} \xrightarrow{S^{-1}f_i} S^{-1}M_i \xrightarrow{S^{-1}f_{i+1}} S^{-1}M_{i+1} \to \ldots$$

è esatta.

Dimostrazione. Dobbiamo dimostrare che $\operatorname{Im} S^{-1}f_i = \ker S^{-1}f_{i+1}$. Sia $\frac{m}{s} \in S^{-1}M_{i-1}$ allora, poiché $\operatorname{Im} f_i = \ker f_{i+1}$ si ha

$$(S^{-1}f_{i+1} \circ S^{-1}f_i)\left(\frac{m}{s}\right) = S^{-1}f_{i+1}\left(\frac{f_i(m)}{s}\right) = \frac{(f_{i+1} \circ f_i)(m)}{s} = \frac{0}{s} = \frac{0}{1}$$

ciò prova che $\operatorname{Im} S^{-1}f_i \subseteq \ker S^{-1}f_{i+1}$. Viceversa sia $\frac{m}{s} \in \ker S^{-1}f_{i+1}$ allora

$$S^{-1}f_{i+1}\left(\frac{m}{s}\right) = \frac{f_{i+1}(m)}{s} = \frac{0}{s}$$

pertanto esiste $u \in S$ tale che $uf_{i+1}(m) = f_{i+1}(um) = 0$, da cui $um \in \ker f_{i+1} = \operatorname{Im} f_i$ quindi esiste $n \in M_{i-1}$ tale che $f_i(n) = um$ da cui $\frac{m}{s} = \frac{f_i(n)}{us} = S^{-1}f_i\left(\frac{n}{us}\right) \in \operatorname{Im} S^{-1}f_i$. $\square$

Osservazione 2.4.5. *Sia S una parte moltiplicativa di A e $\varphi : A \to S^{-1}A$ l'omomorfismo canonico $\varphi(a) = \frac{a}{1}$. Se I è un ideale di A allora*

$$I^e = \left\{ \sum_{finita} \frac{a}{s}\frac{i}{t} : i \in I, a \in A, s, t \in S \right\} = \left\{ \frac{i}{s} : i \in I, s \in S \right\} = S^{-1}I$$

Lemma 2.4.6. *Sia S una parte moltiplicativa di A e I un ideale di A, allora*

$$\frac{a}{s} \in S^{-1}I \iff \exists u \in S : ua \in I.$$

In particolare $S^{-1}I = S^{-1}A$ se e solo se $I \cap S \neq \emptyset$.

Dimostrazione. Proviamo la prima affermazione.

$\Rightarrow$ Esistono $i \in I$ e $t \in S$ tali che $\dfrac{a}{s} = \dfrac{i}{t}$ pertanto $\exists u \in S : (ut)a = (us)i \in I$.

$\Leftarrow$ $\dfrac{a}{s} = \dfrac{ua}{us} \in S^{-1}I$.

Adesso se $S^{-1}I = S^{-1}A$ allora $\frac{1}{1} \in S^{-1}I$ quindi $\exists u \in S : u1 = u \in I$, cioè $u \in I \cap S$. Viceversa se $u \in I \cap S$ allora $\frac{1}{1} = \frac{u}{u} \in S^{-1}I$. $\square$

Proposizione 2.4.7. *Siano M, N due sotto-A-moduli di L, e S una parte moltiplicativa di A. Allora*

1. $S^{-1}(M + N) = S^{-1}M + S^{-1}N$
2. $S^{-1}(M \cap N) = S^{-1}M \cap S^{-1}N$
3. $S^{-1}(M/N) \simeq S^{-1}M/S^{-1}N$ *(se $N \subseteq M$)*

Se I e J sono ideali di A allora

4. $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$
5. $S^{-1}\sqrt{I} = \sqrt{S^{-1}I}$

Dimostrazione.

1. Basta osservare che $\dfrac{m}{s} + \dfrac{n}{t} = \dfrac{tm + sn}{st}$.
2. $S^{-1}(M \cap N)$ è contenuto in $S^{-1}M$ e $S^{-1}N$, quindi $S^{-1}(M \cap N) \subseteq S^{-1}M \cap S^{-1}N$. Viceversa se $\frac{x}{s} \in S^{-1}M \cap S^{-1}N$ allora esistono $u, t \in S$ tali che $ux \in M$ e $tx \in N$, da cui $\frac{x}{s} = \frac{utx}{uts} \in S^{-1}(M \cap N)$.
3. Basta considerare

$$0 \to N \to M \to M/N \to 0$$
$$0 \to S^{-1}N \to S^{-1}M \to S^{-1}(M/N) \to 0,$$

la prima è una successione esatta corta, quindi per la 2.4.4 lo è anche la seconda.

4. $S^{-1}(IJ) = (IJ)^e \subseteq I^e J^e = (S^{-1}I)(S^{-1}J)$ vale sempre. Viceversa se $\frac{i}{s} \in S^{-1}I$ e $\frac{j}{t} \in S^{-1}J$ allora $\frac{ij}{st} \in S^{-1}(IJ)$.

5. Sia $\frac{i}{s} \in S^{-1}\sqrt{I}$, allora esiste $u \in S$ tale che $(ui)^n \in I$, quindi $\left(\frac{i}{s}\right)^n = \frac{(ui)^n}{(us)^n} \in S^{-1}I$, cioè $\frac{i}{s} \in \sqrt{S^{-1}I}$.
Viceversa se $\frac{i}{s} \in \sqrt{S^{-1}I}$ allora $\frac{i^n}{s^n} \in S^{-1}I$, pertanto esiste $u \in S$ tale che $ui^n \in I \Rightarrow (ui)^n \in I$, cioè $ui \in \sqrt{I}$, quindi $\frac{i}{s} \in S^{-1}\sqrt{I}$.

$\square$

Corollario 2.4.8. *Se S è una parte moltiplicativa di A allora*

$$N_{S^{-1}A} = S^{-1}N_A$$

Osservazione 2.4.9. *Sia A un anello, I un suo ideale, $S \subseteq A$ una parte moltiplicativa, l'insieme $\overline{S} = \{s + I : s \in S\} \subseteq A/I$, $\overline{S}$ è una parte moltiplicativa di A/I. Osserviamo che l'anello $\overline{S}^{-1}(A/I)$ è isomorfo a $S^{-1}A/S^{-1}I$ tramite l'isomorfismo*

$$\varphi : S^{-1}A/S^{-1}I \to \overline{S}^{-1}(A/I) \quad \varphi\left(\frac{a}{s} + S^{-1}I\right) = \frac{a+I}{s+I}.$$

Proposizione 2.4.10. *Sia $S \subseteq A$ una parte moltiplicativa, consideriamo $\varphi : A \to S^{-1}A$ l'omomorfismo canonico $\varphi(a) = \frac{a}{1}$. Sia I un ideale di A e J un ideale di $S^{-1}A$. Risulta*

1. *$J^{ce} = J$ (in particolare ogni ideale di $S^{-1}A$ è un ideale esteso).*
2. *$I^{ec} = \bigcup_{s \in S}(I : s)$*
3. *Gli ideali primi P di A tali che $P \cap S = \emptyset$ sono in corrispondenza biunivoca con gli ideali primi di $S^{-1}A$ tramite $P \to S^{-1}P$.*

Dimostrazione.

1. $J^{ce} \subseteq J$ vale sempre. Viceversa
$$\frac{j}{s} \in J \Rightarrow \frac{j}{1} = \varphi(j) \in J \Rightarrow j \in \varphi^{-1}(J) = J^c \Rightarrow \varphi(j) = \frac{j}{1} \in J^{ce} \Rightarrow \frac{j}{s} \in J^{ce}.$$

2. Da 2.4.6 abbiamo
$$x \in I^{ec} = \varphi^{-1}(S^{-1}I) \Leftrightarrow \frac{x}{1} \in S^{-1}I \Leftrightarrow \exists s \in S : sx \in I \Leftrightarrow x \in \bigcup_{s \in S}(I : s). \qquad \square$$

3. Sia P un ideale primo di A tale che $P \cap A = \emptyset$, quindi $S \subseteq A \setminus P$. Proviamo che $S^{-1}P$ è primo. Supponiamo $\frac{x}{s}\frac{y}{t} \in S^{-1}P$, quindi esiste $u \in S \subseteq A \setminus P$ tale che $uxy \in P$, ma $u \notin P$, quindi $xy \in P$, da cui $x \in P$ oppure $y \in P$, cioè $\frac{x}{s} \in S^{-1}P$ oppure $\frac{y}{t} \in S^{-1}P$.
Osserviamo adesso che per ogni $s \in S$ si ha $(P : s) = P$. Infatti $P \subseteq (P : s)$, viceversa se $x \in (P : s)$ allora $xs \in P$, ma $s \notin P$, quindi $x \in P$. Dunque dal punto 2 sappiamo che $P^{ec} = P$. Mentre se Q è un ideale primo di $S^{-1}A$, dal punto 1 sappiamo che $Q^{ce} = Q$. Pertanto le applicazioni $P \to P^e$ e $Q \to Q^c$ sono una l'inversa dell'altra.

Corollario 2.4.11. *Se P è un ideale primo di A allora gli ideali primi di A_P sono in corrispondenza biunivoca con gli ideali primi di A contenuti in P.*

In particolare, ovviamente P è il più grande ideale contenuto in P, pertanto PA_P è l'unico ideale massimale di A_P, quindi A_P è locale.

2.5 Proprietà locali

Sia P un ideale primo di A. Osserviamo che $A \setminus P$ è una parte moltiplicativa di A, infatti

- $a, b \notin P \Rightarrow ab \notin P$
- $1 \notin P$

Definizione 2.5.1. *Dato un ideale primo P di A si definisce **localizzazione** su P l'anello $A_P = (A \setminus P)^{-1}A$. A_p è un anello locale con ideale massimale $(A \setminus P)^{-1}P$.*

Definizione 2.5.2. *Sia A un anello. Una proprietà $\mathcal{P}$ viene detta **locale** se equivalentemente*

1. *Vale per A.*
2. *Vale per A_P per ogni ideali P primo di A.*
3. *Vale per $A_{\underline{m}}$ per ogni ideale $\underline{m}$ massimale.*

Un primo esempio di proprietà locale è dato dalla seguente

Proposizione 2.5.3. *Per un qualsiasi A-modulo M le seguenti condizioni sono equivalenti*

1. *$M = 0$.*
2. *$M_P = 0$ per ogni ideali P primo di A.*
3. *$M_{\underline{m}} = 0$ per ogni ideale $\underline{m}$ massimale di A.*

Dimostrazione. Banalmente (1) $\Rightarrow$ (2) $\Rightarrow$ (3).
(3) $\Rightarrow$ (1) Per assurdo supponiamo che $M \neq 0$, allora esiste $x \in M$ con $x \neq 0$, quindi $1 \notin \mathrm{Ann}(x) \subsetneq A$, pertanto esiste un ideale massimale $\underline{m}$ di A contenente $\mathrm{Ann}(x)$. Per ipotesi $M_{\underline{m}} = 0$ quindi $\frac{x}{1} = \frac{0}{1}$, cioè esiste $u \in A \setminus \underline{m}$ tale che $ux = 0$ pertanto $u \in Ann(x) \subseteq \underline{m}$, assurdo. $\square$

Se $\varphi : M \to N$ è un omomorfismo di A-moduli e P è un ideale primo di A, indichiamo con $\varphi_P = (A \setminus P)^{-1}\varphi$.

Proposizione 2.5.4. *Siano M, N due A-moduli e $\varphi : M \to N$ un omomorfismo di A-moduli, sono equivalenti*

1. *$\varphi : M \to N$ è iniettiva [suriettiva]*
2. *$\varphi_P : M_P \to N_P$ è iniettiva [suriettiva]*

3. $\varphi_{\underline{m}} : M_{\underline{m}} \to N_{\underline{m}}$ *è iniettiva [suriettiva]*

Dimostrazione.

(1) $\Rightarrow$ (2) Dire che $\varphi : M \to N$ è iniettiva equivale a dire che

$$0 \to M \to N$$

è esatta, quindi anche

$$0 \to M_P \to N_P$$

è esatta, da cui $\varphi_P : M_P \to N_P$ è iniettiva.

(2) $\Rightarrow$ (3) Ovvia.

(3) $\Rightarrow$ (1) La successione

$$0 \to \ker\varphi \to M \to N$$

è esatta, pertanto anche

$$0 \to \ker\varphi_{\underline{m}} \to M_{\underline{m}} \to N_{\underline{m}}$$

è esatta. Mostriamo adesso che $\ker\varphi_{\underline{m}} = (\ker\varphi)_{\underline{m}}$, infatti siano $x \in M$ e $y \in A \setminus \underline{m}$, abbiamo questa serie di equivalenze

$$\frac{x}{y} \in \ker\varphi_{\underline{m}} \Leftrightarrow \varphi_{\underline{m}}\left(\frac{x}{y}\right) = \frac{\varphi(x)}{y} = \frac{0}{1} \Leftrightarrow$$
$$\Leftrightarrow \exists u \in A \setminus \underline{m} : u\varphi(x) = \varphi(ux) = 0 \Leftrightarrow ux \in \ker\varphi \Leftrightarrow \frac{x}{y} = \frac{ux}{uy} \in (\ker\varphi)_{\underline{m}}$$

da cui

$$0 = \ker\varphi_{\underline{m}} = (\ker\varphi)_{\underline{m}}$$

dalla proposizione precedente e dall'arbitrarietà di $\underline{m}$ segue $\ker\varphi = 0$.

$\square$

Capitolo 3

Decomposizione primaria

Definizione 3.0.1. *Un ideale I di A si dice* ***primario*** *se*

$$xy \in I \Rightarrow x \in I \text{ oppure } y^n \in I \text{ per qualche } n \in \mathbb{N}.$$

Equivalentemente

- $xy \in I$, $x \notin I \Rightarrow y \in \sqrt{I}$.
- $xy \in I$, $y \notin \sqrt{I} \Rightarrow x \in I$.

Dalla definizione segue subito che ogni ideale primo è primario.

Definizione 3.0.2. *Se un ideale I di A si scrive come intersezione di ideali primari*

$$I = Q_1 \cap \ldots \cap Q_n$$

allora la precedente scrittura sarà detta una ***decomposizione primaria*** *per I. In questo caso I si dice* ***decomponibile****.*

In generale non è detto che ogni ideale I di un anello A abbia una decomposizione primaria.

Proposizione 3.0.3. *Se $f : A \to B$ è un omomorfismo di anelli e J è un ideale primario di B, allora $f^{-1}(J)$ è un ideale primario di A.*

Dimostrazione. Supponiamo che $xy \in f^{-1}(J)$ e $x \notin f^{-1}(J)$, ciò vuol dire che $f(xy) = f(x)f(y) \in J$ e $f(x) \notin J$ quindi esiste $n \in \mathbb{N}$ tale che $f(y)^n = f(y^n) \in J$, cioè $y^n \in f^{-1}(J)$. □

Proposizione 3.0.4. *I è primario se e solo se in A/I ogni divisore dello zero è nilpotente.*

Dimostrazione.

⇒ Sia $\overline{x} = x + I \in A/I$ un divisore dello zero, quindi esiste $\overline{y} = y + I \in A/I$ non nullo ($y \notin I$) tale che $\overline{x}\,\overline{y} = \overline{0} \Leftrightarrow xy \in I$, per ipotesi I è primario quindi esiste $n \in \mathbb{N}$ tale che $x^n \in I$, ovvero $\overline{x}^n = \overline{0}$.

$\Leftarrow$ Supponiamo che $xy \in I$ e $y \notin I$, ciò equivale a dire che $(x+I)(y+I) = I$ in A/I, quindi $x+I$ è un divisore dello zero di A/I (dato che $y+I \neq I$), pertanto è nilpotente, cioè $x^n + I = I \Leftrightarrow x^n \in I$.

$\square$

Proposizione 3.0.5. *Se I è un ideale primario allora $\sqrt{I}$ è primo.*

Dimostrazione. Supponiamo che $xy \in \sqrt{I}$ e $x \notin \sqrt{I}$ allora esiste $n \in \mathbb{N}$ tale che $(xy)^n = x^n y^n \in I$ con $x^n \notin I$, quindi dato che I è primario deve aversi $y^n \in \sqrt{I}$ cioè esiste $m \in \mathbb{N}$ tale che $(y^n)^m = y^{nm} \in I$ cioè $y \in \sqrt{I}$. $\square$

D'ora in poi parleremo di ideale P-primario, nel senso che I è P-primario se è primario con $\sqrt{I} = P$.

Esempio 3.0.6. *Sia $I = (x, y^2) \subseteq k[x, y]$. Abbiamo che*

$$A/I = \frac{k[x,y]}{(x,y^2)} \simeq \frac{k[t]}{(t^2)}$$

quindi in A/I ogni divisore dello zero è nilpotente $\Leftrightarrow$ I è primario. D'altra parte si ha

$$(x,y)^2 = (x^2, xy, y^2) \subseteq (x, y^2) \subseteq (x, y)$$
$$(x,y) = \sqrt{(x,y)^2} \subseteq \sqrt{(x,y^2)} \subseteq \sqrt{(x,y)} = (x,y) \Rightarrow \sqrt{(x,y^2)} = (x,y).$$

Dunque (x, y^2) è (x, y)-primario ma non è una potenza di un primo.

