UNIVERSITÀ DEGLI STUDI DI FERRARA

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI

Corso di Laurea Triennale in Matematica
Indirizzo Matematica Pura

IDEALI PRIMI E LOCALIZZAZIONE

Relatore:
Chiar.mo Prof.
Josef Eschgfäller

Laureanda:
Ilaria Fiorella Paglia

Anno Accademico 2010-2011

Indice

Introduzione

Questa tesi presenta alcuni dei più importanti risultati della teoria degli anelli, riguardanti in modo particolare gli ideali primi e la localizzazione rispetto ad un sottomonoide puro di un anello.

Nella prima parte della tesi la teoria viene svolta nel contesto degli anelli non necessariamente commutativi, mentre nella seconda parte sono trattate, nell'ambito dell'algebra commutativa la teoria della localizzazione e la decomposizione primaria.

Nel primo capitolo sono raccolte alcune notazioni che sono utilizzate in tutto l'elaborato.

Il secondo capitolo introduce il concetto di ideale primo e di anello primo. Elenchiamo alcune caratteristiche dell'anello dei quaternioni $\mathbb{H}$ e del suo sottoanello $\mathbb{H}_{\mathbb{Z}}$. Usiamo il lemma di Brauer, il quale afferma che, dato un ideale sinistro minimale I con $I^2 \neq 0$, esiste un elemento idempotente e tale che $I = Re$, per dimostrare che un dominio non contiene ideali sinistri minimali e quindi non tutti gli anelli contengono ideali minimali. Il capitolo prosegue definendo l'insieme $\operatorname{Spec} A$ degli ideali primi, gli ideali primi minimali, completamente primi e semiprimi. Vediamo anche alcune applicazioni sull'anello R_n^n delle matrici a n righe e n colonne, a coefficienti nell'anello non commutativo R. Nell'ultima parte del capitolo definiamo il radicale di un ideale e relative proprietà utili nell'ultimo capitolo sulla decomposizione primaria.

Nel terzo capitolo ci occupiamo di moduli e anelli noetheriani. Tra gli esempi vediamo il caso di $\mathbb{H}_{\mathbb{Z}}$ e condizioni per la noetherianità di un ∇-anello. Un altro fondamentale esempio è costituito dall'anello dei polinomi $A[x]$ a coefficienti in un anello noetheriano commutativo A. Infatti il teorema della base di Hilbert afferma che, se A è un anello noetheriano commutativo, allora anche $A[x]$ è noetheriano. Di questo teorema diamo, nel quarto capitolo, diverse dimostrazioni: la prima seguendo Gabelli, la seconda seguendo Fieseler-Kaup e l'ultima (la più breve) fornita da Heidrun Sarges.

Nel quinto capitolo sono centrali i risultati riguardanti gli ideali primari, P-primari, i radicali di ideali e gli ideali della forma $I : F$. In questo capitolo vediamo anche la definizione di anello locale (cioè contenente un unico ideale massimale $\mathfrak{m}$) e un paio di esempi. Inoltre costruiamo due anelli particolari in cui il radicale di un ideale è primo, ma l'ideale stesso non è primario.

Dopo la definizione di sottomonoide puro di un anello commutativo, nel sesto capitolo dimostriamo la relazione tra questi e gli ideali primi: infatti gli ideali primi minimali coincidono con i complementari dei sottomonoidi puri massimali.

La localizzazione di un anello A rispetto ad un sottomonoide puro S appare nel settimo capitolo. Per costruire questo anello commutativo $S^{-1}A$ definiamo una relazione di equivalenza $\sim$ sull'insieme $A \times S$ e su di esso le operazioni di addizione e di moltiplicazione. Inoltre verifichiamo che gli elementi di S sono invertibili in $S^{-1}A$. Dato un anello commutativo integro A costruiamo un omomorfismo tra la sua localizzazione $S^{-1}A$ e il suo campo dei quozienti $\mathcal{K}(A)$, sottolineando l'identificazione di $S^{-1}A$ con il sottoanello $\left\{\frac{a}{s} \mid a \in A, s \in S\right\}$ di $\mathcal{K}(A)$. Analogamente, dato $S := \{f^n \mid n \in \mathbb{N}\}$, dove $f \in A$ non è nilpotente, il sottoanello $\left\{\frac{a}{f^n} \mid a \in A, n \in \mathbb{N}\right\}$ coincide con il sottoanello $A\left[\frac{1}{f}\right]$ di $\mathcal{K}(A)$.

Nella seconda parte del capitolo studiamo, per un ideale I di A, l'ideale generalizzato $S^{-1}I$ di $S^{-1}A$; esso è proprio se e solo se $I \cap S = \emptyset$. Importante è anche la contrazione di un ideale generalizzato di A, sia in relazione alla localizzazione che alla decomposizione primaria. Tutto questo ci permette di costruire una biiezione canonica tra l'insieme degli ideali generalizzati S-saturi di A e l'insieme degli ideali generalizzati di $S^{-1}A$. Infine osserviamo che la localizzazione di un anello noetheriano è ancora noetheriana.

Un altro caso particolare lo incontriamo nel capitolo 8 dove, similmente al capitolo precedente, costruiamo la localizzazione di moduli M. Dimostriamo in particolare che l'operazione $M \longmapsto S^{-1}M$ è un funtore esatto.

Come visto nel capitolo 6, un sottomonoide puro è il complementare di un ideale primo, pertanto risulta immediato definire la localizzazione A_P di un ideale primo P. Dimostriamo che l'anello così trovato è locale e il suo unico ideale massimale è PA_P. Inoltre il campo A_P/PA_P è isomorfo a $\mathcal{K}(A/P)$.

Se un ideale I di A è decomponibile, allora ammette anche una decomposizione primaria minimale. Vediamo nel decimo e ultimo capitolo che questa è unica, e che, per ideali in anelli noetheriani, esiste sempre. Definiamo l'insieme $\operatorname{Ass} A/I$ degli ideali primi associati ad I dove
$\operatorname{Ass} A/I := \{P \in \operatorname{Spec} A \mid$ esiste $a \in A$ con$P = \sqrt{I : a}\}$ e verifichiamo che, nel caso di anelli noetheriani, essi coincidono con gli ideali primi della forma $I : a$. Consideriamo la localizzazione di un insieme finito di ideali generalizzati Δ fatta rispetto ad un sottomonoide puro S, e la applichiamo al caso in cui Δ sia proprio la decomposizione primaria minimale di un ideale I. Infatti, dato $\Delta_1 := \{Q \in \Delta \mid \sqrt{Q} \cap S = \emptyset\}$, si ha che $S^{-1}\Delta_1$ (rispettivamente Δ_1) è una decomposizione primaria minimale di $S^{-1}I$ (rispettivamente $S^*S^{-1}I$). Alla fine vediamo che per un anello noetheriano A e un ideale I di A l'insieme $\operatorname{Ass} A/I$ coincide con l'insieme degli ideali primi P che sono della forma $P = I : a$ per un elemento $a \in A$.

1. Notazioni

Osservazione 1.1. Usiamo il termine *anello* per denotare un anello (associativo) $\neq 0$, dotato di un elemento neutro della moltiplicazione. Quest'ultimo viene denotato con 1, oppure, quando bisogna indicare l'anello R stesso, con 1_R.

Similmente un omomorfismo di anelli $\varphi : R \to S$ deve soddisfare la condizione $\varphi(1_R) = 1_S$.

Se R è un anello, un *R-modulo* è un R-modulo sinistro M unitale, cioè tale che $1_R \cdot v = v$ per ogni $v \in M$.

Talvolta considereremo anche R-moduli destri, anch'essi unitali.