Esempio 3.0.7. *Non è detto che se $\sqrt{I}$ è primo allora I è primario.*
Infatti consideriamo in $k[x, y, z]/(xy-z^2)$. Nel quoziente, indicando con $\overline{x} = x+(xy-z^2)$, $\overline{y} = y + (xy - z^2)$, $\overline{z} = z + (xy - z^2)$ sia $P = (\overline{x}, \overline{z})$. P è primo poiché l'ideale (x, z) di $k[x, y, z]$ è primo e contiene $(xy - z^2)$. Adesso abbiamo

$$\overline{x}\,\overline{y} = \overline{z}^2 \in P^2,\ \overline{x} \notin P^2,\ \overline{y} \notin P = \sqrt{P^2}$$

fatti da cui segue che P^2 non è primario.
Questo esempio mostra anche che non tutte le potenze di un ideale primo sono ideali primari.

Proposizione 3.0.8. *Se Q è un ideale tale che $\sqrt{Q} = M$ è massimale, allora Q è M-primario.*

Dimostrazione. Sia P un ideale primo contenente Q. Risulta

$$P \supseteq Q \Rightarrow P = \sqrt{P} \supseteq \sqrt{Q} = M \Rightarrow P = M.$$

Pertanto M è l'unico ideale primo che contiene Q. Dunque il quoziente A/Q ha un solo ideale primo, quindi in A/Q ogni elemento è invertibile oppure nilpotente, in particolare ogni divisore dello zero è nilpotente. $\square$

Sia I un ideale decomponibile

$$I = Q_1 \cap \ldots \cap Q_n$$

con Q_i ideali primari. Sfrondiamo la precedente decomposizione nel seguente modo. Se $\sqrt{Q_i} = \sqrt{Q_j}$, sostiutuiamo a Q_i e Q_j l'ideale $Q_i \cap Q_j$. Esso è primario, infatti se $xy \in Q_i \cap Q_j$ con $x \notin Q_i \cap Q_j$ allora $x \notin Q_i$ oppure $x \notin Q_j$. Supponiamo che $x \notin Q_i$, dato che $xy \in Q_i \cap Q_j \subseteq Q_i$ si ha $y \in \sqrt{Q_i} = \sqrt{Q_j} = \sqrt{Q_i} \cap \sqrt{Q_j} = \sqrt{Q_i \cap Q_j}$.
Inoltre possiamo assumere che

$$Q_i \not\supseteq \bigcap_{j \neq i} Q_j.$$

Una decomposizione così ottenuta si dice **minimale**.
I primi $P_i = \sqrt{Q_i}$ si dicono **primi associati** a I. I primi dell'insieme $\{P_1, \ldots, P_n\}$ minimali rispetto all'inclusione si dicono **primi minimali associati** ad I. I restanti sono detti **primi immersi**.
Se P è un ideale primo che contiene I allora

$$P \supseteq I = Q_1 \cap \ldots \cap Q_n \Rightarrow P = \sqrt{P} \supseteq P_1 \cap \ldots \cap P_n$$

da cui $P \supseteq P_i$ per qualche $i \in \{1, \ldots, n\}$ (1.1.23). Da ciò segue che i primi minimali associati ad I sono i primi minimali nella famiglia degli ideali primi contenenti I.

Lemma 3.0.9. *Sia Q un ideale P-primario di A. Per ogni $x \in A$ abbiamo*

1. $x \in Q \Rightarrow (Q : x) = A$
2. $x \notin Q \Rightarrow (Q : x)$ *è P-primario.*
3. $x \notin P \Rightarrow (Q : x) = Q$.

In particolare se $x \notin Q$ allora $\sqrt{(Q : x)} = P$.

Dimostrazione.

1. Ovvio.
2. Sia $y \in (Q : x)$ allora $xy \in Q$ e $x \notin Q$ quindi $y \in P$. Otteniamo così

   $$Q \subseteq (Q : x) \subseteq P \Rightarrow P = \sqrt{Q} \subseteq \sqrt{(Q : x)} \subseteq \sqrt{P} = P.$$

   Supponiamo adesso che $yz \in (Q : x)$ e $y \notin P$, allora $xyz \in Q$, dal fatto che Q è P-primario segue $xz \in Q$, cioè $z \in (Q : x)$.
3. Ovviamente $Q \subseteq (Q : x)$. Viceversa se $y \in (Q : x)$ allora $xy \in Q$, ma $x \notin P$, quindi $y \in Q$. Ciò prova $(Q : x) \subseteq Q$.

$\square$

Teorema 3.0.10 (Primo teorema di unicità). *Sia I un ideale decomponibile e sia*

$$I = Q_1 \cap \ldots \cap Q_n$$

una decomposizione primaria minimale. Allora i primi $P_i = \sqrt{Q_i}$ associati ad I sono tutti e soli i primi della forma $\sqrt{(I : x)}$ al variare di $x \in A$. In particolare non dipendono dalla decomposizione scelta.

Dimostrazione. Per ogni $x \in A$ tale che $\sqrt{(I : x)}$ è primo si ha

$$(I : x) = (Q_1 \cap \ldots \cap Q_n : x) = (Q_1 : x) \cap \ldots \cap (Q_n : x),$$

ponendo $\underline{n} = \{1, \ldots, n\}$, $\mathcal{I} = \{i \in \underline{n} : x \notin Q_i\}$ dal lemma precedente segue che

$$\sqrt{(I : x)} = \sqrt{(Q_1 : x) \cap \ldots \cap (Q_n : x)} = \bigcap_{i=1}^{n} \sqrt{(Q_i : x)} =$$
$$= \bigcap_{i \in \mathcal{I}} \sqrt{(Q_i : x)} \cap \bigcap_{i \in \underline{n} \setminus \mathcal{I}} \sqrt{(Q_i : x)} = \bigcap_{i \in \mathcal{I}} P_i \cap \bigcap_{i \in \underline{n} \setminus \mathcal{I}} A = \bigcap_{i \in \mathcal{I}} P_i.$$

Essendo $\sqrt{(I : x)}$ primo esiste $i \in \underline{n}$ tale che $\sqrt{(I : x)} = P_i$ (1.1.23).
Viceversa, dato che la decomposizione considerata è minimale, per ogni $i \in \underline{n}$ esiste $x_i \in (\bigcap_{j \neq i} Q_j) \setminus Q_i$, pertanto si ha $\mathcal{I} = \{i\}$, quindi $\sqrt{(I : x_i)} = P_i$. □

Proposizione 3.0.11. *Se I è un ideale decomponibile in A e $I = Q_1 \cap Q_2 \cap \ldots \cap Q_n$ è una sua decomposizione primaria minimale, con $P_i = \sqrt{Q_i}$, allora*

$$\bigcup_{i=1}^{n} P_i = \{x \in A : (I : x) \neq I\}.$$

Dimostrazione.

- $\subseteq$ Se $x \in \bigcup_{i=1}^{n} P_i$ allora esiste $i \in \{1, \ldots, n\}$ tale che $x \in P_i$. Inoltre esiste $y \in A \setminus I$ tale che $P_i = \sqrt{(I : y)}$, quindi $x^m \in (I : y)$ per qualche $m \geq 1$, cioè $x^m y \in I$. Sia m il minimo naturale tale che $x^m y \in I$. Risulta $x^{m-1} y \in (I : x) \setminus I$, quindi $(I : x) \neq I$.

- $\supseteq$ Se $(I : x) \neq I$ allora esiste $y \in A \setminus I$ tale che $xy \in I$, allora $x \in (I : y) \subseteq \sqrt{(I : y)} = \bigcap_{y \notin P_j} P_j \subseteq P_j$ per qualche j, da cui $x \in \bigcup_{j=1}^{n} P_j$.

□

Corollario 3.0.12. *Se A è un anello tale che l'ideale nullo (0) sia decomponibile, allora*

$$\bigcup_{i=1}^{n} P_i = \{x \in A : (0 : x) \neq (0)\} = D \quad \textit{(divisori dello zero).}$$

Proposizione 3.0.13. *Sia S una parte moltiplicativa di A, Q un ideale P-primario*

1. *$S \cap P \neq \emptyset \Rightarrow S^{-1}Q = S^{-1}A$*

2. *$S \cap P = \emptyset \Rightarrow S^{-1}Q$ è $S^{-1}P$-primario e $Q^{ec} = (S^{-1}Q)^c = Q$.*

Dimostrazione.

1. $s \in S \cap P \Rightarrow s^n \in S \cap Q \neq \emptyset \Rightarrow S^{-1}Q = S^{-1}A$.

2. Se $\frac{a}{s} \in S^{-1}Q$, allora esistono $b \in Q, t \in S$ tali che

$$\frac{a}{s} = \frac{b}{t} \Rightarrow \exists u \in S : u(at - bs) = 0 \Rightarrow (ut)a = sb \in Q.$$

Adesso $ut \in S \subseteq A \setminus P$, cioè $ut \notin \sqrt{Q}$, quindi $a \in Q$, cioè $Q^{ec} \subseteq Q$, l'inclusione inversa è sempre vera.
Sia adesso $\frac{a}{s}\frac{b}{t} \in S^{-1}Q$, $\frac{a}{s} \notin S^{-1}Q$, quindi $ab \in Q$ e $a \notin Q$, pertanto $b \in P$, cioè $\frac{b}{t} \in S^{-1}P$. Ciò prova che $S^{-1}Q$ è $S^{-1}P$-primario ($\sqrt{S^{-1}Q} = S^{-1}\sqrt{Q} = S^{-1}P$).

□

Corollario 3.0.14. *Sia I un ideale di A, $I = Q_1 \cap \ldots \cap Q_n$ una sua decomposizione primaria minimale e sia S una parte moltiplicativa di A. Allora*

$$S^{-1}I = \bigcap_{P_i \cap S = \emptyset} S^{-1}Q_i, \quad (S^{-1}I)^c = \bigcap_{P_i \cap S = \emptyset} Q_i.$$

Teorema 3.0.15 (Secondo teorema di unicità)**.** *Gli ideali Q_i che sono P_i-primari, con P_i primi minimali associati ad I sono indipendenti dalla decomposizione.*

Dimostrazione. Se P_i è un primo minimale associato ad I sia $S = A \setminus P_i$, quindi $S \cap P_j \neq \emptyset$ per ogni $j \neq i$ quindi dal corollario precedente abbiamo che

$$S^{-1}I = S^{-1}Q_i \Rightarrow (S^{-1}I)^c = Q_i.$$

Cioè Q_i è indipendente dalla decomposizione. □

Capitolo 4

Anelli e moduli Noetheriani e Artiniani

Proposizione 4.0.1. *Sia $(\Sigma, \leq)$ un insieme parzialmente ordinato. Le seguenti condizioni sono equivalenti*

1. *(**Ascending Chain Condition**, A.C.C) Ogni catena ascendente di Σ*

$$x_0 \leq x_1 \leq x_2 \leq \dots$$

   è stazionaria, cioè esiste $n \in \mathbb{N}$ tale che $x_n = x_{n+1} = x_{n+2} = \dots$

2. *(**Maximal condition**) Ogni sottoinsieme non vuoto di Σ possiede elementi massimali.*

Dimostrazione.
(1) $\Rightarrow$ (2) Sia $\emptyset \neq A \subseteq \Sigma$, supponiamo per assurdo che A non abbiamo elementi massimali. Sia $x_0 \in A$, dato che x_0 non è massimale esiste $x_1 \in A$ tale che $x_0 < x_1$. Allo stesso modo, x_1 non è massimale quindi esiste $x_2 \in A$ tale che $x_1 < x_2$. Procedendo induttivamente in questo modo riusciamo a costruire una catena acendente $x_0 < x_1 < x_2 < \dots$ non stazionaria, assurdo.
(2) $\Rightarrow$ (1) Basta considerare $C = \{x_i : i \in \mathbb{N}\} \subseteq \Sigma$, C ha almeno un elemento massimale x_n, pertanto $x_n = x_i$ per ogni $i \geq n$. □

Diciamo che $(\Sigma, \leq)$ soddisfa la **Descending Chain Condition** (D.C.C.) se $(\Sigma, \geq)$ soddisfa la A.C.C.

Definizione 4.0.2. *Un A-modulo M è detto **noetheriano** se, detto Σ l'insieme dei suoi sottomoduli, $(\Sigma, \subseteq)$ soddisfa la A.C.C. (o equivalentemente la maximal condition).*
*M è detto **artiniano** se $(\Sigma, \subseteq)$ soddisfa la D.C.C.*

Definizione 4.0.3. *Un anello A è **noetheriano** [**artiniano**] se lo è come A-modulo (cioè se vale la A.C.C [D.C.C] sugli ideali)*

Proposizione 4.0.4. *Per ogni A-modulo M si ha*

$$M \text{ è noetheriano } \Leftrightarrow \text{ ogni sottomodulo di } M \text{ è di tipo finito.}$$

Dimostrazione.

- $\Rightarrow$ Sia N un sottomodulo di M. Supponiamo per assurdo che N non sia di tipo finito. Siano quindi $x_0 \in N$, $x_1 \in N \setminus (Ax_0)$, $x_2 \in N \setminus (Ax_0 + Ax_1)$ e così via. In questo modo riusciamo a costruire una catena ascendente di sottomoduli di M che non è stazionaria, assurdo.

- $\Leftarrow$ Sia $N_0 \subseteq N_1 \subseteq N_2 \subseteq \ldots$ una catena ascendente di sottomoduli di M. Consideriamo $N = \bigcup_{i\in\mathbb{N}} N_i$, N è un sottomodulo di M, quindi è di tipo finito, cioè esistono $x_1, x_2, \ldots, x_n \in N$ tali che $N = Ax_1 + \ldots + Ax_n$. Ne segue che essendo $x_i \in N = \bigcup_{k\in\mathbb{N}} N_k$ esiste $h \in \mathbb{N}$ tale che $x_1, x_2, \ldots, x_n \in N_h$, pertanto $N = Ax_1 + \ldots Ax_n \subseteq N_h \subseteq N$ da cui per ogni $i \geq h$ abbiamo
$$N_h \subseteq N_i \subseteq \bigcup_{k\in\mathbb{N}} N_k = N = N_h \Rightarrow N_i = N_h.$$

□

Esempio 4.0.5. *$\mathbb{Z}$ è un anello noetheriano (è un PID), ma non è artiniano, infatti la seguente*
$$(1) \supseteq (2) \supseteq (4) \supseteq \ldots \supseteq (2^n) \supseteq \ldots$$
è una catena discendente infinita.
$k[x_i : i \in \mathbb{N}]$, con k campo, non è noetheriano, infatti la seguente
$$(x_1) \subseteq (x_1x_2) \subseteq (x_1x_2x_3) \subseteq (x_1x_2x_3x_4) \subseteq \ldots$$
è una catena ascendente infinita. Non è neanche artiniano, infatti la seguente
$$(x_1) \supseteq (x_1^2) \supseteq (x_1^3) \supseteq \ldots$$
è una catena discendente infinita.
Osserviamo che se A è un anello noetheriano, non è detto che ogni suo sottoanello $B \subseteq A$ sia anch'esso noetheriano. Basta considerare dall'esempio precedente
$$B = k[x_i : i \in \mathbb{N}] \subseteq k(x_i : i \in \mathbb{N}) = A,$$
infatti A è noetheriano poiché è un campo, mentre B non lo è.

Proposizione 4.0.6. *Sia*
$$0 \to M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$$
una successione esatta di A-moduli. Allora
$$M \text{ è noetheriano [artiniano]} \Leftrightarrow M' \text{ e } M'' \text{ sono noetheriani [artiniani].}$$

Dimostrazione. Proviamo il caso noetheriano, il caso artiniano è analogo.

- $\Rightarrow$ Se $N_0 \subseteq N_1 \subseteq \ldots$ è una catena ascendente di sottomoduli di M' allora $u(N_0) \subseteq u(N_1) \subseteq \ldots$ è una catena ascendente di sottomoduli di M, quindi è stazionaria, cioè esiste $n \in \mathbb{N}$ tale che $u(N_n) = u(N_i)$ per ogni $i \geq n$. Dato che u è iniettiva, abbiamo che $u^{-1}(u(N_i)) = N_i$, da cui segue che anche la catena in M' è stazionaria. Si procede in modo analogo per le catene ascendenti di M'', infatti v è suriettiva quindi abbiamo $v(v^{-1}(N_i)) = N_i$.