Definizione 1.2. Un *ideale* bilaterale, sinistro o destro di un anello R è per definizione $\neq R$. Se vogliamo includere anche R stesso, parliamo di *ideale* (bilaterale, sinistro o destro) *generalizzato*.

Il termine ideale senza specificazione della lateralità indica un ideale bilaterale.

Si noti che 0 è sempre un ideale perchè $R \neq 0$.

Osservazione 1.3. Siano R un anello e M un R-modulo. Allora R e M sono anche gruppi abeliani, quindi $\mathbb{Z}$-moduli, perciò per ogni $n \in M$ e per ogni $v \in M$ sono definiti gli elementi $n1_R \in R$ e $nv \in M$ e si ha

$$nv = \underbrace{v + v + \ldots + v}_{n} = \underbrace{(1_R + 1_R + \ldots + 1_R)}_{n}v = (n1_R)v$$

Definizione 1.4. Per un insieme X ed $n, m \in \mathbb{N} + 1$ usiamo le seguenti notazioni:

$X^n :=$ insieme dei vettori colonna di lunghezza n formati da elementi di X;

$X_m :=$ insieme dei vettori riga di lunghezza m formati da elementi di X;

$X^n_m :=$ insieme delle matrici di m righe e n colonne formate da elementi di X.

Definizione 1.5. Sia R un gruppo abeliano (ad esempio un anello o un modulo su un anello) ed X un insieme. Allora denotiamo con $R^{\underline{X}}$ l'insieme delle applicazioni $u : X \longrightarrow R$ tale che sia finito l'insieme $\{x \in X \mid u(x) \neq 0\}$.

Definizione 1.6. Per un omomorfismo φ di gruppi (e quindi anche di anelli o moduli) denotiamo con $\operatorname{Ker} \varphi$ il nucleo, con $\operatorname{Im} \varphi$ l'immagine di φ.

2. Ideali primi in un anello non commutativo

Situazione 2.1. Sia R un anello.

Definizione 2.2. Un *ideale primo* di R è un ideale P di R tale che se I e J sono ideali di R con $IJ \subset P$, allora $I \subset P$ oppure $J \subset P$.

Definizione 2.3. L'anello R si dice *primo* se 0 è un ideale primo di R.

Osservazione 2.4. L'anello R è primo se e solo se presi ideali I e J di R, tali che $IJ = 0$, allora $I = 0$ oppure $J = 0$.

Lemma 2.5. *Sia P un ideale di R. Allora sono equivalenti:*

(1) P è primo.

(2) L'anello R/P è primo.

(3) Se I e J sono ideali sinistri di R con $IJ \subset P$, allora $I \subset P$ oppure $J \subset P$.

(4) Se I e J sono ideali destri di R con $IJ \subset P$, allora $I \subset P$ oppure $J \subset P$.

(5) Se $a, b \in R$ sono tali che $aRb \subset P$, allora $a \in P$ oppure $b \in P$.

Dimostrazione. (1) $\Longrightarrow$ (2): P sia primo ed U,V ideali di R/P tali che $UV = 0$. Allora esistono ideali I e J di R con $P \subset I$ e $P \subset J$ tali che $I/P = U$, $J/P = V$.

Si ha inoltre $0 = UV = IJ/P$ e ciò significa $IJ \subset P$. Per ipotesi ad esempio $I \subset P$ e allora $U = I/P = 0$.

(2) $\Longrightarrow$ (1): Siano I e J ideali di R tali che $IJ \subset P$. Poniamo $U := (I + P)/P$ e $V := (J + P)/P$. Allora U e V sono ideali di R/P tali che $UV = 0$.

Per ipotesi si ha ad esempio $U = 0$. Ciò implica $I \subset I + P \subset P$.

(1) $\Longrightarrow$ (3): Siano I e J ideali sinistri tali che $IJ \subset P$. Allora IR e JR sono ideali di R e si ha $IRJR \subset IJR \subset PR = P$, cosicché l'ipotesi implica che ad esempio $IR \subset P$ e quindi anche $I \subset P$.

(1) $\Longrightarrow$ (4): Nello stesso modo.

(3) $\Longrightarrow$ (5): Siano $a, b \in R$ tali che $aRb \subset P$. Allora Ra e Rb sono ideali sinistri di R tali che $RaRb \subset RP = P$. Per ipotesi ad esempio $Ra \subset P$ e quindi anche $a \in P$.

(4) $\Longrightarrow$ (5): Nello stesso modo.

(5) $\Longrightarrow$ (1): Siano I e J ideali di P con $IJ \subset P$. Assumiamo, per assurdo, che $I \not\subset P$ e $J \not\subset P$. Allora esistono $a \in I \setminus P$ e $b \in J \setminus P$. Però $aRb \subset aRRb \subset IJ \subset P$ in contrasto con l'ipotesi.

Proposizione 2.6. *Ogni ideale (bilaterale, sinistro, destro) di R è contenuto in un ideale (bilaterale, sinistro, destro) massimale.*

Dimostrazione. Ciò è una conseguenza facile del lemma di Zorn.

Corollario 2.7. *R contiene un ideale massimale.*

Dimostrazione. 0 è un ideale di R ed è contenuto in un ideale massimale per la proposizione 2.6.

Proposizione 2.8. *Ogni ideale massimale di R è primo.*

Dimostrazione. Sia M un ideale massimale di R e siano I e J ideali di R tali che $IJ \subset M$. Assumiamo che $I \not\subset M$. Allora $I+M = R$ cosicché

$$J = RJ = (I+M)J \subset IJ + MJ \subset M + M = M$$

Corollario 2.9. *R contiene un ideale primo.*

Nota 2.10. Come nell'analisi complessa si scrive $x + iy$ per $(x, y) = x\delta_1 + y\delta_2 \in \mathbb{R}_2$, identificando quindi $\mathbb{R}$ con $\mathbb{R} \times 0$ ed 1 con δ_1, i con δ_2, così nell'algebra dei quaternioni che introdurremo adesso si scrive
$x + iy + jz + kt$ per $(x, y, z, t) = x\delta_1 + y\delta_2 + z\delta_3 + t\delta_4 \in \mathbb{R}_4$.

Otteniamo un'applicazione bilineare $\mathbb{R}_4 \times \mathbb{R}_4 \longrightarrow \mathbb{R}_4$ se definiamo i prodotti degli elementi della base standard secondo la seguente tabella:

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Il prodotto di due elementi qualsiasi di $\mathbb{R}_4$ si ottiene per estensione lineare. Si ha così ad esempio:

$$\begin{aligned}
&(2+3i+4j+5k)(6+7i+8j+9k) = 12+14i+16j+18k+18i \\
&+21i^2+24ij+27ik+24j+28ji+32j^2+36jk+30k+35ki+40kj \\
&+45k^2 = 12+14i+16j+18k+18i-21+24k-27j+24j-28k \\
&-32+36i+30k+35j-40i-45 = (12-21-32-45)+(14+18+36 \\
&-40)i+(16-27+24+35)j+(18+24-28+30)k = -86+28i+48j+44k
\end{aligned}$$

Si dimostra facilmente che $\mathbb{R}_4$ con questa moltiplicazione è un anello (e in più una $\mathbb{R}$-algebra) che si chiama l'*anello dei quaternioni*. Questo anello è stato inventato da William Rowan Hamilton (1805-1865) e in suo onore viene spesso denotato, come faremo anche noi, con la lettera $\mathbb{H}$.

Tramite l'algebra dei quaternioni si può descrivere la cinematica dello spazio $\mathbb{R}^3$; per un'esposizione più dettagliata di questo aspetto geometrico rimandiamo al libro di Kuipers; cfr. anche Pottmann/Wallner, pagg. 522-546.

Algebre di quaternioni possono essere definite anche con regole leggermente più generali e su altri campi; cfr. Pierce, pagg. 13-20.

Proposizione 2.11. $\mathrm{Centro}(\mathbb{H}) = \mathbb{R}$

Dimostrazione. Sia $p = a + bi + cj + dk \in \mathrm{Centro}(\mathbb{H})$ con $a, b, c, d \in \mathbb{R}$.

Allora in particolare $pi = ip$. Però

$$\begin{aligned} pi &= ai - b + cji + dki = ai - b - ck + dj \\ ip &= ia - b + cij + dik = ai - b + ck - dj \end{aligned}$$

per cui $c = 0 = d$ e quindi $p = a + ib$. Inoltre $pj = jp$. Però

$$\begin{aligned} pj &= aj + bij = aj + bk \\ jp &= ja + bji = aj - bk \end{aligned}$$

e vediamo che anche $b = 0$, per cui $p \in \mathbb{R}$.

Definizione 2.12.

(1) R si chiama un *dominio*, se per $a, b \in R \setminus 0$ si ha sempre $ab \neq 0$.

Un dominio commutativo è detto anche *dominio integro*.

(2) Un elemento a di R si dice *invertibile*, se esiste un elemento $a^{-1} \in R$ tale che $a \cdot a^{-1} = a^{-1} \cdot a = 1_R$. Si vede facilmente che a^{-1}, quando esiste, è univocamente determinato.

Denotiamo con R^* l'insieme degli elementi invertibili di R.
Si dimostra facilmente che $(R^*, \cdot)$ è un gruppo.

(3) R si chiama un *anello con divisione* (in inglese *division ring* oppure *skew field*, in italiano talvolta anche *corpo*), se ogni elemento $\neq 0$ di R è invertibile, se cioè $R^* = R \setminus 0$.

È chiaro che ogni sottoanello di un anello con divisione è un dominio.

Osservazione 2.13. Ogni dominio è un anello primo.

Osservazione 2.14. Per $p = a + bi + cj + dk \in \mathbb{H}$ con $a, b, c, d \in \mathbb{R}$ poniamo $\bar{p} := a - bi - cj - dk$. Allora:

(1) $p\bar{p} = \bar{p}p = a^2 + b^2 + c^2 + d^2 = \|p\|^2$.
In particolare vediamo che $p\bar{p} \in \mathbb{R}$.

(2) Quindi $p\bar{p} \neq 0$ per $p \neq 0$.
In tal caso perciò è ben definito il numero reale $\dfrac{1}{p\bar{p}}$.

(3) Sia $p \neq 0$. Allora p è invertibile e si ha
$p^{-1} = \dfrac{\bar{p}}{p\bar{p}} = \dfrac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}$

Dimostrazione. (1) Infatti

$$\begin{aligned} p\bar{p} &= (a + bi + cj + dk)(a - bi - cj - dk) \\ &= a^2 - abi - acj - adk + bai - b^2i^2 - bcij - bdik + caj \\ &\quad - cbji - c^2j^2 - cdjk + dak - dbki - dckj - d^2k^2 \\ &= a^2 + b^2 + c^2 + d^2 - bc(ij + ji) - bd(ik + ki) - cd(jk + kj) \\ &= a^2 + b^2 + c^2 + d^2. \end{aligned}$$

(2) e (3) Chiari.

Corollario 2.15. $\mathbb{H}$ *è un anello con divisione.*

Definizione 2.16. Sia $\mathbb{H}_{\mathbb{Z}} := \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$.

È chiaro che $\mathbb{H}_{\mathbb{Z}}$ è un sottoanello di $\mathbb{H}$ e quindi un dominio.

Lemma 2.17. $\mathbb{H}_{\mathbb{Z}}^* = \{\pm 1, \pm i, \pm j, \pm k\}$.

Dimostrazione. (1) Gli elementi indicati sono detti invertibili, infatti $i^{-1} = -i, j^{-1} = -j, k^{-1} = -k$, come segue dalle relazioni $i^2 = j^2 = k^2 = -1$.

(2) Sia $p := a + bi + cj + dk$ con $a, b, c, d \in \mathbb{Z}$ e $p \neq 0$, $p^{-1} \in \mathbb{H}_{\mathbb{Z}}$. Dalla formula nel punto (3) dell'oss. 2.14 segue che $a^2 + b^2 + c^2 + d^2$ divide a, b, c, d e ciò è evidentemente possibile solo se esattamente uno dei quattro numeri a, b, c, d è $\neq 0$; questo numero deve inoltre essere uguale a ± 1.

Corollario 2.18. $\mathbb{H}_{\mathbb{Z}}$ *non è un anello con divisione.*

Definizione 2.19. Un *ideale* (bilaterale, sinistro, destro) *minimale* di R è un ideale (bilaterale, sinistro, destro) minimale tra gli ideali (bilaterali, sinistri, destri) diversi dallo 0 di R.

Osservazione 2.20. $\mathbb{Z}$ non possiede ideali minimali.

Quindi anche in un anello commutativo in generale non esistono ideali minimali.

Definizione 2.21. (1) Sia M un R-modulo. Per un sottoinsieme $X \subset M$ poniamo

$X^{\perp} := \{a \in R \mid aX = 0\}$

(2) Sia N un R-modulo. Per un sottoinsieme $Y \subset N$ poniamo

$Y_{\perp} := \{a \in R \mid Ya = 0\}$

Lemma 2.22 (lemma di Brauer). *Sia I un ideale sinistro minimale di R con $I^2 \neq 0$. Allora esiste un elemento idempotente $e \in I$ tale che $I = Re$.*

Dimostrazione. L'ipotesi $I^2 \neq 0$ implica che esiste un elemento $a \in I$ tale che $Ia \neq 0$. Ia è un ideale sinistro di R contenuto in I, per cui $Ia = I$ a causa della minimalità di I. Ciò implica che esiste $e \in I$ con $a = ea$. Da ciò segue $e^2 - e \in I \cap a^{\perp}$.

L'insieme $I \cap a^{\perp}$ è un ideale sinistro di R che è contenuto in I, ma non coincide con I perché $e \notin a^{\perp}$ (altrimenti si avrebbe $a = ea = 0$). Ma I è minimale, quindi $I \cap a^{\perp} = 0$ e ciò implica $e^2 = e$. Infine $0 \neq Re \subset I$, per cui $Re \equiv I$.

Osservazione 2.23. R sia un dominio. Allora gli unici elementi idempotenti di R sono 0 ed 1.

Dimostrazione. Sia $e \in R$ idempotente. Allora $e(e-1) = 0$, per cui $e = 1$ oppure $e = 0$, poiché siamo in un dominio.

Proposizione 2.24. *R sia un dominio. Allora R non possiede ideali sinistri minimali.*

Dimostrazione. Ciò segue dal lemma 2.22 e dall'oss. 2.23.

Corollario 2.25. *$\mathbb{H}_{\mathbb{Z}}$ non possiede un ideale sinistro minimale.*

Definizione 2.26. Un *ideale primo minimale* di R è un ideale primo di R che non contiene nessun altro ideale primo.