$\Leftarrow$ Sia $N_0 \subseteq N_1 \subseteq N_2 \subseteq \ldots$ una catena ascendente di sottomoduli di M. Consideriamo le due catene ascendenti $u^{-1}(N_0) \subseteq u^{-1}(N_1) \subseteq u^{-1}(N_2) \subseteq \ldots$, $v(N_0) \subseteq v(N_1) \subseteq v(N_2) \subseteq \ldots$ di sottomoduli rispettivamente di M' e M''. Esse sono entrambe stazionarie, pertanto esiste $h \in \mathbb{N}$ tale che $u^{-1}(N_i) = u^{-1}(N_h)$, $v(N_i) = v(N_h)$ per ogni $i \geq h$. Supponiamo per assurdo che $N_h \subsetneq N_{h+1}$, sia $x \in N_{h+1} \setminus N_h$. Se esiste $y \in M'$ tale che $x = u(y)$ allora $y \in u^{-1}(N_{h+1}) = u^{-1}(N_h)$, da cui $x = u(y) \in N_h$, assurdo. Pertanto $x \notin \operatorname{Im} u = \ker v$, quindi $v(x) \neq 0$, $v(x) \in v(N_{h+1}) = v(N_h)$, pertanto esiste $x' \in N_h$ tale che $v(x') = v(x) \Leftrightarrow v(x - x') = 0$ da cui $x - x' \in \ker v = \operatorname{Im} u$, quindi esiste $z \in M'$ tale che $u(z) = x - x' \in N_{h+1}$, ma $x \notin N_h$ pertanto $x - x' \notin N_h$, dunque $z \in u^{-1}(N_{h+1}) \setminus u^{-1}(N_h)$, assurdo.

□

Corollario 4.0.7. *Se M è un A-modulo e $N \subseteq M$ è un suo sottomodulo, allora M è noetheriano [artiniano] se e solo se N e M/N sono noetheriani [artiniani].*
In particolare se M è noetheriano [artiniano] il quoziente M/N è noetheriano [artiniano].

Dimostrazione. In base alla proposizione precedente, basta considerare la seguente successione esatta

$$0 \to N \xrightarrow{i} M \xrightarrow{\pi} M/N \to 0$$

□

Osserviamo che se I è un ideale di A, se A è noetheriano allora A/I è noetheriano (come A-modulo). (DA FARE) è un anello noetheriano

Corollario 4.0.8. *Siano M_1, M_2 due A-moduli, allora*

$$M_1, M_2 \text{ sono noetheriani [artiniani] } \Leftrightarrow M_1 \oplus M_2 \text{ è noetheriano [artiniano]}$$

Dimostrazione. Basta considerare la successione esatta

$$0 \to M_1 \xrightarrow{i} M_1 \oplus M_2 \xrightarrow{p_2} M_2 \to 0$$

dove $p_2(x, y) = y$. □

Analogo discorso vale nel caso generale $M_1 \oplus M_2 \oplus \ldots \oplus M_n$, basta applicare induttivamente il precedente corollario.

Corollario 4.0.9. *Se A è un anello noetheriano [artiniano] e M è un A-modulo di tipo finito allora M è noetheriano [artiniano].*

Dimostrazione. Per ipotesi esistono $x_1, x_2, \ldots, x_n \in M$ tali che $M = Ax_1 + Ax_2 + \ldots + Ax_n$. Consideriamo l'omomrfismo suriettivo

$$\varphi : \bigoplus_{i=1}^{n} A \to M \quad \text{tale che } \varphi(\underline{e_i}) = x_i$$

allora abbiamo

$$A \text{ noetheriano} \Rightarrow \bigoplus_{i=1}^{n} A \text{ noetheriano} \Rightarrow M \simeq \bigoplus_{i=1}^{n} A/\ker\varphi \text{ noetheriano.}$$

□

Corollario 4.0.10. *Sia S una parte moltiplicativa di A. Se A è noetheriano [artiniano] allora anche $S^{-1}A$ è noetheriano [artiniano].*

Dimostrazione. Infatti se $S^{-1}I_0 \subseteq S^{-1}I_1 \subseteq S^{-1}I_2 \subseteq \ldots$ è una catena ascendente di ideali di $S^{-1}A$ allora la catena $I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$ è una catena ascendente di ideali di A. Per ipotesi essa è stazionaria, da cui segue che anche la catena in $S^{-1}A$ è stazionaria. $\square$

Teorema 4.0.11 (Teorema della base di Hilbert)**.** *Se A è noetheriano allora $A[x]$ è noetheriano.*

Dimostrazione. Sia I un ideale di $A[x]$. Supponiamo per assurdo che I non sia finitamente generato. Sia f_1 un polinomio di grado minimo su I e sia $d_1 = \deg(f_1)$. Per ipotesi $I \setminus (f_1) \neq \emptyset$, quindi sia f_2 un polinomio di grado minimo su $I \setminus (f_1)$ e sia $d_2 = \deg(f_2)$. Procedendo induttivamente costuriamo una successione $f_1, f_2, \ldots, f_n, \ldots$ di polinomi di grado rispettivamente $d_1, d_2, \ldots, d_n, \ldots$ e indichiamo con $a_i x^{d_i}$ il termine di grado massimo di f_i. Consideriamo la seguente catena ascendente di ideali in A

$$(a_1) \subseteq (a_1, a_2) \subseteq (a_1, a_2, a_3) \subseteq \ldots$$

essa è stazionaria per ipotesi, pertanto esiste $h \in \mathbb{N}$ tale che $(a_1, \ldots, a_h) = (a_1, \ldots, a_i)$ per ogni $i \geq h$, pertanto $a_{h+1} \in (a_1, a_2, \ldots, a_h)$, dunque esistono $b_1, b_2, \ldots, b_n \in A$ tali che

$$a_{h+1} = b_1 a_1 + b_2 a_2 + \ldots + b_h a_h.$$

Adesso il polinomio

$$f_{h+1} - \sum_{i=1}^{h} b_i f_i x^{d_{h+1} - d_i}$$

ha grado minore di d_{h+1} e appartiene a $I \setminus (f_1, \ldots, f_h)$, assurdo. $\square$

($A[x]$ è noetheriano come anello, cioè come $A[x]$-modulo, non come A-modulo).

Corollario 4.0.12. *Se A è noetheriano allora $A[x_1, x_2, \ldots, x_n]$ è noetheriano.*

Dimostrazione. Basta applicare il teorema precedente per induzione su n. $\square$

In particolare se k è un campo allora $k[x_1, \ldots, x_n]$ è noetheriano.

Corollario 4.0.13. *Se A è un anello noetheriano e B è una A-algebra finitamente generata allora B è noetheriano.*

Dimostrazione. Infatti se A è noetheriano allora lo è anche $f(A)[x_1, x_2, \ldots, x_n]$ pertanto, dato che B è una A-algebra finitamente generata esistono $b_1, b_2, \ldots, b_n \in B$ tali che

$$B = f(A)[b_1, b_2, \ldots, b_n] \simeq \frac{f(A)[x_1, x_2, \ldots, x_n]}{(x_1 - b_1, x_2 - b_2, \ldots, x_n - b_n)},$$

ne segue che anche B è noetheriano. $\square$

Proposizione 4.0.14. *Se A è un anello noetheriano e I è un ideale allora esiste $n \in \mathbb{N}$ tale che*

$$\left(\sqrt{I}\right)^n \subseteq I.$$

Dimostrazione. Infatti $\sqrt{I} = (a_1, \ldots, a_t)$, per ogni a_i esiste n_i tale che $a_i^{n_i} \in I$, quindi basta prendere $n = \sum_{i=1}^{t} n_i$ per cui si abbia $\left(\sqrt{I}\right)^n \subseteq I$. □

Corollario 4.0.15. *Se A è noetheriano allora $N_A = \sqrt{(0)}$ è nilpotente (cioè esiste $n \in \mathbb{N}$ tale che ${N_A}^n = (0)$).*

4.1 Lunghezza di un modulo

Definizione 4.1.1. *Sia M un A-modulo. Se $N_0, N_1, \ldots, N_h$ sono sottomoduli di M tali che*

$$N_0 \subsetneq N_1 \subsetneq \ldots \subsetneq N_h$$

*allora diremo che la precedente catena ha **lunghezza** h.*
Se $N_0 = (0)$ e $N_h = M$ la catena

$$(0) \subsetneq N_1 \subsetneq \ldots \subsetneq N_{h-1} \subsetneq M$$

*è detta **serie di composizione** se non è raffinabile (cioè se N_{i+1}/N_i è un modulo **semplice**, ossia privo di sottomoduli non banali).*

Definizione 4.1.2. *Siano M un A-modulo e $\mathcal{L}$ l'insieme di tutte le serie di composizione di M. Si definisce **lunghezza** di M come*

$$\lambda(M) = \begin{cases} \min\{h : \text{ lunghezza di } L \in \mathcal{L}\} & \mathcal{L} \neq \emptyset \\ +\infty & \mathcal{L} = \emptyset \end{cases}$$

Teorema 4.1.3. *Sia M un A-modulo e supponiamo che esso abbia una serie di composizione.*

1. *$N \subseteq M \Rightarrow \lambda(N) \leq \lambda(M)$, inoltre $N = M \Leftrightarrow \lambda(N) = \lambda(M)$.*
2. *Ogni catena di sottomoduli di M ha lunghezza minore o uguale a $\lambda(M)$.*
3. *Ogni serie di composizione di M ha lunghezza $\lambda(M)$.*
4. *Ogni catena di sottomoduli di M si raffina con una serie di composizione.*
5. *Una catena di sottomoduli è una serie di composizione se e solo se ha lunghezza $\lambda(M)$.*

Dimostrazione.

1. Sia
$$(0) \subsetneq M_1 \subsetneq \ldots \subsetneq M_{h-1} \subsetneq M \tag{4.1}$$
una serie di composizione di M, allora intersecando con N otteniamo
$$(0) \subseteq N \cap M_1 \subseteq \ldots \subseteq N \cap M_{h-1} \subseteq N.$$

Dato che M_{i+1}/M_i è semplice considerando l'omomorfismo $\varphi : M_{i+1} \cap N \to M_{i+1}/M_i$ composizione dell'immersione $M_{i+1} \cap N \hookrightarrow M_{i+1}$ e della proiezione $M_{i+1} \twoheadrightarrow M_{i+1}/M_i$ allora

$$\ker \varphi = \{x \in M_{i+1} \cap N : x \in M_i\} = M_i \cap N$$

quindi $\dfrac{M_{i+1} \cap N}{M_i \cap N}$ è isomorfo a un sottomodulo di M_{i+1}/M_i che è semplice, pertanto $\dfrac{M_{i+1} \cap N}{M_i \cap N}$ è semplice da cui $\lambda(N) \leq \lambda(M)$. Inoltre ovviamente se $N = M$ allora $\lambda(N) = \lambda(M)$. Viceversa se $\lambda(N) = \lambda(M)$ allora si ha $N \cap M_i \subsetneq N \cap M_{i+1}$ per ogni $i \in \{0, 1, \dots, h-1\}$ (altrimenti $\lambda(N) < \lambda(M)$). Adesso consideriamo

$$(0) \subsetneq N \cap M_1 \subseteq M_1$$

allora deve aversi $N \cap M_1 = M_1 \Rightarrow M_1 \subseteq N$, altrimenti la catena 4.1 sarebbe raffinabile. Pertanto

$$\frac{N \cap M_2}{N \cap M_1} = \frac{N \cap M_2}{M_1} \subseteq M_2/M_1 \text{ che è semplice}$$

quindi, dato che $N \cap M_1 \subsetneq N \cap M_2$, deve aversi $\dfrac{N \cap M_2}{M_1} = M_2/M_1$, cioè $N \cap M_2 = M_2 \Rightarrow M_2 \subseteq N$. Iterando il procedimento dopo un numero finito di passi otteniamo $M \subseteq N$, quindi $N = M$.

2. Sia

$$(0) \subsetneq M_1 \subsetneq M_2 \subsetneq \dots \subsetneq M_{h-1} \subsetneq M$$

una catena qualsiasi di sottomoduli di M di lunghezza h. Dal punto precedente abbiamo che

$$0 < \lambda(M_1) < \lambda(M_2) < \dots < \lambda(M_{h-1}) < \lambda(M) \Rightarrow h \leq \lambda(M).$$

3. Dal punto precedente ogni serie di composizione ha lunghezza minore o uguale a $\lambda(M)$. Ma $\lambda(M)$ è il minimo delle lunghezze di tutte le serie di composizione, da cui abbiamo la tesi.

4. Data una catena

$$(0) \subsetneq M_1 \subsetneq M_2 \subsetneq \dots \subsetneq M_{h-1} \subsetneq M,$$

se essa non è una serie di composizione allora esiste $i \in \{0, 1, \dots, h_1\}$ tale che M_{i+1}/M_i non è semplice, quindi esiste un sottmodulo N tale che $M_i \subsetneq N \subsetneq M_{i+1}$. A questo punto raffiniamo la catena con N e ripetiamo il procedimento, dopo un numero finito di passi passi otteniamo una serie di composizione.

5. $\Rightarrow$ Segue dal punto 3.

   $\Leftarrow$ Se la catena non fosse una serie di composizione potrei raffinarla (in base al punto 4) ottenendo una serie di composizione di lunghezza maggiore di $\lambda(M)$, contro il punto 3.

□

Proposizione 4.1.4. *Un A-modulo M ha una serie di composizione se e solo se M è noetheriano e artiniano.*

Dimostrazione.

$\Rightarrow$ Ovvio

$\Leftarrow$ Se $M \neq (0)$ sia M_1 un sottomodulo massimale tra tutti i sottomoduli propri di M (l'esistenza di M_1 ci è garantita dalla noetherianità di M). Così abbiamo che M/M_1 è semplice. Se $M_1 \neq (0)$ sia M_2 un sottomodulo massimale tra tutti i sottomoduli di M contenuti propriamente in M_1. Come prima M_1/M_2 è semplice. Se $M_2 \neq (0)$ reiteriamo il procedimento su M_2. In questo modo otteniamo una catena discendente di sottmoduli di M

$$M \supsetneq M_1 \supsetneq M_2 \supsetneq \dots$$

Dato che M è artiniano deve esistere un $n \in \mathbb{N}$ tale che $M_n = (0)$ (altrimenti avremmo costruito una catena discendente infinita), ottenendo così una serie di composizione.

□

4.2 Decomposizione primaria negli anelli noetheriani

Definizione 4.2.1. *Un ideale I di A è detto **irriducibile** se*

$$\text{da } I = J \cap H \text{ segue che } I = J \text{ oppure } I = H.$$

Dalla Proposizione 1.1.23 segue subito che ogni ideale primo è irriducibile.

Proposizione 4.2.2. *In un anello noetheriano ogni ideale è intersezione finita di ideali irriducibili.*

Dimostrazione. Supponiamo per assurdo che l'insieme

$$\Sigma = \{I \text{ ideale di } A : I \text{ non è intersezione finita di ideali irriducibili}\}$$

sia non vuoto. Sia M un elemento massimale di Σ, allora M non è irriducibile quindi esistono J, H tali che $M = J \cap H$, $M \subsetneq J, H$, quindi $J, H \notin \Sigma$, pertanto essi sono intersezione finita di ideali irriducibili

$$J = \bigcap_{i=1}^{j} J_i, \quad H = \bigcap_{i=1}^{h} H_i \Rightarrow M = J \cap H = \left(\bigcap_{i=1}^{j} J_i\right) \cap \left(\bigcap_{i=1}^{h} H_i\right),$$

contro $M \in \Sigma$. □

Proposizione 4.2.3. *Se A è un anello noetheriano e I è un ideale irriducibile allora I è primario.*

Dimostrazione. Passando al quoziente basta dimostrare che se (0) è un ideale irriducibile allora è primario. Supponiamo che $xy = 0$ e $x \neq 0$ e consideriamo la catena ascendente

$$\mathrm{Ann}(y) \subseteq \mathrm{Ann}(y^2) \subseteq \mathrm{Ann}(y^3) \subseteq \dots$$

Per ipotesi esiste $h \in \mathbb{N}$ tale che $\mathrm{Ann}(y^h) = \mathrm{Ann}(y^{h+1})$. Adesso sia $z \in (y^h) \cap (x)$, allora esistono $\alpha, \beta \in A$ tali che $z = \alpha x = \beta y^h$, allora

$$zy = \alpha xy = 0 = \beta y^{h+1} \Rightarrow \beta \in \mathrm{Ann}(y^{h+1}) = \mathrm{Ann}(y^h)$$

da cui $z = \beta y^h = 0$, cioè $(x) \cap (y^h) = (0)$. Per ipotesi (0) è irriducibile, da cui dato che $x \neq 0$ deve aversi $(y^h) = (0) \Rightarrow y^h = 0$, cioè $y \in \sqrt{(0)}$. Ciò prova che (0) è primario. □

Corollario 4.2.4. *Se A è noetheriano allora ogni ideale I di A ha una decomposizione primaria*

Corollario 4.2.5. *Se A è noetheriano allora il nilradicale N_A è intersezione finita di primi.*

Dimostrazione. Infatti basta considerare una decomposizione primaria di (0)

$$(0) = Q_1 \cap \dots \cap Q_n$$

da cui passando ai radicali, indicando con $P_i = \sqrt{Q_i}$ risulta

$$N_A = \sqrt{(0)} = \sqrt{Q_1 \cap \dots \cap Q_n} = P_1 \cap \dots \cap P_n.$$

□

Proposizione 4.2.6. *Se A è un anello noetheriano, i primi associati a un ideale I di A sono tutti e soli i primi della forma $(I : x)$, per qualche $x \in A$.*

Dimostrazione. Sia $I = Q_1 \cap Q_2 \cap \dots \cap Q_n$ una decomposizione primaria minimale di I. Avendo posto $J = \bigcap_{j \neq i} Q_j$, dal primo teorema di unicità si ha che per ogni $x \in J \setminus Q_i$ risulta $P_i = \sqrt{(I : x)}$, quindi $(I : x) \subseteq P_i$. Dato che A è noetheriano dalla Proposizione 4.0.14 esiste $m \in \mathbb{N}$ tale che $P_i^m \subseteq Q_i$, quindi $P_i^m J \subseteq Q_i J \subseteq Q_i \cap J = I$. Supponiamo che m sia il più piccolo naturale tale che $P_i^m J \subseteq I$. Se adesso scegliamo $x \in P_i^{m-1} J \setminus I$ allora $xP_i \subseteq I$ quindi $P_i \subseteq (I : x)$. D'altra parte $x \in P_i^{m-1} J \setminus I \subseteq J \setminus Q_i$, quindi $(I : x) \subseteq P_i$. Viceversa se $x \in A$ è tale che $(I : x) = P$ è primo allora $P = \sqrt{(I : x)}$ quindi P è un primo associato ad I. □

4.3 Anelli Artiniani

Proposizione 4.3.1. *Se D è un dominio artiniano allora D è un campo.*

Dimostrazione. Sia $x \in D \setminus \{0\}$, consideriamo la catena discendente

$$(x) \supseteq (x^2) \supseteq (x^3) \supseteq \dots$$

essendo D artiniano la precedente catena è stazionaria, quindi esiste $n \in \mathbb{N}$ tale che $(x^n) = (x^{n+1})$, pertanto esiste $d \in D$ tale che $x^n = dx^{n+1}$. Poiché D è un dominio vale la proprietà di cancellazione, quindi otteniamo $dx = 1$, cioè x è invertibile. □

Proposizione 4.3.2. *Se A è un anello artiniano allora*

1. *Ogni ideale primo è massimale.*
2. $N_A = \mathcal{J}(A)$.
3. *Il numero degli ideali primi è finito.*

Dimostrazione.