Definizione 2.27. Poniamo

$$\begin{aligned} \operatorname{Spec} R &:= \text{ insieme degli ideali primi di } R \\ \operatorname{Max} R &:= \text{ insieme degli ideali massimali di } R \end{aligned}$$

Per un sottoinsieme $X \subset R$ sia inoltre

$\operatorname{Spec} R : X := \{P \in \operatorname{Spec} R \mid X \subset P\}$

Proposizione 2.28. *Ogni ideale primo P di R contiene un ideale primo minimale.*

Dimostrazione. Consideriamo l'insieme $\operatorname{Spec} R$, ordinato per inclusione. Dal cor. 2.7 sappiamo che $\operatorname{Spec} R \neq \emptyset$. Sia $\mathcal{C}$ una catena non vuota in $\operatorname{Spec} R$ e $Q := \bigcap\limits_{T \in \mathcal{C}} T$. Allora Q è un ideale di R contenuto in P.

Dobbiamo dimostrare che Q è primo. Siano $a, b \in R$ tali che $aRb \subset Q$. Assumiamo, per assurdo, che $a, b \notin Q$. Allora esistono $S, T \in \mathcal{C}$ con $a \notin S$ e $b \notin T$. Siccome $\mathcal{C}$ è una catena, abbiamo ad esempio $S \subset T$. Allora $a, b \notin S$, mentre $aRb \subset Q \subset S$. Ma ciò non è possibile, perché S è primo.

Il lemma di Zorn implica l'enunciato.

Definizione 2.29. Un ideale P di R si dice *completamente primo*, se R/P è un dominio, cioè se $ab \in P$ implica $a \in P$ oppure $b \in P$.

È evidente dalle definizioni che un ideale completamente primo è primo e che, quando R è commutativo, un ideale primo è completamente primo.

Lemma 2.30. *Siano $\varphi : R \to \widetilde{R}$ un omomorfismo di anelli e J un ideale di $\widetilde{R}$. Allora:*

(1) $\varphi^{-1}(J)$ è un ideale di R.

(2) Se J è primo e φ è suriettivo, allora anche $\varphi^{-1}(J)$ è primo.

(3) Se J è completamente primo, allora $\varphi^{-1}(J)$ è completamente primo.

Dimostrazione. (1) Siano $a, b \in \varphi^{-1}(J)$ ed $r \in R$. Allora

$$\begin{aligned} \varphi(a+b) &= \varphi(a) + \varphi(b) \in J + J = J \\ \varphi(ra) &= \varphi(r)\varphi(a) \in \widetilde{R}J = J \\ \varphi(ar) &= \varphi(a)\varphi(r) \in J\widetilde{R} = J \end{aligned}$$

(2) Siano φ suriettivo e J primo. Siano $a, b \in R$ tali che $aRb \subset \varphi^{-1}(J)$, cioè $\varphi(aRb) \subset J$. Ciò implica

$$\varphi(a)\widetilde{R}\varphi(b) = \varphi(a)\varphi(R)\varphi(b) = \varphi(aRb) \subset J$$

Allora $\varphi(a) \in J$ oppure $\varphi(b) \in J$, cioè $a \in \varphi^{-1}(J)$ oppure $b \in \varphi^{-1}(J)$.

(3) Sia J un ideale completamente primo. Siano $a, b \in R$ tali che $ab \in \varphi^{-1}(J)$, cioè $\varphi(a)\varphi(b) = \varphi(ab) \in J$. Ciò implica che $\varphi(a) \in J$ oppure $\varphi(b) \in J$, cioè $a \in \varphi^{-1}(J)$ oppure $b \in \varphi^{-1}(J)$.

Lemma 2.31. *Siano $\varphi : R \to \widetilde{R}$ un omomorfismo suriettivo di anelli e P un ideale di R. Allora:*

(1) $\varphi(P)$ è un ideale generalizzato di $\widetilde{R}$.

(2) Se $\operatorname{Ker}\varphi \subset P$, allora $\varphi(P)$ è un ideale di $\widetilde{R}$.

(3) Se $\operatorname{Ker}\varphi \subset P$ e P è primo, allora anche $\varphi(P)$ è primo.

<u>Dimostrazione.</u> (1) È chiaro che $\varphi(P)$ è un sottogruppo additivo di $\widetilde{R}$. Siano $u \in \varphi(P)$ e $t \in \widetilde{R}$. Allora esistono $p \in P$ ed $a \in R$ tali che $u = \varphi(p)$ e $\varphi(a) = t$. Siccome P è un ideale di R, si ha $ap \in P$. Perciò $tu = \varphi(a)\varphi(p) = \varphi(ap) \in \varphi(P)$ e similmente $ut \in \varphi(P)$.

(2) Assumiamo, per assurdo, che $1_{\widetilde{R}} \in \varphi(P)$. Allora esiste $a \in P$ tale che $\varphi(a) = 1_{\widetilde{R}}$. Siccome anche $\varphi(1_R) = 1_{\widetilde{R}}$, allora $1_R - a \in \operatorname{Ker}\varphi \subset P$ e ciò implica $1_R \in P$, una contraddizione.

(3) Siano $u, v \in \widetilde{R} \setminus \varphi(P)$. Per ipotesi esistono $s, t \in R$ tali che $\varphi(s) = u$ e $\varphi(t) = v$. Necessariamente $s, t \notin P$, perciò, essendo P primo, esiste $a \in R$ tale che $sat \notin P$.

È sufficiente dimostrare che $u\varphi(a)v = \varphi(sat) \notin \varphi(P)$.

Assumiamo, per assurdo, che esista $p \in P$ tale che $\varphi(sat) = \varphi(p)$. Allora $p - sat \in \operatorname{Ker}\varphi \subset P$ e quindi $sat \in P$, una contraddizione.

Corollario 2.32. *Sia I un ideale di R.*

(1) Se P è un ideale primo di R tale che $P \supset I$, allora P/I è un ideale primo di R/I.

(2) Se Q è un ideale primo di R/I, allora esiste un unico ideale primo P di R con $P \supset I$ e tale che $Q = P/I$. Esplicitamente si ha $P = \{a \in R \mid I + a \in Q\}$.

Corollario 2.33. *Sia I un ideale di R. Allora esiste una biiezione naturale*

$$\begin{aligned} \operatorname{Spec} R/I &\longleftrightarrow \operatorname{Spec} R : I \\ Q &\longmapsto \{a \in R \mid I + a \in Q\} \\ P/I &\longleftarrow\!\shortmid P \end{aligned}$$

Corollario 2.34. *Sia I un ideale di R. Allora ogni elemento di $\operatorname{Spec} R : I$ contiene un elemento minimale di $\operatorname{Spec} R : I$.*

<u>Dimostrazione.</u> Ciò segue dalla prop. 2.28, utilizzando il cor. 2.33.

Lemma 2.35. *Ogni insieme non vuoto di ideali di R possieda un elemento massimale. Allora esistono ideali primi $P_1, \ldots, P_n$ di R tali che $P_1 P_2 \ldots P_n = 0$.*

Dimostrazione. Assumiamo, per assurdo, che l'enunciato non sia vero. Allora l'insieme $\mathcal{A}$ degli ideali di R, che non contengono un prodotto finito di ideali primi, contiene l'ideale 0 e quindi non è vuoto. Per ipotesi esiste un elemento massimale E di $\mathcal{A}$.

Allora però anche l'anello R/E è un controesempio e possiamo sostituire R con R/E, avendo adesso per la massimalità di E la seguente situazione:

(1) Un prodotto finito di ideali primi di R non è mai 0.

(2) In particolare 0 non è primo.

(3) Ogni ideale $\neq 0$ di R contiene un prodotto finito di ideali primi.

Per il punto (2) esistono ideali $I, J \neq 0$ tali che $IJ = 0$. Per il punto (3) esistono ideali primi $P_1, \ldots, P_m, Q_1, \ldots, Q_n$ tali che $P_1 \ldots P_m \subset I$ e $Q_1 \ldots Q_n \subset J$. Ma allora $0 = IJ \supset P_1 \ldots P_m Q_1 \ldots Q_n$ in contrasto con il punto (1).

Corollario 2.36. *Se in R esistono ideali primi $P_1, \ldots, P_m$ tali che $P_1 \ldots P_m = 0$, allora R contiene al massimo m ideali primi minimali.*

Dimostrazione. Sia Q un ideale primo minimale di R. Allora $P_1 \ldots P_m = 0 \subset Q$ implica che ad esempio $Q \supset P_1$ perché Q è primo. Allora $Q = P_1$ per la minimalità di Q. Vediamo così che ogni ideale primo minimale di R appartiene all'insieme $\{P_1, \ldots, P_m\}$.

Proposizione 2.37. *R sia noetheriano a sinistra o a destra. Allora:*

(1) Esistono ideali primi $P_1, \ldots, P_m$ di R tali che $P_1 P_2 \ldots P_m = 0$.

(2) R contiene solo un numero finito di ideali primi minimali.

Dimostrazione. (1) Segue dal lemma 2.35.

(2) Segue dal punto (1), utilizzando il cor. 2.36.

Definizione 2.38. Un ideale H di R si dice *semiprimo*, se H è intersezione (anche infinita) di ideali primi.

L'anello R si dice *semiprimo*, se 0 è intersezione di ideali primi di R.

Osservazione 2.39. Un ideale H di R è semiprimo se e solo se R/H è semiprimo.

Dimostrazione. Ciò segue dal cor. 2.33.

Osservazione 2.40. Gli ideali semiprimi di $\mathbb{Z}$ sono esattamente gli ideali $m\mathbb{Z}$, dove $m = 0$ oppure $m \in \mathbb{N}+1$ è un numero libero da quadrati (cioè tale che $p^2 \nmid m$ per ogni primo p).

Osservazione 2.41. Siano I, J, P ideali di R tali che $IJ \subset P$. Allora:

(1) $(I + P)(J + P) \subset P$.

(2) Se $I \not\subset P$ e $J \not\subset P$, allora $I+P$ e $J+P$ sono ideali di R.

Dimostrazione. (1) $(I+P)(J+P) = IJ + PJ + IP + P^2 \subset P$.

(2) Sia ad esempio $I+P=R$. Allora dal punto (1) si ha che $J+P \subset P$ e quindi anche $J \subset P$, una contraddizione.

Definizione 2.42. Un *m-sistema* in R è un sottoinsieme $S \subset R$ con la proprietà che per ogni $s,t \in S$ esiste $x \in R$ tale che $sxt \in S$.

Osservazione 2.43. Un ideale P di R è primo se e solo se $R \setminus P$ è un m-sistema.

Dimostrazione. Ciò segue dal punto (5) del lemma 2.5.

Lemma 2.44. *S sia un m-sistema in R tale che $0 \notin S$. Sia $\mathcal{D}$ l'insieme degli ideali J di R tali che $J \subset R \setminus S$. Allora:*

(1) Ogni elemento di $\mathcal{D}$ è contenuto in un elemento massimale di $\mathcal{D}$.

(2) Ogni elemento massimale di $\mathcal{D}$ è un ideale primo.

Dimostrazione. (1) Per ipotesi $0 \in \mathcal{D}$, per cui $\mathcal{D} \neq \emptyset$. Sia $\mathcal{C}$ una catena non vuota di $\mathcal{D}$. Considero $P := \bigcup\limits_{T \in \mathcal{C}} T$ e vedo che $P \in \mathcal{D}$.

Per ogni $T \in \mathcal{C}$ si ha che $T \subset R \setminus S$, da cui segue che anche $P \subset R \setminus S$. Inoltre P è un ideale di R poiché è unione di ideali di R.

(2) Siano P un elemento massimale di $\mathcal{D}$ e I, J ideali di R tali che $IJ \subset P$. Assumiamo, per assurdo, che $I \not\subset P$ e $J \not\subset P$. Per l'oss. 2.41 $I+P$ e $J+P$ sono ideali di R con $(I+P)(J+P) \subset P$. Allora $P \subsetneqq I+P$ e $P \subsetneqq J+P$, cosicché dalla massimalità di P in $\mathcal{D}$ segue che esistono $s \in S \cap (I+P)$ e $t \in S \cap (J+P)$. Segue che esiste $x \in R$ tale che $sxt \in S$. D'altra parte $sxt \in (I+P)R(J+P) = (I+P)(J+P) \subset P$, una contraddizione.

Definizione 2.45. Per $a \in R$ sia $\mathcal{S}(a)$ l'insieme degli m-sistemi in R che contengono a.

Osservazione 2.46. Sia $a \in R$. Allora $\{a^n \mid n \in \mathbb{N}\} \in \mathcal{S}(a)$.

Definizione 2.47. Per un ideale I di R sia

$$\sqrt{I} := \{a \in R \mid S \cap I \neq \emptyset \text{ per ogni } S \in \mathcal{S}(a)\}$$

Teorema 2.48. *Sia I un ideale di R. Allora $\sqrt{I}$ è l'intersezione di tutti gli ideali primi di R che contengono I.*

Dimostrazione. (1) Siano $a \in \sqrt{I}$ e $P \in \operatorname{Spec} R : I$. Assumiamo, per assurdo, che $a \notin P$, ovvero $a \in R \setminus P =: S$. Per l'oss. 2.43 $S \in \mathcal{S}(a)$, cosicché l'ipotesi $a \in \sqrt{I}$ implica $S \cap I \neq \emptyset$. Ma $I \subset P$ implica che anche $S \cap P \neq \emptyset$, una contraddizione.

(2) Sia $a \notin \sqrt{I}$. Ciò significa che esiste un $S \in \mathcal{S}(a)$ tale che $I \subset R \setminus S$. Allora per il lemma 2.44 esiste un ideale primo $P \in \operatorname{Spec} R : I$, tale che $P \subset R \setminus S$, da cui segue che $a \notin P$.

Corollario 2.49. *Sia I un ideale di R. Allora $\sqrt{I}$ è il più piccolo ideale semiprimo di R che contiene I.*

Corollario 2.50. *Un ideale H di R è semiprimo se e solo se $H = \sqrt{H}$.*

Un ideale semiprimo è quindi uguale all'intersezione di tutti gli ideali primi che lo contengono.

Definizione 2.51. Un *n-sistema* in R è un sottoinsieme $T \subset R$ con la proprietà che per ogni $t \in T$ esiste $x \in R$ tale che $txt \in T$.

Definizione 2.52. Per $t, x \in R$ poniamo $t[x] := txt$.

Lemma 2.53. *Siano $t, x_1, x_2, \ldots \in R$. Allora*

$$S := \{t, t[x_1], t[x_1][x_2], t[x_1][x_2][x_3], \ldots\}$$

è un m-sistema.

Dimostrazione. Poniamo $s_0 := t$ ed $s_i := t[x_1] \ldots [x_i]$ per $i > 0$ e consideriamo $s_i, s_j \in S$.

Per $i = j$ allora $s_i x_{i+1} s_i = s_{i+1} \in S$.

Per $i > j$ esiste $y \in R$ tale che $s_i = s_j[y]$. Allora

$s_i x_{i+1} s_j y s_j = s_i x_{i+1} s_i = s_{i+1} \in S$.

Per $i < j$ si conclude allo stesso modo.

Lemma 2.54. *(1) Ogni m-sistema è un n-sistema.*

(2) T sia un n-sistema in R. Allora per ogni $t \in T$ esiste un m-sistema S in R tale che $t \in S \subset T$.

Dimostrazione. (1) Chiaro.