1. Sia P un ideale primo di A. Il quoziente A/P è un dominio artiniano, quindi per la proposizione precedente esso è un campo, il che equivale a dire che P è massimale.
2. Segue dal punto precedente.
3. Sia $\mathcal{M}$ l'insieme degli ideali primi (o massimali) di A e sia

$$\Sigma = \{I \text{ ideale di } A : I = P_1 \cap \ldots \cap P_t \text{ con } P_i \in \mathcal{M}\}.$$

$\mathcal{M} \subseteq \Sigma \neq \emptyset$, pertanto, dato che A è artiniano, sia $I = P_1 \cap P_2 \cap \ldots \cap P_t$ ($P_i \in \mathcal{M}$) un elemento minimale di Σ. Sia adesso $P \in \mathcal{M}$, allora

$$I \cap P = P_1 \cap P_2 \cap \ldots \cap P_t \cap P \in \Sigma, \quad I \cap P \subseteq I.$$

Dalla minimalità di I abbiamo che $I \cap P = I$, cioè $I = P_1 \cap \ldots \cap P_t \subseteq P$. Dalla Proposizione 1.1.23 abbiamo che esiste $i \in \{1, \ldots, t\}$ tale che $P_i \subseteq P$, dalla massiamltà di P_i otteniamo $P = P_i$. Pertanto $\mathcal{M} = \{P_1, \ldots, P_t\}$, cioè A ha un numero finito di ideali primi (o massimali).

□

Osservazione 4.3.3. *Se A è un anello artiniano e $P_1, \ldots, P_t$ sono i suoi ideali primi (o massimali) allora possiamo considerare l'omomorfismo*

$$\varphi : A \to \prod_{i=1}^{t} A/P_i, \quad \varphi(a) = (a + P_1, \ldots, a + P_t).$$

Dato che $P_i + P_j = A$ ($i \neq j$) in quanto P_i e P_j sono massimali, in base al teorema cinese del resto φ è suriettiva. Inoltre $\ker \varphi = P_1 \cap \ldots \cap P_t$, pertanto se A è anche ridotto (cioè se $N_A = P_1 \cap \ldots \cap P_t = (0)$) allora A è somma diretta di campi

$$A \simeq \prod_{i=1}^{t} A/P_i$$

quindi A è anche noetheriano.

Vediamo un esempio di modulo artiniano che non è noetheriano.

Esempio 4.3.4. *Sia $G(p^n) \subseteq \mathbb{C}$ l'insieme delle radici p^n-esime dell'unità, dove $p \in \mathbb{N}$ è primo. $G(p^n)$ è un gruppo abeliano (rispetto alla moltiplicazione), quindi è anche uno $\mathbb{Z}$-modulo. Adesso sia*

$$G(p^\infty) = \bigcup_{n \in \mathbb{N}} G(p^n),$$

$G(p^\infty)$ è un gruppo abeliano, quindi è uno $\mathbb{Z}$-modulo. Gli unici suoi sottomoduli sono del tipo $G(p^n)$, pertanto considerando la catena ascendente

$$\langle 1 \rangle \subsetneq G(p) \subsetneq G(p^2) \subsetneq \dots$$

vediamo subito che $G(p^\infty)$ non è noetheriano ma è artiniano.

Proposizione 4.3.5. *Per un k-spazio vettoriale V sono equivalenti*

1. *V ha dimensione finita.*
2. *V ha lunghezza finita.*
3. *V è noetheriano.*
4. *V è artiniano.*

Dimostrazione.

(1) $\Rightarrow$ (2) Sia $V_0 \subsetneq V_1 \subsetneq \dots \subsetneq V_h$ una catena di sottomoduli (e quindi sottospazi vettoriali) di V. Dato che V ha dimensione finita allora deve aversi $h \leq \dim(V)$, quindi V ha lunghezza finita.

(2) $\Rightarrow$ (3) , (2) $\Rightarrow$ (4) seguono dalla Proposizione 4.1.4.

(3) $\Rightarrow$ (1) Per ipotesi V è finitamente generato (come k-modulo), in altri termini esso ha un insieme di generatori finito (come k-spazio vettoriale) da cui possiamo estrarre una base finita, pertanto V ha dimensione finita.

(4) $\Rightarrow$ (1) Per assurdo supponiamo che V abbia dimensione infinita e sia $X = \{x_i : i \in \mathbb{N}\} \subseteq V$ un insieme linearmente indipendente numerabile. Per ogni $i \in \mathbb{N}$ poniamo $V_i = \mathcal{L}(x_i, x_{i+1}, x_{i+2}, \dots)$, abbiamo così ottenuto una catena discendente

$$V_0 \supsetneq V_1 \supsetneq V_2 \supsetneq \dots$$

non stazionaria, contro l'artinianità di V.

□

Corollario 4.3.6. *Se A è un anello tale che $(0) = M_1 M_2 \cdots M_n$, dove gli M_i sono ideali massimali (non necessariamente distinti), allora*

$$A \text{ è noetheriano } \Leftrightarrow A \text{ è artiniano.}$$

Dimostrazione. Osserviamo che per ogni $i \in \{1, \dots, n\}$ A/M_i è un campo, inoltre il quoziente $M_1 M_2 \dots M_i / M_1 M_2 \dots M_{i+1}$ è annullato da M_{i+1} quindi è un A/M_{i+1}-spazio vettoriale, analogamente anche il prodotto $M_1 M_2 \dots M_{n-1}$ è un A/M_n-spazio vettoriale, pertanto per questi la A.C.C. è equivalente alla D.C.C. in base alla proposizione precedente. Dunque consideriamo le catene esatte corte

$$0 \to M_1 \dots M_{n-1} \to M_1 \dots M_{n-2} \to \frac{M_1 \dots M_{n-2}}{M_1 \dots M_{n-1}} \to 0$$
$$0 \to M_1 \dots M_{n-2} \to M_1 \dots M_{n-3} \to \frac{M_1 \dots M_{n-3}}{M_1 \dots M_{n-2}} \to 0$$
$$\vdots$$
$$0 \to M_1 M_2 \to M_1 \to \frac{M_1}{M_1 M_2} \to 0$$
$$0 \to M_1 \to A \to A/M_1 \to 0.$$

Applicando ripetutamente la Proposizione 4.0.6 otteniamo che se vale la A.C.C. [D.C.C.] per A allora vale anche per M_1 e A/M_1, quindi vale anche per $M_1 M_2$ e $M_1/M_1 M_2$ e così via risalendo fino a $M_1 \dots M_{n-1}$ e $M_1 \dots M_{n-2}/M_1 \dots M_{n-1}$. Per questi ultimi la A.C.C. e la D.C.C. sono condizioni equivalenti, pertanto, sempre per la Proposizione 4.0.6, anche per $M_1 \dots M_{n-2}$ vale la D.C.C. [A.C.C.], quindi vale anche per $M_1 \dots M_{n-3}$ (ricordando che per ogni quoziente $M_1 \dots M_{i+1}/M_1 \dots M_i$ la A.C.C. è equivalente alla D.C.C) e così via risalendo fino ad A. □

Proposizione 4.3.7. *Se A è aritiniano N_A è nilpotente.*

Dimostrazione. Per ipotesi la catena discendente

$$N_A \supseteq N_A^2 \supseteq N_A^3 \supseteq \dots$$

è stazionaria, pertanto esiste $n \in \mathbb{N}$ tale che $N_A^n = N_A^{n+1}$. Per assurdo supponiamo che $I = N_A^n \neq (0)$. Sia $\Sigma = \{J \text{ ideale di } A : JI \neq (0)\}$, abbiamo che $N_A I = N_A^{n+1} = N_A^n = I \neq (0)$, pertanto $N_A \in \Sigma \neq \emptyset$. Sia allora H un elemento minimale di Σ. Per definizione abbiamo che $H \neq (0)$ quindi esiste $h \in H$ tale che $hI \neq (0)$, pertanto $(h) \in \Sigma$. Dalla minimalità di H segue che $H = (h)$. D'altra parte si ha

$$(hI)I = hI^2 = hN_A^{2n} = hN_A^n = hI \neq (0) \quad hI \subseteq (h) = H$$

quindi $hI = (h)$, ne segue che esiste $i \in I$ tale che $h = hi$ da cui per induzione segue facilmente che

$$h = hi^n \quad \forall n \in \mathbb{N}.$$

Ma $i \in I = N_A^n \subseteq N_A$, quindi esiste $m \in \mathbb{N}$ tale che $i^m = 0$, pertanto $h = hi^m = 0 \Rightarrow H = (0)$, assurdo. □

Teorema 4.3.8. *Sia A un anello.*

A è artiniano $\Leftrightarrow$ A è noetheriano e ogni ideale primo è massimale.

Dimostrazione.

⇒ Dalla Proposizione 4.3.2 abbiamo che ogni ideale primo è massimale e che A ha un numero finito di ideali primi, quindi $N_A = \bigcap_{i=1}^n P_i$. Inoltre, dalla proposizione precedente N_A è nilpotente quindi esiste $m \in \mathbb{N}$ tale che $N_A^m = (0)$. In aggiunta abbiamo che $P_i + P_j = A$ per $i \neq j$ (essendo ideali massimali) pertanto risulta

$$(0) = N_A^m = \bigcap_{i=1}^n P_i^m = \prod_{i=1}^n P_i^m.$$

Dal Corollario 4.3.6 abbiamo che A è noetheriano.

⇐ Da 4.2.5 sappiamo che N_A è intersezione finita di ideali primi, inoltre da 4.0.15 sappiamo che il nilradicale è nilpotente, cioè $\left(\bigcap_{i=1}^n P_i\right)^k = N_A^k = (0)$, dato che ogni primo è massimale abbiamo che $P_i + P_j = A$ da cui

$$(0) = N_A^k = \left(\bigcap_{i=1}^n P_i\right)^k = \left(\prod_{i=1}^n P_i\right)^k = \prod_{i=1}^n P_i^k,$$

pertanto dal Corollario 4.3.6 A è artiniano.

□

Osservazione 4.3.9. *Sia (A, M) un anello locale noetheriano. Consideriamo la catena discendente*

$$M \supseteq M^2 \supseteq M^3 \supseteq \dots$$

dato che M^i è finitamente generato per ogni $i \in \mathbb{N}$ e $\mathcal{J}(A) = M$, dal lemma di Nakayama segue che se $M^{i+1} = MM^i = M^i$ allora $M^i = (0)$. Dunque ci sono due possibilità: o $M^i \supsetneq M^{i+1}$ per ogni $i \in \mathbb{N}$, oppure esiste $i \in \mathbb{N}$ tale che $M^i = (0)$. Nel primo caso otteniamo una catena discendente non stazionaria, quindi A non è artiniano. Nel secondo caso per ogni ideale primo P si ha

$$M^i = (0) \subseteq P \Rightarrow M = \sqrt{M^i} \subseteq \sqrt{P} = P \Rightarrow M = P.$$

In altri termini ogni ideale primo è massimale (cioè ogni ideale primo è uguale all'unico ideale massimale di A). Pertanto dalla proposizione precedente avremmo che A è artiniano.

Capitolo 5

Dipendenza integrale

5.1 Estensioni di anelli

Definizione 5.1.1. *Se A è un sottoanello di B l'inclusione $A \subseteq B$ si chiama **estensione di anelli**.*
*L'estensione di anelli $A \subseteq B$ è **finita** se B è un A-modulo di tipo finito. Si parla di estensione **finitamente generata** se B è una A-algebra finitamente generata.*

Proposizione 5.1.2. *Un'estensione di anelli $A \subseteq B$ finita è finitamente generata.*

Dimostrazione. Basta osservare che se $B = Ax_1 + \ldots + Ax_n$ allora $B = A[x_1, \ldots, x_n]$. □

5.2 Estensioni integrali

Definizione 5.2.1. *Sia $A \subseteq B$ un'estensione di anelli. Diremo che $b \in B$ è **intero** su A se esiste un polinomio monico $f \in A[x]$ tale che $f(b) = 0$.*

Nel caso in cui A sia un campo $x \in B$ è intero se e solo se è algebrico su A.
Ovviamente ogni $a \in A$ è intero su A essendo radice del polinomio $x - a$.

Definizione 5.2.2. *Un'estensione di anelli $A \subseteq B$ è **intera** (o **integrale**) se ogni elemento $x \in B$ è intero su A. In questo caso si dice che l'anello B è **intero** su A*

Proposizione 5.2.3. *Sia $A \subseteq B$ un'estensione di anelli. Le seguenti condizioni sono equivalenti*

1. *$x \in B$ è intero su A.*
2. *$A[x]$ è un A-modulo di tipo finito.*
3. *$A[x] \subseteq C \subseteq B$ dove l'anello C è un A-modulo di tipo finito.*
4. *Esiste un $A[x]$-modulo M fedele che è un A-modulo di tipo finito.*

Dimostrazione.

(1) ⇒ (2) Se $x \in B$ è intero su A allora

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0 \quad a_i \in A$$

da cui si ha

$$x^n = -(a_{n-1}x^{n-1} + \ldots + a_1 x + a_0),$$

quindi si dimostra facilmente per induzione che $x^m \in A + Ax + \ldots + Ax^{n-1}$ per ogni $m \geq n$. Da cui $A[x] = A + Ax + \ldots + Ax^{n-1}$, cioè $A[x]$ è un A-modulo di tipo finito.

(2) ⇒ (3) $C = A[x]$.

(3) ⇒ (4) $M = C$, C è fedele poiché $\mathrm{Ann}(C) \subseteq \mathrm{Ann}(1) = (0)$.

(4) ⇒ (1) Per ipotesi $M = Ax_1 + \ldots + Ax_n$, quindi si ha

$$\begin{aligned} xx_1 &= a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \\ xx_2 &= a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n \\ &\vdots \\ xx_n &= a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n \end{aligned}$$

da cui per ogni $i \in \{1, \ldots, n\}$

$$\sum_{j=1}^{n} (\delta_{ij}x - a_{ij})x_j = 0.$$

Dunque moltiplicando per la matrice $A^{\#}$ trasposta della matrice aggiunta di $A = (\delta_{ij}x - a_{ij})$ si ha che $\det(A^{\#})x_i = 0$ per ogni $i \in \{1, \ldots, n\}$. Dato che M è fedele deve aversi $\det(A^{\#}) = f(x) = 0$, dove f è un polinomio monico a coefficienti in A.

□

Corollario 5.2.4. *Sia $A \subseteq B$ un'estensione di anelli. Se $x_1, \ldots, x_n \in B$ sono interi su A allora l'estensione $A \subseteq A[x_1, \ldots, x_n]$ è finita.*

Dimostrazione. Procediamo per induzione su n. Per $n = 1$ la tesi segue dalla proposizione precedente. Supponiamo il teorema vero per $n-1$ e dimostriamolo per n. Dall'ipotesi induttiva abbiamo che entrambe le estensioni $A \subseteq A[x_1, \ldots, x_{n-1}]$ e $A[x_1, \ldots, x_{n-1}] \subseteq A[x_1, \ldots, x_{n-1}][x_n] = A[x_1, \ldots, x_n]$ sono finite, ne segue la tesi. □

Corollario 5.2.5. *Un'estensione di anelli $A \subseteq B$ è finita se e solo se è intera e finitamente generata.*

Dimostrazione.