(2) Per ipotesi esiste $x_1 \in R$ tale che $t[x_1] \in T$, quindi esiste anche $x_2 \in R$ tale che $t[x_1][x_2] \in T$ e così via.

Sia $S := \{t, t[x_1], t[x_1][x_2], t[x_1][x_2][x_3], \ldots\}$. È chiaro che $t \in S \subset T$. Per il lemma 2.53 S è un m-sistema.

Proposizione 2.55. *Per un ideale H di R sono equivalenti:*

(1) H è semiprimo.

(2) Per ogni $a \in R$ l'inclusione $aRa \subset H$ implica $a \in H$.

(3) $R \setminus H$ è un n-sistema.

Dimostrazione. (1) $\Longrightarrow$ (2): Se H è semiprimo, allora $H = \bigcap\limits_{P \in \operatorname{Spec} R : H} P$.
Sia $a \in R$ tale che $aRa \subset H$. Per il punto (5) del lemma 2.5 allora $a \in P$ per ogni $P \in \operatorname{Spec} R : H$, ovvero $a \in H$.

(2) $\Longleftrightarrow$ (3): Chiaro.

(3) $\Longrightarrow$ (1): $R \setminus H$ sia un n-sistema. Dimostriamo che $\sqrt{H} \subset H$.
Sia $a \in \sqrt{H}$. Assumiamo, per assurdo, che $a \notin H$. Per il lemma 2.54 esiste un m-sistema S di R tale che $a \in S \subset R \setminus H$ e quindi $S \cap H = \emptyset$. Ma ciò non è possibile perché $a \in \sqrt{H}$.

Proposizione 2.56. *Per un ideale H di R sono equivalenti:*

(1) H è semiprimo.

(2) Se I è un ideale sinistro o destro di R con $I^2 \subset H$, allora $I \subset H$.

(3) Se I è un ideale di R con $I^2 \subset H$, allora $I \subset H$.

Dimostrazione. (1) $\Longrightarrow$ (2): Sia I un ideale sinistro o destro di R tale che $I^2 \subset H$. Se H è semiprimo allora H è l'intersezione di tutti gli ideali primi che lo contengono. Perciò $I \subset P$ per ogni $P \in \operatorname{Spec} R : H$ e pertanto $I \subset H$.

(2) $\Longrightarrow$ (3): Chiaro.

(3) $\Longrightarrow$ (1): Dimostriamo che H soddisfa il punto (2) della prop. 2.55. Sia $a \in R$ tale che $aRa \subset H$. Allora $RaRRaR = RaRaR \subset RHR = H$ e quindi, per ipotesi, $RaR \subset H$, perché RaR è un ideale. Ciò implica $a \in H$.

Definizione 2.57. $\sqrt{0}$ si chiama il *radicale* di Baer-McCoy di R.

Per il teorema 2.48 $\sqrt{0}$ è un ideale semiprimo e coincide con l'intersezione di tutti gli ideali primi di R.

Osservazione 2.58. Sia I un ideale di R. Allora per ogni $a \in \sqrt{I}$ esiste $n \in \mathbb{N}$ tale che $a^n \in I$.

Dimostrazione. Sia $a \in \sqrt{I}$. Per l'oss. 2.46 $S := \{a^n \mid n \in \mathbb{N}\} \in \mathcal{S}(a)$ per cui $S \cap I \neq \emptyset$. Da ciò segue l'enunciato.

Corollario 2.59. *Ogni elemento di $\sqrt{0}$ è nilpotente.*

Definizione 2.60. Un ideale (sinistro, destro, bilatero) I di R si dice *nilpotente*, se esiste $n \in \mathbb{N}$ tale che $I^n = 0$.

Lemma 2.61. *Siano H un ideale semiprimo ed I un ideale sinistro o destro di R tale che $I^n \subset H$ per qualche $n \in \mathbb{N}$. Allora $I \subset H$.*

Dimostrazione. Quando $n = 1$, è chiaro.

Lo dimostriamo per $n > 1$. Assumiamo che l'enunciato valga per $n - 1$. Si noti che per $n \geq 2$ si ha che $2n - 2 \geq n$. Allora

$(I^{n-1})^2 = I^{2n-2} \subset I^n \subset H$

D'altra parte H è semiprimo, quindi dal punto (2) della prop. 2.56 segue che $I^{n-1} \subset H$, pertanto usando l'ipotesi di induzione segue la tesi.

Corollario 2.62. *$\sqrt{0}$ contiene ogni ideale sinistro o destro nilpotente di R.*

Dimostrazione. Ciò segue dal lemma 2.61, perché $\sqrt{0}$ è semiprimo per il cor. 2.49.

Proposizione 2.63. *R sia noetheriano a sinistra o a destra. Allora l'ideale $\sqrt{0}$ è nilpotente.*

Dimostrazione. Dal punto (1) della prop. 2.37 segue che esistono ideali primi $P_1, \dots, P_m$ di R tali che $P_1 \dots P_m = 0$. In particolare $\sqrt{0} \subset P_i$ per ogni $i \in \{1, \dots, m\}$, allora $\sqrt{0}^m \subset P_1 \dots P_m = 0$.

Osservazione 2.64. Sono equivalenti:

(1) R è semiprimo.

(2) $\sqrt{0} = 0$.

(3) R non possiede un ideale sinistro nilpotente $\neq 0$.

(4) R non possiede un ideale nilpotente $\neq 0$.

Dimostrazione. (1) $\Longleftrightarrow$ (2): Segue direttamente dal cor. 2.50.

(2) $\Longrightarrow$ (3): Segue direttamente dal cor. 2.62.

(3) $\Longrightarrow$ (4): Chiaro.

(4) $\Longrightarrow$ (1): Sia I un ideale di R con $I^2 = 0$. L'ipotesi implica $I = 0$ e quindi è soddisfatta la condizione (3) nella prop. 2.56.

Definizione 2.65. L'anello R si dice *ridotto*, se non contiene elementi nilpotenti $\neq 0$.

Osservazione 2.66. Un anello ridotto è semiprimo.

Dimostrazione. Per il cor. 2.59 $\sqrt{0} = 0$. L'anello è quindi semiprimo per l'oss. 2.64.

Definizione 2.67. Un elemento $a \in R$ si dice *fortemente nilpotente*, se per ogni successione $x_1, x_2, x_3, \dots$ di elementi di R esiste $n \in \mathbb{N}+1$ tale che $a[x_1] \dots [x_n] = 0$.

Proposizione 2.68. *$\sqrt{0}$ è l'insieme di tutti gli elementi fortemente nilpotenti di R.*

Dimostrazione. (1) Sia $a \in \sqrt{0}$. Allora per ogni $S \in \mathcal{S}(a)$, $0 \in S$. Assumiamo, per assurdo, che a non sia un elemento fortemente nilpotente di R. Esiste allora una successione di elementi $x_1, x_2, x_3 \dots$ di R tali che per ogni $n \in \mathbb{N}+1$ si ha $a[x_1] \dots [x_n] \neq 0$. Allora posso considerare $S := \{a, a[x_1], a[x_1][x_2], \dots\}$.

Per il lemma 2.53 $S \in \mathcal{S}(a)$ ma $0 \notin S$, una contraddizione.

(2) Sia a un elemento fortemente nilpotente di R e sia $S \in \mathcal{S}(a)$. Per il punto (1) del lemma 2.54, S è un n-sistema e dato che $a \in S$, allora esiste $x_1 \in R$ tale che $a[x_1] \in S$. Allora posso costruire una successione di elementi $x_1, \dots, x_n$ di R tali che $0 = a[x_1] \dots [x_n] \in S$, cioè $a \in \sqrt{0}$.

Osservazione 2.69. Sono equivalenti:

(1) R è semiprimo.

(2) Se I e J sono ideali di R con $IJ = 0$, allora $I \cap J = 0$.

Dimostrazione. (1) $\Longrightarrow$ (2): R sia semiprimo. Sia $IJ = 0$. Allora $IJ \subset P$ per ogni $P \in \operatorname{Spec} R$. Perciò $I \subset P$ o $J \subset P$ e quindi $I \cap J \subset P$ per ogni $P \in \operatorname{Spec} R$. Ciò implica $I \cap J \subset \sqrt{0} = 0$.

(2) $\Longrightarrow$ (1): Sia I un ideale di R con $I^2 = 0$, segue che $I \cap I = I = 0$. Allora il punto (3) della prop. 2.56 è verificato, quindi 0 è semiprimo.

Osservazione 2.70. Per ogni $n \in \mathbb{N} + 1$, per ogni $i, j, k, l \in \{1, \ldots, n\}$ e per ogni $A \in R^n_n$ vale $A^i_j \delta_l \delta^k = \delta_l \delta^i A \delta_j \delta^k$

Proposizione 2.71. *(1) Sia I un ideale di R. Allora I^n_n è un ideale di R^n_n.*

(2) Sia L un ideale di R^n_n. Allora esiste un ideale I di R, univocamente determinato, tale che $L = I^n_n$.
Esplicitamente si ha $I = \{A^1_1 \mid A \in L\}$.

Dimostrazione. (1) Chiaro.

(2) È chiaro che $I^n_n = J^n_n$ per ideali I, J di R implica $I = J$. Sia I come nell'enunciato. Dimostriamo che $L = I^n_n$.

(2a) Sia $A \in L$. Per ogni $B \in R^n_n$ si ha che $AB \in L$ oppure $BA \in L$.

In particolare per ogni $i, j \in \{1, \ldots, n\}$ esiste $\widetilde{A} \in L$ tale che
$A^i B_j = \widetilde{A}^1_1 \in I$. Dato che $B^i_j \in R$ allora $A^i_j \in I$ per ogni i, j, cioè $A \in I^n_n$.

(2b) Sia $A \in I^n_n$. Allora $A^i_j \in I$ per ogni $i, j \in \{1, \ldots, n\}$, dove I è un ideale di R. Sia poi $B \in R^n_n$ allora $B^i_j \in R$. In particolare $AB = \sum A^i B_j \delta_i \delta^j$ con $i, j \in \{1, \ldots, n\}$, dove $A^i B_j \in IR = I$. Pertanto $A \in L$.

Definizione 2.72. L'anello R si chiama *semplice*, se R non possiede ideali $\neq 0$.

Osservazione 2.73. R sia semplice. Allora anche R^n_n è un anello semplice per ogni $n \in \mathbb{N} + 1$.

Corollario 2.74. *R sia un anello con divisione. Allora R^n_n è un anello semplice per ogni $n \in \mathbb{N} + 1$.*

Osservazione 2.75. Sia $n \in \mathbb{N} + 1$. Allora R è primo se e solo se R^n_n è primo.

Dimostrazione. (1) Siano I, J ideali di R allora $L := I^n_n$ e $N := J^n_n$ sono ideali di R^n_n. Siano L, N tali che $LN = 0_{R^n_n}$, allora $IJ = 0$. Segue che $I = 0$ oppure $J = 0$. Sia ad esempio $I = 0$, ciò implica che $L = 0$.

(2) Siano L, N ideali di R^n_n tali che $LN = 0_{R^n_n}$. Dal punto (2) della prop. 2.71 segue che esistono due ideali I, J di R tali che
$I = \{A^1_1 \mid A \in L\}$ e $J = \{B^1_1 \mid B \in N\}$. D'altra parte R^n_n è primo perciò $L = 0_{R^n_n}$ oppure $N = 0_{R^n_n}$, cioè $I = 0$ oppure $J = 0$.

3. Anelli noetheriani

Situazione 3.1. Siano R un anello ed M un R-modulo.

Definizione 3.2. M si dice *noetheriano*, se ogni sottomodulo di M è finitamente generato.

Proposizione 3.3. *Sono equivalenti:*

(1) M è noetheriano.

(2) Per ogni catena $\mathcal{C} \neq \emptyset$ di sottomoduli di M si ha $\bigcup\limits_{N \in \mathcal{C}} N \in \mathcal{C}$.

(3) Ogni insieme $\neq \emptyset$ di sottomoduli di M possiede un elemento massimale.

(4) Per ogni successione infinita ascendente $M_0 \subset M_1 \subset M_2 \subset \ldots$ di sottomoduli di M esiste k tale che $M_i = M_k$ per ogni $i \geq k$.

(5) Per ogni successione infinita ascendente $M_0 \subset M_1 \subset M_2 \subset \ldots$ di sottomoduli finitamente generati di M esiste k tale che $M_i = M_k$ per ogni $i \geq k$.

Dimostrazione. (1) $\Longrightarrow$ (2): Consideriamo una catena $\mathcal{C} \neq \emptyset$ di sottomoduli di M. Allora $P := \bigcup\limits_{N \in \mathcal{C}} N$ è un sottomodulo di M. Per ipotesi P è finitamente generato. Perciò esistono $e_1, \ldots, e_k \in P$ tali che $P = Re_1 + Re_2 + \cdots + Re_k$. Siccome $\mathcal{C}$ è una catena, possiamo trovare un $N \in \mathcal{C}$ tale che $e_1, \ldots, e_k \in N$. Ciò implica $P \subset N$. Siccome ovviamente $N \subset P$, abbiamo $P = N \in \mathcal{C}$.

(2) $\Longrightarrow$ (3): Ciò segue dal lemma di Zorn.

(3) $\Longrightarrow$ (4): Chiaro.

(4) $\Longrightarrow$ (5): Chiaro.

(5) $\Longrightarrow$ (1): Sia N un sottomodulo di M. Assumiamo, per assurdo, che N non sia finitamente generato. Scegliamo $e_1 \in N$. Per ipotesi $Re_1 \neq N$, per cui esiste $e_2 \in N \setminus Re_1$. Ovviamente $Re_1 \subsetneqq Re_1 + Re_2$. Per ipotesi $Re_1 + Re_2 \neq N$, per cui esiste $e_3 \in N \setminus (Re_1 + Re_2)$. Ovviamente $Re_1 + Re_2 \subsetneqq Re_1 + Re_2 + Re_3$.

Continuando in questo modo otteniamo una successione infinita ascendente

$$Re_1 \subsetneqq Re_1 + Re_2 \subsetneqq Re_1 + Re_2 + Re_3 \subsetneqq \ldots$$

di sottomoduli finitamente generati di N, in contrasto con l'ipotesi.

Definizione 3.4. R si dice

(1) *noetheriano a sinistra*, se è noetheriano come R-modulo;

(2) *noetheriano a destra*, se è noetheriano come R-modulo destro;

(3) *noetheriano*, se è noetheriano a sinistra e a destra.

Osservazione 3.5. Siano $\varphi : M \longrightarrow N$ un omomorfismo di R-moduli e Q un sottomodulo di N. Allora:

(1) $\varphi^{-1}(Q)$ è un sottomodulo di M.

(2) Se φ è suriettivo, allora $Q = \varphi\varphi^{-1}(Q)$.

Osservazione 3.6. M sia noetheriano ed N un sottomodulo di M. Allora anche N è noetheriano.

<u>Dimostrazione.</u> Ciò è chiaro, perché ogni sottomodulo di N è anche sottomodulo di M.

Osservazione 3.7. M sia noetheriano e $\varphi : M \longrightarrow N$ un omomorfismo suriettivo di R-moduli. Allora anche N è noetheriano.