⇒ Abbiamo già visto che ogni estensione finita è finitamente generata. Per ogni $x \in B$ abbiamo che $A[x] \subseteq B$ e B è un A-modulo di tipo finito pertanto dalla proposizione precedente segue che x è intero su A.

$\Leftarrow$ Per ipotesi $B = A[x_1, \ldots, x_n]$, inoltre B è intero su A quindi $x_1, \ldots, x_n \in B$ sono interi su A. La tesi segue dal corollario precedente.

$\square$

Proposizione-Definizione 5.2.6. *Data un'estensione di anelli $A \subseteq B$ l'insieme*

$$\overline{A^B} = \{x \in B : x \text{ è intero su } B\}$$

è un anello detto ***chiusura integrale*** *di A in B.*
Se $\overline{A^B} = A$ allora A è detto ***integralmente chiuso*** *in B.*
Se $\overline{A^B} = B$ allora B è intero su A.
Se A è un dominio diremo che A è ***integralmente chiuso****, senza specificare rispetto a quale anello, quando A è integralmente chiuso nel suo campo dei quozienti $Q(A)$.*

Dimostrazione. Siano $x, y \in \overline{A^B}$. Da un precedente corollario abbiamo che l'estensione $A \subseteq A[x, y]$ è finita, quindi è anche intera, pertanto $x \pm y, xy \in A[x, y]$ sono interi su A. $\square$

Proposizione 5.2.7 (Transitività delle estensioni integrali)**.** *Se $A \subseteq B \subseteq C$ sono estensioni di anelli allora*

$$A \subseteq C \text{ è intera } \iff A \subseteq B,\ B \subseteq C \text{ sono intere.}$$

Dimostrazione.

- $\Rightarrow$ Se $c \in C$ è intero su A allora è intero anche su B (basta osservare che $A[x] \subseteq B[x]$). Inoltre ogni $b \in B \subseteq C$ è intero su A.

- $\Leftarrow$ Sia $c \in C$, per ipotesi c è intero su B quindi esiste $f \in B[x]$ monico tale che

  $$f(c) = c^n + b_{n-1}c^{n-1} + \ldots + b_1 c + b_0 = 0, \quad b_i \in B.$$

  Adesso $b_0, \ldots, b_{n-1} \in B$ sono interi su A e c è intero su $A[b_0, \ldots, b_{n-1}]$, pertanto le estensioni

  $$A \subseteq A[b_0, \ldots, b_{n-1}] \subseteq A[b_0, \ldots, b_{n-1}, c]$$

  sono finite, ne segue che $A \subseteq A[b_0, \ldots, b_{n-1}, c]$ è finita, quindi c è intero su A.

$\square$

Proposizione 5.2.8. *Ogni UFD è integralmente chiuso.*

Dimostrazione. Sia $\frac{r}{s} \in Q(A)$ intero su A, con $r, s \in A$ primi tra di loro. Allora abbiamo una relazione del tipo

$$r^n + a_1 r^{n-1} s + \ldots + a_{n-1} r s^{n-1} + a_n s^n = 0$$

da cui s divide r^n, cioè r, quindi s è invertibile e $\frac{r}{s} \in A$. $\square$

Proposizione 5.2.9. *Sia $A \subseteq B$ un'estensione integrale.*

1. *Se $J \trianglelefteq B$ e $I = J^c = J \cap A$, allora $A/I \subseteq B/J$ è un'estensione integrale.*

2. *Se S è un parte moltiplicativa di A (quindi anche di B) allora $S^{-1}A \subseteq S^{-1}B$ è un'estensione integrale.*

Dimostrazione.

1. Considerando la composizione $A \hookrightarrow B \twoheadrightarrow B/J$ il nucleo è $J \cap A = I$, quindi $A/I \subseteq B/J$. Adesso dato $b + J \in B/J$, sappiamo che $b \in B$ è intero su A, quindi esiste un polinomio $f \in A[x]$ monico tale che $f(b) = 0$. Passando alle classi di resto modulo J si ha che $\overline{f} \in A/I[x]$ con $\overline{f}(b + J) = \overline{0}$ quindi $b + J$ è intero su A/I.

2. Consideriamo $\phi : S^{-1}A \to S^{-1}B$ con $\phi\left(\frac{a}{s}\right) = \frac{a}{s}$. Adesso

$$\phi\left(\frac{a}{s}\right) = \frac{a}{s} = \frac{0}{1} = 0_{S^{-1}B} \Leftrightarrow \exists u \in S :\ ua = 0 \Leftrightarrow \frac{a}{s} = \frac{0}{1} = 0_{S^{-1}A},$$

pertanto ϕ è un omomorfismo iniettivo.
Adesso sia $\frac{b}{s} \in S^{-1}B$, $b \in B$ è intero su A, quindi

$$b^n + a_{n-1}b^{n-1} + \ldots + a_1 b + a_0 = 0$$

dividendo ambo i membri per s^n otteniamo

$$\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s}\left(\frac{b}{s}\right)^{n-1} + \ldots + \frac{a_1}{s^{n-1}}\frac{b}{s} + \frac{a_0}{s^n} = 0,$$

pertanto $\frac{b}{s}$ è intero su $S^{-1}A$.

$\square$

5.3 Going up e going down

Proposizione 5.3.1. *Sia $A \subseteq B$ un'estensione integrale di domini. Sotto queste ipotesi A è un campo se e solo se B è un campo.*

Dimostrazione.

$\Rightarrow$ Sia $b \in B \setminus 0$, b è intero su A quindi per ipotesi b soddisfa una relazione del tipo

$$b^n + a_{n-1}b^{n-1} + \ldots + a_i b + a_0 = 0,$$

con $a_i \in A$. Inoltre possiamo supporre che essa sia di grado minimo, quindi, dato che b non è uno zerodivisore risulta $a_0 \neq 0$, da cui otteniamo

$$b(b^{n-1} + a_{n-1}b^{n-2} + \ldots + a_1)(-a_0)^{-1} = 1,$$

pertanto b è invertibile.

$\Leftarrow$ Sia $a \in A \setminus \{0\}$, $a^{-1} \in B$ è intero su A, pertanto ($a_i \in A$)

$$a^{-n} + a_{n-1}a^{-(n-1)} + \ldots + a_1 a^{-1} + a_0 = 0$$
$$a^{-1} = -(a_{n-1} + \ldots a_1 a^{n-2} + a_0 a^{n-1}) \in A.$$

□

Corollario 5.3.2. *Sia $A \subseteq B$ un'estensione integrale, se Q è un ideale primo di B allora posto $P = Q \cap A$ si ha che Q è massimale se e solo se P è massimale.*

Dimostrazione. Dalla 5.2.9 sappiamo che l'estensione di domini $A/P \subseteq B/Q$ è integrale. La tesi segue adesso dalla proposizione precedente. □

Proposizione 5.3.3 (Incomparability)**.** *Sia $A \subseteq B$ un'estensione integrale. Se P è un ideale primo di A e $Q \subseteq Q'$ sono due ideali primi di B tali che $P = Q \cap A = Q' \cap A$ allora $Q = Q'$.*

Dimostrazione. Sia $S = A \backslash P$. Per 5.2.9 sappiamo che l'estensione $S^{-1}A \subseteq S^{-1}B$ è intera. In $S^{-1}A$ l'ideale $S^{-1}P$ è l'unico ideale massiamle. Dato che $S \cap Q = S \cap Q' = S \cap P = \emptyset$ gli ideali $S^{-1}Q$ ed $S^{-1}Q'$ sono primi. Inoltre

$$S^{-1}Q \cap S^{-1}A = S^{-1}(Q \cap A) = S^{-1}P$$

analogamente $S^{-1}Q' \cap S^{-1}A = S^{-1}P$. Dal corollario precedente segue che $S^{-1}Q$ ed $S^{-1}Q'$ sono massimali, da cui poiché $S^{-1}Q \subseteq S^{-1}Q'$ si ha $S^{-1}Q = S^{-1}Q'$ da cui $Q = Q'$. □

Teorema 5.3.4 (Lying over)**.** *Sia $A \subseteq B$ un'estensione integrale. Se P è un ideale primo di A allora esiste un ideale primo Q di B tale che $Q \cap A = P$.*

Dimostrazione. Sia $S = A \setminus P$. Consideriamo il seguente diagramma commutativo

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d] & S^{-1}A \arrow[d] \\ B \arrow[r, "\beta"] & S^{-1}B \end{tikzcd}$$

Di nuovo $S^{-1}P$ è l'unico ideale massimale di $S^{-1}A$. Sia N un ideale massimale di $S^{-1}B$, allora $N \cap S^{-1}A$ è massimale (corollario precedente), pertanto $N \cap S^{-1}A = S^{-1}P$, quindi $\alpha^{-1}(N \cap S^{-1}A) = P$ (ricordiamo che gli ideali primi di $S^{-1}A$ sono in corrispondenza biunivoca con gli ideali primi di A contenuti in P). Ma dato che il precedente diagramma è commutativo si ha $P = \alpha^{-1}(N \cap S^{-1}A) = \beta^{-1}(N) \cap A$, inoltre $Q = \beta^{-1}(N)$ è un ideale primo di B. □

Teorema 5.3.5 (Going up)**.** *Sia $A \subseteq B$ un'estensione integrale. Se $P_0 \subset P_1 \subset \ldots \subset P_n$ è una catena di ideali primi di A e $Q_0 \subset Q_1 \subset \ldots \subset Q_i$ è una catena di primi di B tali che $Q_j \cap A = P_j$ per ogni $j \leq i$, allora esistono $Q_{i+1} \subset Q_{i+2} \subset \ldots \subset Q_n$ ideali primi di B tali che $Q_j \cap A = P_j$ per ogni $j \geq i+1$ e $Q_i \subset Q_{i+1}$.*

Dimostrazione. Ci possiamo ridurre al caso $n = 1$, $i = 0$. Consideriamo l'estensione integrale $A/P_0 \subseteq B/Q_0$, dato che $\overline{P_1} = P_1/P_0$ è primo, per il teorema del lying over esiste un ideale primo $\overline{Q_1} = Q_1/Q_0$ di B/Q_0 tale che $\overline{Q_1} \cap A/P_0 = \overline{P_1}$. □

Corollario 5.3.6. *Se $A \subseteq B$ è un'estensione integrale allora* $\dim A = \dim B$ *(dimensione di Krull definita dopo).*

Dimostrazione. Infatti ogni catena di primi in B $Q_0 \subset Q_1 \subset \ldots \subset Q_n$ produce una catena in A facendo le intersezioni $P_i = Q_i \cap A$. Il viceversa segue dai teoremi del lying over e del going up. $\square$

Teorema 5.3.7 (Going down)**.** *Sia $A \subseteq B$ un'estensione integrale di domini e A integralmente chiuso. Data una catena di ideali primi $P_0 \subset P_1 \subset \ldots \subset P_n$ in A e una catena $Q_i \subset Q_{i+1} \subset \ldots \subset Q_n$ tale che $Q_j \cap A = P_j$ per ogni $j \geq i$ allora esistono ideali primi $Q_0 \subset Q_1 \subset Q_{i-1}$ di B tali che $Q_j \cap A = P_j$ per ogni $j \leq i-1$ e $Q_{i-1} \subset Q_i$.*

Se il teorema del going down è verificato allora anche l'altezza degli ideali si mantiene.

Proposizione 5.3.8. *Sia $A \subseteq B$ un'estensione integrale e P un ideale primo di A. Se Q è un ideale primo di B che si contrae in P allora Q è un primo minimale su P^e.*

Dimostrazione. Sia Q' un ideale primo di B tale che $P^e \subseteq Q' \subseteq Q$, risulta

$$P \subseteq P^{ec} = P^e \cap A \subseteq Q' \cap A \subseteq Q \cap A = P,$$

quindi $Q' \cap A = P$, dall'incomparability segue $Q' = Q$. $\square$

Corollario 5.3.9. *Sia $A \subseteq B$ un'estensione integrale e supponiamo che B sia noetheriano. Se P è un ideale primo di A allora il numero di ideali primi di B che si contraggono in P è finito.*

Dimostrazione. Poiché B è noetheriano, P^e ha una decomposizione primaria, quindi ha un numero finito di primi minimali. La tesi segue dalla proposizione precedente. $\square$

Capitolo 6

Varietà algebriche affini

Sia k un campo. Indichiamo con $\mathbb{A}^n(k)$ lo spazio affine n-dimensionale su k.

Definizione 6.0.1. *Dato* $F \subseteq k[x_1, \dots, x_n]$ *poniamo*

$$V(F) = \{P \in \mathbb{A}^n(k) : f(P) = 0 \quad \forall f \in F\} \subseteq \mathbb{A}^n(k).$$

L'insieme $V(F)$ *è detto* ***varietà algebrica affine***.

Osserviamo che tutti i polinomi appartenenti all'ideale generato da F si annullano in tutti i punti di $V(F)$. In altri termini se $I = \langle F \rangle = \{\sum_{i=1}^n a_i f_i : a_i \in k[x_1, \dots, x_n], f_i \in F\}$ è l'ideale generato da F allora

$$V(F) = V(I).$$

Dato che $k[x_1, \dots, x_n]$ è noetheriano allora ogni suo ideale è finitamente generato. Pertanto ogni varietà algebrica affine è l'insieme dei punti di $\mathbb{A}^n(k)$ che soddisfano un numero finito di equazioni polinomiali

$$f_i(x_1, \dots, x_n) = 0 \quad (i = 1, \dots, m).$$

Definizione 6.0.2. *Dato* $X \subseteq \mathbb{A}^n(k)$ *definiamo l'insieme*

$$\mathscr{I}(X) = \{f \in k[x_1, \dots, x_n] : f(P) = 0 \quad \forall P \in X\} \subseteq k[x_1, \dots, x_n].$$

È facile verificare che per ogni $X \subseteq \mathbb{A}^n(k)$ l'insieme $\mathscr{I}(X)$ è un ideale di $k[x_1, \dots, x_n]$.

Abbiamo così definito due applicazioni

$$\begin{array}{llcll} V: & \{I \trianglelefteq k[x_1, \dots, x_n]\} & \to & \mathcal{P}(\mathbb{A}^n(k)) & I \mapsto V(I) \\ \mathscr{I}: & \mathcal{P}(\mathbb{A}^n(k)) & \to & \{I \trianglelefteq k[x_1, \dots, x_n]\} & X \mapsto \mathscr{I}(X). \end{array}$$

Proposizione 6.0.3.

1. $I \subseteq \mathscr{I}(V(I))$
2. $I \subseteq J \Rightarrow V(I) \supseteq V(J)$
3. $V(\mathscr{I}(V(I))) = V(I)$
4. $V(1) = \emptyset$, $V(0) = \mathbb{A}^n(k)$.
5. $V\left(\sum_{\lambda\in\Lambda} I_\lambda\right) = \bigcap_{\lambda\in\Lambda} V(I_\lambda)$
6. $V(IJ) = V(I\cap J) = V(I)\cup V(J)$

1. $X \subseteq V(\mathscr{I}(X))$
2. $X \subseteq Y \Rightarrow \mathscr{I}(X) \supseteq \mathscr{I}(Y)$
3. $\mathscr{I}(V(\mathscr{I}(X))) = \mathscr{I}(X)$
4. $\mathscr{I}(\mathbb{A}^n(k)) = (0), \mathscr{I}(\emptyset) = k[\,\underline{x}\,]$
5. $\mathscr{I}(\bigcup_{\lambda\in\Lambda} X_\lambda) = \bigcap_{\lambda\in\Lambda} \mathscr{I}(X_\lambda)$
6. $\mathscr{I}(X\cap Y) \supseteq \mathscr{I}(X) + \mathscr{I}(Y)$

Dimostrazione.

1. Se $f \in I$ allora $f(P) = 0$ per ogni $P \in V(I)$, cioè $f \in \mathscr{I}(V(I))$.
2. Se $P \in V(J)$ allora $f(P) = 0$ per ogni $f \in I \subseteq J$ quindi $P \in V(I)$.
3. $V(I) \subseteq V(\mathscr{I}(V(I)))$ (punto 1), $I \subseteq \mathscr{I}(V(I)) \Rightarrow V(I) \supseteq V(\mathscr{I}(V(I)))$ (punto 2).
4. $1(P) = 1 \neq 0$ per ogni $P \in \mathbb{A}^n(k)$, mentre $0(P) = 0$ per ogni $P \in \mathbb{A}^n(k)$.
5. $\subseteq$ Se $P \in V\left(\sum_{\lambda\in\Lambda} I_\lambda\right)$ allora $f_\lambda(P) = 0$ per ogni $f_\lambda \in I_\lambda, \lambda \in \Lambda$, quindi $P \in V(I_\lambda)$ per ogni $\lambda \in \Lambda$, cioè $P \in \bigcap_{\lambda\in\Lambda} V(I_\lambda)$.

   $\supseteq$ Se $P \in \bigcap_{\lambda\in\Lambda} V(I_\lambda)$ allora per ogni $\sum_{i=1}^n f_{\lambda_i} \in \sum_{\lambda\in\Lambda} I_\lambda$ con $f_{\lambda_i} \in I_{\lambda_i}$ si ha $\left(\sum_{i=1}^n f_{\lambda_i}\right)(P) = \sum_{i=1}^n f_{\lambda_i}(P) = 0$, da cui $P \in V\left(\sum_{\lambda\in\Lambda} I_\lambda\right)$.
6. Sia $P \in V(IJ)$. Se per ogni $f \in I$ si ha $f(P) = 0$ allora $P \in V(I)$, altrimenti esiste $f \in I$ tale che $f(P) \neq 0$, quindi per ogni $g \in J$ si ha $fg \in IJ$ quindi $0 = (fg)(P) = f(P)g(P)$ da cui $g(P) = 0$, pertanto $P \in V(J)$. In ogni caso $P \in V(I)\cup V(J)$. Pertanto $V(IJ) \subseteq V(I)\cup V(J)$.
   Adesso abbiamo $I\cap J \subseteq I \Rightarrow V(I\cap J) \supseteq V(I)$, analogamente $V(I\cap J) \supseteq V(J)$ da cui $V(I\cap J) \supseteq V(I)\cup V(J)$. Inoltre $IJ \subseteq I\cap J$ da cui $V(IJ) \supseteq V(I\cap J)$, ottenendo infine
   $$V(IJ) \supseteq V(I\cap J) \supseteq V(I)\cup V(J) \supseteq V(IJ).$$

(nel punto 4, $\mathscr{I}(\mathbb{A}^n(k)) = (0)$ vale solo nel caso k infinito). □

Proposizione 6.0.4. *Per ogni $X \subseteq \mathbb{A}^n(k)$ e per ogni ideale $I \trianglelefteq k[x_1,\dots,x_n]$ si ha*

1. $\mathscr{I}(X) = \sqrt{\mathscr{I}(X)}$
2. $V(I) = V(\sqrt{I})$

Dimostrazione.

1. Sia $f \in \sqrt{\mathscr{I}(X)}$ allora $f^n \in \mathscr{I}(X)$, cioè $f^n(P) = 0 \Rightarrow f(P) = 0$ per ogni $P \in X$, quindi $f \in \mathscr{I}(X)$. L'inclusione inversa vale sempre.

2. $I \subseteq \sqrt{I} \Rightarrow V(I) \supseteq V(\sqrt{I})$. Viceversa sia $P \in V(I)$, allora per ogni $f \in \sqrt{I}$ abbiamo $f^n \in I$ per qualche $n \in \mathbb{N}$, da cui $f^n(P) = 0 \Rightarrow f(P) = 0$, cioè $P \in V(\sqrt{I})$.

□

Proposizione 6.0.5. *Se $V_1, V_2 \subseteq \mathbb{A}^n(k)$ sono due varietà algebriche allora*

$$V_1 \subsetneq V_2 \Longleftrightarrow \mathscr{I}(V_1) \supsetneq \mathscr{I}(V_2).$$

Dimostrazione. Basta osservare che essendo V_1 e V_2 due varietà algebriche esistono due ideale I, J di $k[x_1, \dots, x_n]$ tali che $V_1 = V(I)$, $V_2 = V(J)$, pertanto

$$V(\mathscr{I}(V_1)) = V(\mathscr{I}(V(I))) = V(I) = V_1$$

$$V(\mathscr{I}(V_2)) = V(\mathscr{I}(V(J))) = V(J) = V_2.$$

Adesso basta applicare le proprietà della Proposizione 6.0.3. □

Corollario 6.0.6. *Ogni catena discendente di varietà algebriche*

$$V_1 \supseteq V_2 \supseteq V_3 \supseteq \dots$$

è stazionaria.

Dimostrazione. Dalla proposizione precedente abbiamo che a ogni catena discendente di varietà algebriche

$$V_1 \supseteq V_2 \supseteq V_3 \supseteq \dots$$

corrisponde una catena ascendente di ideali di $k[x_1, \dots, x_n]$

$$\mathscr{I}(V_1) \subseteq \mathscr{I}(V_2) \subseteq \mathscr{I}(V_3) \subseteq \dots$$

che deve essere stazionaria poiché $k[x_1, \dots, x_n]$ è noetheriano. Pertanto, riapplicando l'operatore V otteniamo che anche la catena discendente di varietà algebriche deve essere stazionaria. □

Definizione 6.0.7. *Sia $\mathcal{V} \subseteq \mathbb{A}^n(k)$ una varietà algebrica non vuota. Si definisce la* ***dimensione*** *di $\mathcal{V}$ come la massima lunghezza di catene di sottovarietà irriducibili*

$$\{P\} \subset \dots \subset V_{d-1} \subset V_d = \mathcal{V}.$$

L'insieme vuoto ha dimensione -1.

6.1 Topologia di Zariski

In base alle proprietà della Proposizione 6.0.3 abbiamo che le varietà algebriche affini godono delle stesse proprietà della famiglia di insiemi chiusi di una topologia.

Definizione 6.1.1. *La topologia su $\mathbb{A}^n(k)$ in cui i chiusi sono le varietà algebriche affini si chiama* ***topologia di Zariski***.

Definizione 6.1.2. *Uno spazio topologico X è* ***irriducibile*** *se dati due chiusi F, G tali che $X = F \cup G$ si ha $X = F$ oppure $X = G$.*
Un sottoinsieme $Y \subseteq X$ è ***irriducibile*** *se lo è rispetto alla topologia indotta.*

Proposizione 6.1.3. *Per uno spazio topologico le seguenti proprietà sono equivalenti*

1. *X è irriducibile.*
2. *Se U, V sono due aperti non vuoti di X allora $U \cap V \neq \emptyset$.*
3. *Ogni aperto di X è denso.*

Dimostrazione. (1) $\Leftrightarrow$ (2) segue dalla definizione prendendo i complementari.
(2) $\Leftrightarrow$ (3) segue dal fatto che un insieme è denso se e solo se interseca ogni aperto non vuoto. $\square$

Proposizione 6.1.4. *Una varietà algebrica $\mathcal{V} \subseteq \mathbb{A}^n(k)$ è irriducibile (rispetto alla topologia di Zariski) se e solo se $\mathscr{I}(\mathcal{V})$ è un ideale primo.*

Dimostrazione.

- $\Rightarrow$ Se $fg \in \mathscr{I}(\mathcal{V})$ allora $(f)(g) \subseteq \mathscr{I}(\mathcal{V})$ da cui

$$V(f) \cup V(g) = V((f)(g)) \supseteq V(\mathscr{I}(\mathcal{V})) = \mathcal{V}.$$

  Poiché $\mathcal{V}$ è irriducibile abbiamo che $\mathcal{V} \subseteq V(f)$ oppure $\mathcal{V} \subseteq V(g)$, cioè $(f) \subseteq \mathscr{I}(V(f)) \subseteq \mathscr{I}(\mathcal{V})$ oppure $(g) \subseteq \mathscr{I}(V(g)) \subseteq \mathscr{I}(\mathcal{V})$, in altri termini $f \in \mathscr{I}(\mathcal{V})$ oppure $g \in \mathscr{I}(\mathcal{V})$.

- $\Leftarrow$ Se $\mathcal{V} = V_1 \cup V_2$, con V_1, V_2 due varietà algebriche, allora $\mathscr{I}(\mathcal{V}) = \mathscr{I}(V_1) \cap \mathscr{I}(V_2)$ da cui per la Proposizione 1.1.23 deve verficarsi uno dei due casi

$$\mathscr{I}(\mathcal{V}) = \mathscr{I}(V_1) \Rightarrow V(\mathscr{I}(\mathcal{V})) = V(\mathscr{I}(V_1)) \Rightarrow \mathcal{V} = V_1$$
$$\mathscr{I}(\mathcal{V}) = \mathscr{I}(V_2) \Rightarrow V(\mathscr{I}(\mathcal{V})) = V(\mathscr{I}(V_2)) \Rightarrow \mathcal{V} = V_2.$$

$\square$

Definizione 6.1.5. *Si definisce* ***dimesione di Krull*** $\dim X$ *di uno spazio topologico X non vuoto l'estremo superiore delle lunghezze n di tutte le catene*

$$X_0 \subset X_1 \subset \ldots \subset X_n$$

di sottoinsiemi X_i di X chiusi irriducibili e non vuoti.
Lo spazio topologico vuoto ha dimensione pari a -1.

La dimensione di una varietà algebrica $\mathcal{V}$ corrisponde alla dimensione di Krull di $\mathcal{V}$ rispetto alla topologia indotta dalla topologia di Zariski.

6.2 Spettro di un anello

Sia A un anello e sia

$$\mathrm{Spec}(A) = \{P \trianglelefteq A : P \text{ è primo}\}.$$

Per ogni $E \subseteq A$ poniamo

$$V(E) = \{P \in \mathrm{Spec}(A) : E \subseteq P\}.$$

Proposizione 6.2.1.

1. $E \subseteq F \Rightarrow V(E) \supseteq V(F)$ *per ogni* $E, F \subseteq A$.
2. $V(E) = V(I) = V(\sqrt{I})$ *dove* I *è l'ideale genearato da* $E \subseteq A$.
3. $V(0) = \mathrm{Spec}(A)$, $V(1) = \emptyset$.
4. $V\left(\bigcup_{\lambda\in\Lambda} E_\lambda\right) = \bigcap_{\lambda\in\Lambda} V(E_\lambda)$ *per ogni famiglia* $\{E_\lambda\}_{\lambda\in\Lambda} \subseteq \mathcal{P}(A)$.
5. $V(IJ) = V(I \cap J) = V(I) \cup V(J)$ *per ogni* I, J *ideali di* A.

Dimostrazione.

1. Se $P \in V(F)$ allora $P \supseteq F \supseteq E$ da cui $P \in V(E)$.
2. Se $P \in V(E)$ allora $I \subseteq P$ in quanto I è il più piccolo ideale che contiene l'insieme E. Pertanto $V(E) = V(I)$. Dal Corollario 1.1.18 abbiamo che per ogni $Q \in V(I)$

$$Q \supseteq \bigcap_{P\in V(I)} P = \sqrt{I}$$

   da cui $V(I) = V(\sqrt{I})$.
3. Banale
4. $P \in V\left(\bigcup_{\lambda\in\Lambda} E_\lambda\right) \Leftrightarrow P \supseteq \bigcup_{\lambda\in\Lambda} E_\lambda \Leftrightarrow P \supseteq E_\lambda$ per ogni $\lambda \in \Lambda \Leftrightarrow P \in \bigcap_{\lambda\in\Lambda} V(E_\lambda)$.
5. $IJ \subseteq I \cap J \Rightarrow V(IJ) \supseteq V(I \cap J)$. Adesso se $P \in V(IJ)$ allora $IJ \subseteq P$, dal Lemma 1.1.7 abbiamo che $I \subseteq P$ oppure $J \subseteq P$, quindi $P \in V(I) \cup V(J)$. Se $P \in V(I) \cup V(J)$ allora $I \subseteq P$ oppure $J \subseteq P$, in ogni caso $I \cap J \subseteq P$, pertanto $P \in V(I \cap J)$. Abbiamo provato che

$$V(I \cap J) \subseteq V(IJ) \subseteq V(I) \cup V(J) \subseteq V(I \cap J).$$

□

La proposizione precedente mostra che gli insiemi del tipo $V(E)$ godono delle stesse proprietà della famiglia di insiemi chiusi di una topologia.

Definizione 6.2.2. *La topologia su* $\mathrm{Spec}(A)$ *dove i chiusi sono gli insiemi del tipo* $V(E)$ *con* $E \subseteq A$ *si chiama* ***Topologia di Zariski*** *di* A.

Definizione 6.2.3 (Dimensione di Krull). *Si definisce* ***dimensione di Krull*** $\dim A$ *di un anello* A *l'estremo superiore delle lunghezze di catene di ideali primi*

$$P_0 \subset P_1 \subset \ldots \subset P_n.$$

Essa coincide con la dimensione di Krull di $\mathrm{Spec}(A)$ *rispetto alla topologia di Zariski. L'**altezza** di un ideale primo* $P \in \mathrm{Spec}(A)$ *è l'estremo superiore delle lunghezze di catene del tipo precedente dove* $P_n = P$*, o equivalentemente la dimensione di* A_P*. Per un ideale* I *qualsiasi l'**altezza*** $\mathrm{ht}(I)$ *di* I *è l'estremo inferiore delle altezze degli ideali primi che lo contengono. Inoltre poniamo* $dim I = \dim(R/I)$ *detta la* ***dimensione*** *(o* ***coaltezza****) dell'ideale* I*.*

Così dalla Proposizione 6.0.5 e dalla Proposizione 6.1.4 segue che per una varietà algebrica $\mathcal{V} \subseteq \mathbb{A}^n(k)$, ponendo

$$k[\mathcal{V}] = \frac{k[x_1, \ldots, x_n]}{\mathscr{I}(\mathcal{V})}$$

si ha che la dimensione della varietà algebrica $\mathcal{V}$ coincide con $\dim k[\mathcal{V}]$.

Un'altra definizione di dimensione di una varietà algebrica $\mathcal{V}$ può essere data attraverso il grado di trascendenza dell'estensione $k \subseteq k[\mathcal{V}]$.

6.3 Teorema degli zeri di Hilbert

Proposizione 6.3.1 (Artin-Tate). *Siano* $A \subseteq B \subseteq C$ *tre anelli. Supponiamo che* A *sia noetheriano,* C *sia una* A*-algebra finitamente generata e anche un* B*-modulo di tipo finito. Allora* B *è una* A*-algebra finitamente generata (quindi* B *è anche noetheriano).*

Dimostrazione. Siano $x_1, \ldots, x_m, y_1, \ldots, y_n \in C$ tali che

$$C = A[x_1, \ldots, x_m]$$
$$C = By_1 + \ldots + By_n.$$

Risulta

$$x_i = \sum_{j=1}^{n} b_{ij} y_i, \quad y_i y_j = \sum_{k=1}^{n} b_{ijk} y_k,$$

per certi $b_{ij}, b_{ijk} \in B$. Sia

$$B_0 = A\left[b_{ij}, b_{jkt} : \begin{array}{r} i \in \{1, \ldots, m\} \\ j, k, t \in \{1, \ldots, n\} \end{array} \right].$$

B_0 è una A-algebra finitamente generata, quindi è anche noetheriano. Inoltre utilizzando le relazioni scritte sopra abbiamo che C è un B_0-modulo di tipo finito pertanto è un B_0-modulo noetheriano, quindi B è un B_0-modulo di tipo finito (in quanto sotto-B_0-modulo di C). Dunque, poiché B_0 è una A-algebra finitamente generata allora anche B è un A-algebra finitamente generata. $\square$

Definizione 6.3.2. *Sia $\mathbb{F} \subseteq \mathbb{K}$ una estensione di campi. Gli elementi $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ si dicono **algebricamente indipendenti** su $\mathbb{F}$ se per ogni polinomio $f \in \mathbb{F}[x_1, \ldots, x_n]$ non nullo si ha $f(\alpha_1, \ldots, \alpha_n) \neq 0$.*

L'indipendenza algebrica è una generalizzazione della trascendenza, infatti dire che $x \in \mathbb{K}$ è algebricamente indipendente su $\mathbb{F}$ equivale a dire che x è trascendente su $\mathbb{F}$.

Teorema 6.3.3. *Sia $k \subseteq E$ un'estensione di campi. Se E è un k-algebra finitamente generata allora l'estensione $k \subseteq E$ è finita.*

Prima dimostrazione. Poniamo $E = k[x_1, \ldots, x_n]$. Se per assurdo E non è algebrico su k allora supponiamo che $x_1, \ldots, x_r$ siano algebricamente indipendenti su k e che $x_{r+1}, \ldots, x_n$ siano algebrici su $F = k(x_1, \ldots, x_r)$ (osserviamo che F è isomorfo al campo dei quozienti dell'anello dei polinomi in r variabili a coefficienti in k, dal momento che $x_1, \ldots, x_r$ sono algebricamente indipendenti su k). Quindi $F \subseteq E$ è un'estensione finita, in altri termini E è un F-modulo di tipo finito. Applichiamo adesso la proposizione precedente su $k \subseteq F \subseteq E$, così F risulta una k-algebra finitamente generata, cioè $F = k[y_1, \ldots, y_m]$ con $y_i = f_i/g_i$, dove $f_i, g_i \in k[x_1, \ldots, x_r]$. Sia adesso $h = g_1 g_2 \ldots g_m + 1 \in k[x_1, \ldots, x_r]$, h non ha nessun divisore in comune con ognuno degli g_i, risulta

$$\frac{1}{h} = \frac{p(x_1, \ldots, x_r)}{g_1^{t_1} g_2^{t_2} \ldots g_m^{t_m}} \Rightarrow p(x_1, \ldots, x_n) = \frac{g_1^{t_1} g_2^{t_2} \ldots g_m^{t_m}}{h} \in k[x_1, \ldots, x_r],$$

contro il fatto che h non ha nessun divisore in comune con gli g_i, assurdo. $\square$

Corollario 6.3.4. *Sia k un campo e A una k-algebra finitamente generata. Sia $\underline{m}$ un ideale massiamle di A, allora $A/\underline{m}$ è un'estensione finita di k. Inoltre se k è algebricamente chiuso allora $A/\underline{m} \simeq k$.*

Dimostrazione. $A/\underline{m}$ è una k-algebra finitamente generata, e ha come generatori le classi di resto dei generatori di A come k-algebra. Adesso basta applicare il teorema precedente con $E = A/\underline{m}$. Se k è algebricamente chiuso, l'estensione $k \subseteq E$ è finita quindi è anche algebrica da cui $k = E$. $\square$

Corollario 6.3.5 (Nullstellensatz debole)**.** *Sia k un campo algebricamente chiuso. Un ideale I di $k[x_1, \ldots, x_n]$ è proprio se e solo se*

$$V(I) = \{P \in \mathbb{A}^n(k) : f(P) = 0 \quad \forall f \in I\} \neq \emptyset.$$

Dimostrazione.

$\Rightarrow$ I è contenuto in un ideale massimale M di $A = k[x_1, \ldots, x_n]$. Dal corollario precedente sappiamo che $k[\overline{x_1}, \ldots, \overline{x_n}] = A/M \simeq k$ quindi esiste un isomorfismo di campi $\phi : k[\overline{x_1}, \ldots, \overline{x_n}] \to k$ tale che $\phi(\overline{x_i}) = \alpha_i \in k$. Adesso ad ogni $f \in M$ corrisponde in A/M la classe nulla

$$f(x_1, \ldots, x_n) + M = f(\overline{x_1}, \ldots, \overline{x_n}) = \overline{0},$$

quindi si ha anche

$$f(\alpha_1, \ldots, \alpha_n) = f(\phi(\overline{x_1}), \ldots, \phi(\overline{x_n})) = \phi(f(\overline{x_1}, \ldots, \overline{x_n})) = \phi(\overline{0}) = 0.$$

Dunque dall'arbitrarietà di $f \in M$ abbiamo $P = (\alpha_1, \ldots, \alpha_n) \in V(M) \subseteq V(I) \neq \emptyset$.

$\Leftarrow$ Basta osservare che $V(k[x_1,\ldots,x_n]) = \emptyset$, infatti $\forall P \in \mathbb{A}^n(k)$ si ha $1(P) = 1 \neq 0$.

$\square$

Osserviamo che il Nullstellensatz debole è equivalente al teorema precedente, infatti se $k \subseteq k[\alpha_1,\ldots,\alpha_n] = E$ è un'estensione di campi allora consideriamo l'omomorfismo $\phi : k[x_1,\ldots,x_n] \to E$ con $\phi(x_i) = \alpha_i$. L'ideale $\ker\phi = M$ è massimale poiché E è un campo, per ipotesi esiste $P = (\beta_1,\ldots,\beta_n) \in \mathbb{A}^n(\overline{k})$ tale che $f(P) = 0$ per ogni $f \in M$. Pertanto sia $\varphi : k[x_1,\ldots,x_n] \to k[\beta_1,\ldots,\beta_n]$ con $\varphi(x_i) = \beta_i$, si ha $M \subseteq \ker\varphi$, dalla massimalità di M abbiamo $\ker\varphi = M$, quindi

$$E \simeq \frac{k[x_1,\ldots,x_n]}{M} \simeq k[\beta_1,\ldots,\beta_n].$$

Dunque dato che $\beta_i \in \overline{k}$ allora E è algebrico su k, cioè $k \subseteq E$ è finita.

L'ipotesi che k sia algebricamente chiuso è necessaria, infatti se $k = \mathbb{R}$ abbiamo che

$$V(x^2+1) = \emptyset.$$

Corollario 6.3.6. *Se k è un campo algebricamente chiuso allora ogni ideale massimale di $k[x_1,\ldots,x_n]$ è della forma $(x_1-\alpha_1,\ldots,x_n-\alpha_n)$ con $\alpha_1,\ldots,\alpha_n \in k$.*

Dimostrazione. Sia M massimale in $k[x_1,\ldots,x_n]$. Sappiamo che esiste $P = (\alpha_1,\ldots,\alpha_n) \in V(M)$. Adesso se $f(P) = 0$ allora $f \in M$, altrimenti $(f) + M = k[x_1,\ldots,x_n]$, quindi $1 = \lambda f + m \Rightarrow 1(P) = \lambda(P)f(P) + m(P) = 0$, assurdo. Pertanto $f \in M$. Dunque $x_i - \alpha_i \in M$, cioè l'ideale massimale $(x_1-\alpha_1,\ldots,x_n-\alpha_n)$ è contenuto in M, da cui abbiamo l'uguaglianza. $\square$

Teorema 6.3.7 (Nullstellensatz)**.** *Sia k un campo algebricamente chiuso e sia I un ideale di $k[x_1,\ldots,x_n]$. Allora*

$$\mathscr{I}(V(I)) = \sqrt{I}.$$

Dimostrazione.

$\subseteq$ Osserviamo prima di tutto che $k[x_1,\ldots,x_n]$ è noetheriano, quindi l'ideale I è finitamente generato $I = (f_1,\ldots,f_n)$.
Sia $f \in \mathscr{I}(V(I))$ e sia $J = I + (fT-1) \trianglelefteq k[x_1,\ldots,x_n,T]$. Per assurdo sia $\overline{P} = (a_1,\ldots,a_n,b) \in V(J) \subseteq \mathbb{A}^{n+1}(k)$ abbiamo che $P = (a_1,\ldots,a_n) \in V(I)$ infatti per ogni $g \in I$ si ha $g + 0 \in I + (fT-1) = J$, quindi $g(\overline{P}) = g(P) = 0$. D'altra parte abbiamo

$$(fT-1)(\overline{P}) = f(P)b - 1 = -1 \neq 0,$$

assurdo, quindi $V(J) = \emptyset \Rightarrow J = k[x_1,\ldots,x_n,T]$. Pertanto $1 \in J = I + (fT-1)$, da cui si ha

$$1 = \sum_{i=1}^{n} \lambda_i f_i + \lambda(fT-1)$$

dove gli f_i sono i generatori di I e $\lambda, \lambda_i \in k[x_1, \ldots, x_n, T]$. Consideriamo adesso l'omomorfismo $\phi : k[x_1, \ldots, x_n, T] \to k(x_1, \ldots, x_n)$ con $\phi(x_i) = x_i$, $\phi(T) = 1/f$. Risulta

$$1 = \phi(1) = \phi\left(\sum_{i=1}^{n} \lambda_i f_i + \lambda(fT - 1)\right) = \sum_{i=1}^{n} \phi(\lambda_i) f_i = \sum_{i=1}^{n} \frac{\tilde{\lambda}_i}{f^{m_i}} f_i.$$

Ponendo $m = \max\{m_i : i = 1, \ldots, n\}$ si ha

$$f^m = \sum_{i=1}^{n} f^{m-m_i} \tilde{\lambda}_i f_i \in I \Rightarrow f \in \sqrt{I}.$$

$\supseteq$ Se $f \in \sqrt{I}$ allora $f^n \in I$ quindi per ogni $P \in V(I)$ si ha $f^n(P) = 0 \Leftrightarrow f(P) = 0$, cioè $f \in \mathscr{I}(V(I))$ (oppure $\sqrt{I} \subseteq \mathscr{I}(V(\sqrt{I})) = \mathscr{I}(V(I))$).

□

Abbiamo dimostrato il Nullstellensatz (forte) a partire dal Nullstellensatz debole, vediamo che le due forme sono in realtà equivalenti:

$$\text{Nullstellensatz} \Longrightarrow \text{Nullstellensatz debole.}$$

Infatti se I è un ideale di $k[x_1, \ldots, x_n]$ con $V(I) = \emptyset$, risulta

$$\sqrt{I} = \mathscr{I}(V(I)) = \mathscr{I}(\emptyset) = k[x_1, \ldots, x_n] \Rightarrow I = k[x_1, \ldots, x_n].$$

Proposizione 6.3.8. *Ogni varietà algebrica può essere scritta come unione di varietà algebriche irriducibili.*

Dimostrazione. Sia $V(I)$ una varietà algebrica. Essendo $k[x_1, \ldots, x_n]$ noetheriano, dal Corollario 4.2.4 abbiamo che I ha una decomposizione primaria

$$I = Q_1 \cap \ldots \cap Q_n$$

da cui

$$\begin{aligned} V(I) = V(\sqrt{I}) = V(\sqrt{Q_1 \cap \ldots \cap Q_n}) = \\ = V(\sqrt{Q_1} \cap \cdots \cap \sqrt{Q_n}) = V(\sqrt{Q_1}) \cup \ldots \cup V(\sqrt{Q_n}), \end{aligned}$$

dove le varietà $V(\sqrt{Q_i})$ sono irriducibili dal momento che $\mathscr{I}(V(\sqrt{Q_i})) = \sqrt{\sqrt{Q_i}} = \sqrt{Q_i}$ è un ideale primo. □

Capitolo 7

Normalizzazione di Noether

Teorema 7.0.1 (Principio di identità dei polinomi)**.** *Sia k un campo infinito.*
Se $f \in k[x_1, \ldots, x_n]$ è tale che $f(P) = 0$ per ogni $P \in k^n$ allora f è il polinomio nullo.

Dimostrazione. Procediamo per induzione su n. Se $n = 1$ dal teorema di Ruffini segue che f può avere al più un numero di radici pari al suo grado, ma dato che k è infinito f deve essere necessariamente il polinomio nullo.
Supponiamo il teorema vero per $n - 1$, dimostriamolo per n. Fissiamo $\alpha_1, \ldots, \alpha_{n-1} \in k$, per ipotesi il polinomio $f(\alpha_1, \ldots, \alpha_{n-1}, x_n) \in k[x_n]$ ha infinite radici, quindi per l'ipotesi induttiva esso è il polinomio nullo, cioè i suoi coefficienti devono essere tutti nulli. Ma i coefficienti di $f(\alpha_1, \ldots, \alpha_{n-1}, x_n)$ sono polinomi calcolati in $\alpha_1, \ldots, \alpha_{n-1}$, dall'arbitrarietà di questi ultimi e dall'ipotesi induttiva segue che essi sono polinomi nulli, pertanto abbiamo che f è il polinomio nullo. □

Teorema 7.0.2 (Normalizzazione di Noether)**.** *Sia k un campo e $A = k[x_1, \ldots, x_n]$ una k-algebra finitamente generata.*

1. *Esistono $r \leq n$ e $y_1, \ldots, y_r \in A$ algebricamente indipendenti su k tali che l'estensione $k[y_1, \ldots, y_r] \subseteq A$ è intera.*

2. *Se I è un ideale proprio di A allora $I \cap k[y_1, \ldots, y_r] = (y_\delta, y_{\delta+1}, \ldots, y_r)$, per qualche $\delta \leq r$.*

Proviamo solamente il primo punto nel caso k infinito.

Dimostrazione. Procediamo per induzione su n. Se $n = 1$ allora $A = k[x]$. Se x è algebrico su k allora è anche intero su k, quindi $r = 0$ e $k \subseteq A$ è intera. Se x è trascendente su k allora $r = 1$ e $k[x] = A$ è banalmente intera. Supponiamo il teorema vero per $n - 1$ e dimostriamolo per n. Se $x_1, \ldots, x_n$ sono algebricamente indipendenti su k allora $r = n$ e $k[x_1, \ldots, x_n] = A$ è banalmente intera. Altrimenti supponiamo esista $f \in k[X_1, \ldots, X_n]$ tale che $f(x_1, \ldots, x_n) = 0$. Scriviamo f come somma di polinomi omogenei f_i di grado $i = 0, 1, \ldots, d$

$$f = f_0 + f_1 + \ldots + f_d,$$

con $f_d \neq \underline{0}$. Dunque per il principio di identità dei polinomi esistono $b_1, b_2, \ldots, b_{n-1}, b_n \in k$ non tutti nulli (a meno di riordinamento degli indici possiamo supporre $b_n \neq 0$) tali che $f_d(b_1, b_2, \ldots, b_{n-1}, b_n) \neq 0$, allora ponendo $c_i = b_i / b_n$ per $i \leq n - 1$, abbiamo

$$f_d(b_1, b_2, \ldots, b_{n-1}, b_n) = b_n^d f_d(c_1, \ldots, c_{n-1}, 1) \neq 0 \Rightarrow f_d(c_1, \ldots, c_{n-1}, 1) \neq 0.$$

Poniamo $y_i = x_i - c_i x_n$ per ogni $i \leq n-1$. Risulta

$$0 = f(x_1, \ldots, x_n) = f(y_1 + c_1 x_n, \ldots, y_{n-1} + c_{n-1} x_n, x_n) = g_0 + g_1 x_n + \ldots + g_d x_n^d \quad (7.1)$$

e dev'essere

$$g_d(y_1, \ldots, y_{n-1}) x_n^d = f_d(c_1 x_n, \ldots, c_{n-1} x_n, x_n) = x_n^d f_d(c_1, \ldots, c_{n-1}, 1)$$

da cui moltiplicando la 7.1 per $f_d(c_1, \ldots, c_{n-1}, 1)^{-1}$ otteniamo una relazione di dipendenza integrale di x_n su $k[y_1, \ldots, y_{n-1}]$. Dall'ipotesi induttiva, esistono $r \leq n-1$ e $t_1, \ldots, t_r \in k[y_1, \ldots, y_{n-1}]$ algebricamente indipendenti su k, tali che $k[t_1, \ldots, t_r] \subseteq k[y_1, \ldots, y_{n-1}]$ sia intera. Da cui l'estensione $k[t_1, \ldots, t_r] \subseteq A$ è intera. □

Corollario 7.0.3. *L'anello dei polinomi $k[x_1, \ldots, x_n]$ ha dimensione n.*

Dimostrazione. Procediamo per induzione su n. Per $n = 0$ sappiamo che $\dim k = 0$. Supponiamo il teorema vero fino a $n-1$ e proviamolo per n. Osserviamo che la catena $(0) \subset (x_1) \subset (x_1, x_2) \subset \ldots \subset (x_1, \ldots, x_n)$ ci permette di dire che $\dim k[x_1, \ldots, x_n] \geq n$. Sia adesso

$$(0) \subset P_1 \subset P_2 \subset \ldots \subset P_m$$

una qualunque catena di primi e proviamo che $m \leq n$. Per il lemma di normalizzaizone di Noether abbiamo che esistono $y_1, \ldots, y_n$ algebricamente indipendenti su k tali che $k[y_1, \ldots, y_n] \subseteq k[x_1, \ldots, x_n]$ è intera e inoltre $P_1 \cap k[y_1, \ldots, y_n] = (y_\delta, y_{\delta+1}, \ldots, y_n)$ per qualche $\delta \leq n$, da cui anche l'estensione

$$k[y_1, \ldots, y_{\delta-1}] = \frac{k[y_1, \ldots, y_n]}{(y_\delta, y_{\delta+1}, \ldots, y_n)} \subseteq \frac{k[x_1, \ldots, x_n]}{P_1}$$

è intera. Dall'ipotesi induttiva $\dim k[y_1, \ldots, y_{\delta-1}] = \dim k[x_1, \ldots, x_n]/P_1 = \delta - 1$, quindi la catena di primi

$$(\overline{0}) \subset P_2/P_1 \subset P_3/P_1 \subset \ldots \subset P_m/P_1$$

in $k[x_1, \ldots, x_n]/P_1$ può avere lunghezza al più $\delta - 1$, cioè $m \leq \delta \leq n$. □

Corollario 7.0.4. *Se $A = k[x_1, \ldots, x_n]$ è un dominio allora* $\dim A = \operatorname{tr}\deg_k(Q(A))$.

Dimostrazione. Infatti per il lemma di normalizzazione di Noether esistono $y_1, \ldots, y_d \in A$ algebricamente indipendenti su k tali che $k[y_1, \ldots, y_n] \subseteq A$ è intera. Da cui passando al campo dei quozienti abbiamo

$$k \subseteq k(y_1, \ldots, y_d) \subseteq Q(A)$$

dove la prima estensione è puramente trascendente di grado d e la seconda è un'estensione algebrica. □

Capitolo 8

Teorema dell'ideale principale

Lemma 8.0.1. *Sia A un dominio e $y, u \in A\setminus\{0\}$, allora abbiamo il seguente isomorfismo di A-moduli*

$$\frac{(u,y)}{(u)} \simeq \frac{(u^2,uy)}{(u^2)}.$$

Inoltre se $(y : u^2) = (y : u)$ allora si ha anche

$$\frac{(u)}{(u^2)} \simeq \frac{(u^2,y)}{(u^2,uy)}.$$

Dimostrazione. Sia $\varphi : (u,y) \to (u^2,uy)/(u^2)$ con $\varphi(x) = ux + (u^2)$. φ è un omomorfismo suriettivo, inoltre $\ker\varphi = (u)$.
Per la seconda realazione, osserviamo che $A/(u) \simeq (u)/(u^2)$ tramite l'isomorfismo che manda $x + (u)$ in $ux + (u^2)$. Adesso sia $\varphi : A \to (u^2,y)/(u^2,uy)$ con $\varphi(x) = yx + (u^2,uy)$. φ è un omomorfismo suriettivo. Inoltre $\varphi(u) = uy + (u^2,uy) = \overline{0}$, pertanto $(u) \subseteq \ker\varphi$. Viceversa sia $x \in \ker\varphi$, allora

$$\begin{gathered}
yx = \alpha u^2 + \beta uy \in (u^2,uy)\\
\alpha u^2 = y(x-\beta u) \Rightarrow \alpha \in (y : u^2) = (y : u)\\
\Rightarrow \alpha u = \gamma y \Rightarrow \alpha u^2 = \gamma uy\\
yx = y(\gamma+\beta)u \Rightarrow x = (\gamma+\beta)u \in (u).
\end{gathered}$$

Dunque $\ker\varphi = (u)$, quindi $(u)/(u^2) \simeq A/(u) \simeq (u^2,y)/(u^2,uy)$. □

Corollario 8.0.2. *Sotto le stesse ipotesi del lemma precedente, se $A/(u^2)$ è artiniano allora $(u,y) = (u^2,y)$.*

Dimostrazione. Infatti se $A/(u^2)$ è artiniano è anche noetheriano, pertanto ogni suo sottomodulo ha lunghezza finita. Ne segue che

$$\begin{aligned}
\lambda\left(\frac{(u,y)}{(u^2)}\right) &= \lambda\left(\frac{(u,y)}{(u)}\right) + \lambda\left(\frac{(u)}{(u^2)}\right) =\\
&= \lambda\left(\frac{(u^2,uy)}{(u^2)}\right) + \lambda\left(\frac{(u^2,y)}{(u^2,uy)}\right) = \lambda\left(\frac{(u^2,y)}{(u^2)}\right),
\end{aligned}$$

da cui $(u,y)/(u^2) = (u^2,y)/(u^2)$, cioè $(u,y) = (u^2,y)$. □

Teorema 8.0.3 (Teorema dell'ideale principale di Krull).
Sia A un anello noetheriano, $x \in A$ non invertibile e P un ideale primo minimale di (x), allora $\mathrm{ht}(P) \leq 1$.

Dimostrazione. Supponiamo per assurdo che esistano due primi P_1, P_2 tali che $P_2 \subset P_1 \subset P$. Per ipotesi $x \notin P_1$, altrimenti P non sarebbe un primo minimale di (x). Quozientiamo con P_2 e localizziamo in P/P_2. Con abuso di notazione continuiamo a indicare con P l'ideale $S^{-1}(P/P_2)$, con x l'elemento $(x + P)/1$, con P_1 l'ideale $S^{-1}(P_1/P)$ e così via (dove $S = (A/P_2) \setminus (P/P_2)$). In questo modo l'anello che otteniamo è locale con ideale massimale P e si ha $(x) \subset P$, $(0) \subset P_1 \subset P$ (ricordiamo che gli ideali primi di $S^{-1}(A/P_2)$ sono in corrispondenza biunivoca con gli ideali primi Q di A tali che $P_2 \subseteq Q \subseteq P$). Sia $y \in P_1 \setminus \{0\}$, abbiamo la seguente catena di moduli

$$(y : x) \subseteq (y : x^2) \subseteq (y : x^3) \subseteq \dots$$

dato che A è noetheriano esiste $n \in \mathbb{N}$ tale che $(y : x^n) = (y : x^{n+1})$. Poniamo $u = x^n$, allora $(y : u) = (y : u^2)$. Inoltre P è l'unico ideale primo che contiene x, quindi l'unico che contiene u^2, pertanto $A/(u^2)$ ha un solo ideale primo, dunque è artiniano. Dal lemma precedente segue che $(u, y) = (u^2, y)$. In particolare

$$\begin{gathered} u = \alpha u^2 + \beta y \\ u(1 - \alpha u) = \beta y \\ u = (1 - \alpha u)^{-1} \beta y \in (y) \subseteq P_1 \end{gathered}$$

(infatti $u \in P$ quindi $1 - \alpha u$ è invertibile), ne segue $x \in P_1$, assurdo. □

Teorema 8.0.4 (Teorema dell'ideale principale generalizzato).
Sia A un anello noetheriano. Se I è un ideale di A con n generatori $I = (a_1, a_2, \dots, a_n)$, allora per ogni ideale primo P minimale di I si ha $\mathrm{ht}(P) \leq n$.

Dimostrazione. Procediamo per induzione su n. Per $n = 1$ il teorema segue dal teorema dell'ideale principale. Supponiamo il teorema vero fino a $n-1$ e dimostriamolo per n. Per assurdo supponiamo che esista un ideale primo $P_1 \subset P$ tale che $\mathrm{ht}(P_1) \geq n$. Supponiamo inoltre che non esistano ideali primi compresi tra P_1 e P. Localizziamo in P. Per ipotesi risulta $P_1 \subsetneq I$, quindi, a meno di riordinamento degli indici, supponiamo che $a_1 \notin P_1$ e consideriamo l'ideale $(P_1, a_1) \subseteq P$. P è l'unico ideale primo che contiene (P_1, a_1), pertanto $P = \sqrt{(P_1, a_1)}$. Dato che A è noetheriano allora per 4.0.14 si ha $P^k \subseteq (P_1, a_1)$ per qualche $k \in \mathbb{N}$, da cui $a_i^k = b_i + c_i a_1$ per ogni $i \geq 2$, con $b_i \in P_1$, $c_i \in A$. Sia $J = (b_2, \dots, b_n)$, dall'ipotesi induttiva abbiamo che $\mathrm{ht}(J) \leq n - 2$, quindi deve esistere un primo minimale Q di J tale che $J \subset Q \subset P_1$. Per ogni $i \geq 2$ si ha $a_i^k \in (Q, a_1)$, quindi ogni ideale primo che contiene (Q, a_1) contiene I, da cui P è l'unico ideale primo che contiene (Q, a_1). Adesso quozientiamo rispetto a Q, otteniamo che P/Q è un primo minimale di $(Q, a_1)/Q = (\overline{a_1})$, ma $(\overline{0}) \subset P_1/Q \subset P/Q$, così $\mathrm{ht}(P/Q) \geq 2$, contro il teorema dell'ideale principale, assurdo. □

Dato che in un anello noetheriano ogni ideale ha un numero finito di generatori segue

Corollario 8.0.5. *In un anello noetheriano A ogni ideale ha altezza finita. Se A è semilocale allora* $\dim A$ *è finita. Se $(A, \underline{m})$ è locale e* $\dim A = d$ *allora $\underline{m}$ ha almeno d generatori.*

Corollario 8.0.6. *Se A è un anello noetheriano e $I = (a_1, \ldots, a_n)$ è un suo ideale tale che* $\mathrm{ht}(I) = n$ *allora ogni suo primo minimale ha altezza n.*

Dimostrazione. Dal teorema precedente ogni primo P minimale di I ha altezza al più n, da cui $n = \mathrm{ht}(I) \leq \mathrm{ht}(P) \leq n$. □

Lemma 8.0.7. *Sia A un anello noetheriano. Se $P_1, \ldots, P_n$ sono i primi minimali di A e $x \in A \setminus (P_1 \cup \ldots \cup P_n)$ allora* $\mathrm{ht}(x) = 1$.

Dimostrazione. Dal teorema dell'ideale principale abbiamo $\mathrm{ht}(x) \leq 1$. Inoltre se P è un primo che contiene (x) allora $P_i \subset P$ per qualche $i \leq n$, da cui $\mathrm{ht}(x) \geq 1$. □

Osserviamo che se P è un ideale primo contenente un ideale I, P è un primo minimale di I se e solo se $\mathrm{ht}_{A/I}(P/I) = 0$.

Proposizione 8.0.8. *Sia A un anello noetheriano e $I = (a_1, \ldots, a_n)$ un suo ideale. Se P è un dieale primo contente I tale che* $\mathrm{ht}_{A/I}(P/I) \leq k$ *allora* $\mathrm{ht}_A(P) \leq n + k$.

Dimostrazione. Procediamo per induzione su k. Per $k = 0$ la tesi segue dal teorema dell'ideale principale generalizzato. Supponiamo il teorema vero fino a $k-1$, dimostriamolo per $k > 0$. P non è un primo minimale di I, quindi detti $P_1, \ldots, P_t$ i primi minimali di I abbiamo $P \nsubseteq P_i$, da 1.1.23 segue che $P \nsubseteq P_1 \cup \ldots \cup P_t$. Sia $y \in P \setminus (P_1 \cup \ldots \cup P_t)$ e $J = (I, y)$, per la scelta di y applicando il lemma precedente all'ideale $J/I = (\overline{y})$ di A/I abbiamo che $\mathrm{ht}_{A/I}(J/I) = 1$. Osservando infine che gli idaeli primi di A/J sono in corrispondenza biunivoca con gli ideali primi di A/I che contengono J ne segue che

$$\mathrm{ht}_{A/J}(P/J) = \mathrm{ht}_{A/I}(P/I) - \mathrm{ht}_{A/I}(J/I) = \mathrm{ht}_{A/I}(P/I) - 1 \leq k - 1.$$

Dato che J ha $n+1$ generatori, dall'ipotesi induttiva $\mathrm{ht}_A(P) \leq k-1+(n+1) = n+k$. □

Corollario 8.0.9. *Sia A un anello noetheriano. Se P è un ideale primo di A tale che* $\mathrm{ht}(P) = l$ *e $x \in P$ allora*

1. $\mathrm{ht}(P/(x)) \in \{l, l-1\}$.
2. *Se $x \notin Q$, per ogni Q primo minimale di A, allora* $\mathrm{ht}(P/(x)) = l - 1$.

Dimostrazione.

1. Dalla proposizione precedente abbiamo che $l = \mathrm{ht}_A(P) \leq \mathrm{ht}_{A/(x)}(P) + 1$, cioè risulta $\mathrm{ht}_{A/(x)}(P/(x)) \geq l - 1$. Inoltre $\mathrm{ht}_{A/(x)}(P/(x)) \leq l$ poiché i primi di $A/(x)$ corrispondono ai primi di A contenenti (x).
2. Se $x \in P$ non appartiene a nessun ideale primo minimale di A allora $\mathrm{ht}_A(x) = 1$ (Lemma 8.0.7), da cui $\mathrm{ht}_{A/(x)}(P/(x)) = \mathrm{ht}_A(P) - \mathrm{ht}_A(x) = l - 1$.

□

Teorema 8.0.10. *Sia A un anello noetheriano.*

1. *Se I è un ideale di A tale che* $\mathrm{ht}(I) = n \geq 1$ *allora esistono $a_1, \ldots, a_n \in I$ tali che* $\mathrm{ht}(a_1, \ldots, a_i) = i$ *per ogni $i \leq n$.*

2. Se I è primo posso scegliere $a_1, \ldots, a_n$ in modo che I sia minimale su $(a_1, \ldots, a_n)$.

Dimostrazione.

1. Siano $P_1, \ldots, P_t$ gli ideali primi minimali di A. Per ipotesi e da 1.1.23 abbiamo che $I \nsubseteq (P_1 \cup \ldots \cup P_t)$. Sia $a_1 \in I \setminus (P_1 \cup \ldots \cup P_t)$, risulta $\mathrm{ht}(a_1) = 1$. Adesso procedendo induttivamente supponiamo di aver già scelto gli elementi $a_1, \ldots, a_i \in I$ tali che $\mathrm{ht}(a_1, \ldots, a_j) = j$ per ogni $j \leq i$. Siano $Q_1, \ldots, Q_l$ i primi minimali di $(a_1, \ldots, a_i)$, per il teorema dell'ideale principale generalizzato abbiamo che $\mathrm{ht}(Q_h) \leq i < n$, quindi $I \nsubseteq Q_h$ per ogni $h \leq l$, da cui $I \nsubseteq (Q_1 \cup \ldots \cup Q_l)$. Sia $a_{i+1} \in I \setminus (Q_1 \cup \ldots \cup Q_l)$. Adesso se P è un primo minimale di $(a_1, \ldots, a_{i+1})$ allora $Q_h \subset P$ per qualche $h \leq l$, da cui $\mathrm{ht}(P) \geq i + 1$, d'altra parte dal teorema dell'ideale principale generalizzato abbiamo $\mathrm{ht}(P) \leq i + 1$, da cui $\mathrm{ht}(P) = i + 1$. Dunque $\mathrm{ht}(a_1, \ldots, a_{i+1}) = i + 1$.

2. Se I è primo, dato che esso ha la stessa altezza di $(a_1, \ldots, a_n)$ allora non può esistere un primo P tale che $(a_1, \ldots, a_n) \subset P \subset I$, il che equivale a dire che I è un primo minimale di $(a_1, \ldots, a_n)$.

□

Corollario 8.0.11. *Sia $(A, \underline{m})$ un anello noetheriano locale tale che $\dim A = \mathrm{ht}(\underline{m}) = d$. Esistono $a_1, \ldots, a_d \in \underline{m}$ tali che $\mathrm{ht}(a_1, \ldots, a_d) = d$.*

Quindi $(a_1, \ldots, a_d)$ è $\underline{m}$-primario (il quoziente ha un solo ideale primo, quindi ogni divisore dello zero è nilpotente). Inoltre dal teorema dell'ideal principale generalizzato si ha che ogni ideale $\underline{m}$-primario non può avere meno di d generatori.

Definizione 8.0.12. *Sia $(A, \underline{m})$ un anello noetheriano tale che $\dim A = d$. L'insieme $\{a_1, \ldots, a_n\}$ è un **sistema di parametri** se $(a_1, \ldots, a_n)$ è $\underline{m}$-primario.*

Definizione 8.0.13. *Sia $(A, \underline{m})$ un anello noetheriano, si chiama **dimensione d'immersione** di A il numero*

$$\nu = \dim_{A/\underline{m}}(\underline{m}/\underline{m}^2).$$

Dal Corollario 2.1.4 abbiamo che la dimensione d'immersione è la cardinalità di un qualsiasi insieme minimale di generatori di $\underline{m}$. Dunque in generale $\nu \geq \mathrm{ht}(\underline{m}) = \dim A$.

Definizione 8.0.14. *Se $(A, \underline{m})$ è un anello noetheriano locale tale che $\nu = \dim A$ allora A è detto **locale regolare**.*

Capitolo 9

Teorema di Cayley-Hamilton*

Sia V un k-spazio vettoriale di dimensione finita $\dim(V) = n$, indichiamo con

$$\mathrm{End}(V) = \mathrm{Hom}_k(V, V).$$

$(\mathrm{End}(V), +, \circ)$ è un anello. Osserviamo che ogni elemento di k può essere visto come elemento di $\mathrm{End}(V)$, cioè

$$\varphi : k \to \mathrm{End}(V) \quad (\varphi(a))(v) = av \quad \forall v \in V$$

è un omomorfismo iniettivo di anelli.
Inoltre, fissata una base $\mathcal{A} = \{x_1, x_2, \dots, x_n\}$ di V e $f \in \mathrm{End}(V)$ si ha

$$\begin{cases} f(x_1) = a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \\ f(x_2) = a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n \\ \vdots \\ f(x_n) = a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n \end{cases}$$

in questo modo l'applicazione $\psi : \mathrm{End}(V) \to k^{n,n}$ che manda $f \in \mathrm{End}(V)$ in $A = (a_{ij}) \in k^{n,n}$ è un isomorfismo di anelli.
Per ogni $f \in \mathrm{End}(V)$ posto $A = \psi(f)$ si definisce **polinomio caratteristico** di f (o di A) il polinomio dato da

$$p(x) = \det(A - xI) \in k[x] \subseteq \mathrm{End}(V)[x].$$

Inoltre data una matrice $F = (f_{ij}) \in \mathrm{End}(V)^{n,n}$ e un vettore $\underline{x} \in V^n$ possiamo considerare il prodotto

$$* : \mathrm{End}(V) \times V^n \to V^n \quad F * \underline{x} = \left(\sum_{j=1}^{n} f_{ij}(x_j) \right).$$

$*$ è un'azione del gruppo moltiplicativo $(\mathrm{End}(V)^{n,n}, \cdot)$ su V^n. Ponendo $\underline{x} = (x_1, x_2, \dots, x_n) \in V^n$, possiamo vedere ogni endomorfismo $f \in \mathrm{End}(V)$ come matrice di $\mathrm{End}(V)^{n.n}$, precisamente associando a f la matrice fI, quindi

$$fI * \underline{x} = (f(x_i) : i = 1, \dots, n).$$

Teorema 9.0.1 (Cayley-Hamilton). *Ogni endomorfismo di V si annulla nel suo polinomio caratteristico.*

Dimostrazione. Sia $f \in \mathrm{End}(V)$, poniamo $\psi(f) = A = (a_{ij}) \in k^{n,n} \subseteq \mathrm{End}(V)^{n,n}$. Adesso abbiamo

$$fI * \underline{x} = A * \underline{x} \Rightarrow (fI - A) * \underline{x} = \underline{0}$$

moltiplicando per la matrice aggiunta $A^{\#}$ di $(fI - A) = B$ (cioè la trasposta della matrice dei cofattori) ad ambo i membri otteniamo

$$A^{\#}(B * \underline{x}) = (A^{\#}B) * \underline{x} = (\det B)I * \underline{x} = \underline{0}$$

quindi $\det(If - A)(x_i) = 0 \quad \forall i = 1, \ldots, n$, cioè $p(f) = \det(fI - A) = 0_{\mathrm{End}(V)}$. $\square$