<u>Dimostrazione.</u> Sia Q un sottomodulo di N. Per l'oss. 3.5 $\varphi^{-1}(Q)$ è un sottomodulo di M con $Q = \varphi\varphi^{-1}(Q)$. Per ipotesi esistono $e_1, \ldots, e_k \in M$ tali che $\varphi^{-1}(Q) = Re_1 + \cdots + Re_k$. È chiaro che allora

$$Q = R\varphi(e_1) + \cdots + R\varphi(e_k)$$

cioè Q è finitamente generato da $\varphi(e_1), \ldots, \varphi(e_k)$.

Osservazione 3.8 (legge modulare). Siano A, B, C sottomoduli di M tali che $A \subset B$. Allora

$$B \cap (A + C) = A + (B \cap C)$$

<u>Dimostrazione.</u> Scarpone, cor. 2.10.

Proposizione 3.9. *Sia N un sottomodulo di M. Allora sono equivalenti:*

(1) M è noetheriano.

(2) N e M/N sono noetheriani.

<u>Dimostrazione.</u> (1) $\Longrightarrow$ (2): Oss. 3.6 e 3.7.

(2) $\Longrightarrow$ (1): Sia $M_0 \subset M_1 \subset M_2 \subset \ldots$ una successione ascendente infinita di sottomoduli di M. Allora abbiamo due successioni ascendenti

$$M_0 \cap N \subset M_1 \cap N \subset M_2 \cap N \subset \ldots$$

$$(M_0 + N)/N \subset (M_1 + N)/N \subset (M_2 + N)/N \subset \ldots$$

di sottomoduli rispettivamente di N e di M/N. Per ipotesi esiste k tale che per ogni $i \geq k$ si ha $M_i \cap N = M_k \cap N$ e $(M_i + N)/N = (M_k + N)/N$ e quindi $M_i + N = M_k + N$.

Per ogni $i \geq k$ allora $M_k \subset M_i$, pertanto dall'oss. 3.8 otteniamo

$$\begin{aligned} M_i &= M_i + (M_i \cap N) = M_i + (M_k \cap N) \\ &= M_k \cap (M_i + N) = M_k \cap (M_k + N) = M_k \end{aligned}$$

Corollario 3.10. *Sia I un ideale di R. Se R è noetheriano a sinistra o a destra, anche R/I è noetheriano a sinistra, rispettivamente a destra.*

Corollario 3.11. *M ed N siano R-moduli noetheriani. Allora $M \oplus N$ è noetheriano.*

<u>Dimostrazione.</u> Possiamo considerare M come sottomodulo di $M \oplus N$. Allora $(M \oplus N)/M \cong N$, cosicché l'enunciato segue dalla prop. 3.9.

Nota 3.12. Siano X un insieme ed $f : X \longrightarrow M$ un'applicazione qualsiasi. Allora esiste un unico omomorfismo di R-moduli
$\varphi : R^{\underline{X}} \longrightarrow M$ tale che $\varphi(\delta_x) = f(x)$ per ogni $x \in X$.

Qui abbiamo posto $\delta_x := \bigcirc_y (x = y) : X \longrightarrow R$.

Dimostrazione. Chiaro.

Lemma 3.13. *Esistono un R-modulo libero L e un omomorfismo suriettivo $L \longrightarrow M$.*

Se M è finitamente generato, anche L può essere scelto in modo che L sia finitamente generato.

Dimostrazione. Sia E un sistema di generatori per M. Consideriamo l'inclusione $i : E \longrightarrow M$. Allora per la nota 3.12 esiste un omomorfismo di r-moduli $\varphi : R^{\underline{E}} \longrightarrow M$ tale che $\varphi(\delta_e) = i(e) = e$ per ogni $e \in E$.

Se M è finitamente generato, possiamo scegliere E finito.

Proposizione 3.14. *R sia noetheriano a sinistra ed M finitamente generato. Allora M è noetheriano.*

Dimostrazione. Per il lemma 3.13 esiste un omomorfismo suriettivo di R-moduli $R^n \longrightarrow M$. Per il cor. 3.11 R^n è noetheriano. L'enunciato segue dall'oss. 3.7.

Osservazione 3.15. Siano A un anello e $\rho : A \longrightarrow R$ un omomorfismo di anelli. Allora M è anche un A-modulo se per $a \in A$ e $v \in M$ poniamo $av := \rho(a)v$.

In particolare R stesso è un A-modulo.

Proposizione 3.16. *Siano A un anello e $\rho : A \longrightarrow R$ un omomorfismo di anelli. A sia noetheriano a sinistra ed M sia finitamente generato come A-modulo. Allora M è noetheriano come R-modulo.*

Dimostrazione. Sia N un sottomodulo di M. Per la prop. 3.14 M è noetheriano come A-modulo. Perciò esistono $\alpha_1, \ldots, \alpha_k \in N$ tali che $N = A\alpha_1 + \cdots + A\alpha_k$. Siccome N è anche un R-modulo, abbiamo
$N = A\alpha_1 + \cdots + A\alpha_k \subset R\alpha_1 + \cdots + R\alpha_k \subset N$.

Corollario 3.17. *Siano A un anello e $\rho : A \longrightarrow R$ un omomorfismo di anelli. A sia noetheriano a sinistra ed R sia finitamente generato come A-modulo. Allora R è un anello noetheriano a sinistra.*

Corollario 3.18. *Siano A un anello commutativo e $\rho : A \longrightarrow R$ un omomorfismo di anelli. A sia noetheriano ed R sia finitamente generato come A-modulo. Allora R è un anello noetheriano.*

Esempio 3.19. $\mathbb{H}_{\mathbb{Z}}$ è un anello noetheriano.

Dimostrazione. $\mathbb{H}_{\mathbb{Z}} := \mathbb{Z} + i\mathbb{Z} + j\mathbb{Z} + k\mathbb{Z}$, cosicché siamo nella situazione del cor. 3.18. Cfr. def. 2.16.

Nota 3.20. Sia $n \in \mathbb{N} + 1$. Allora R^n_n è generato come R-modulo dalle matrici $\delta_i \delta^j$ con $i, j = 1, \ldots, n$.

Se perciò R è noetheriano a sinistra, dalla prop. 3.14 segue che R_n^n è un R-modulo noetheriano.

Osservazione 3.21. Siano $n \in \mathbb{N}+1$ ed S un sottoanello di R_n^n. Allora sono equivalenti:

(1) S è un R-sottomodulo di R_n^n.

(2) $a\delta \in S$ per ogni $a \in R$.

(3) Ogni S-sottomodulo di S è un R-sottomodulo di R_n^n.

Dimostrazione. (1) $\Longrightarrow$ (2): Per ipotesi $1_{R_n^n} = \delta \in S$. D'altra parte S è un R-sottomodulo di R_n^n, quindi per ogni $a \in R$ si ha che $a\delta \in S$.

(2) $\Longrightarrow$ (3): Siano I un S-sottomodulo di S ed $A \in I$. Per ogni $a \in R$ allora $a\delta \in S$ e quindi $aA = (a\delta)A \in I$.

(3) $\Longrightarrow$ (1): Chiaro.

Proposizione 3.22. *R sia noetheriano a sinistra, $n \in \mathbb{N}+1$ ed S un sottoanello di R_n^n tale che $a\delta \in S$ per ogni $a \in R$.*

Allora S è un anello noetheriano a sinistra.

Dimostrazione. Per la nota 3.20 R_n^n è un R-modulo noetheriano. Sia I un ideale sinistro di S. Per l'oss. 3.21 I è un R-sottomodulo di R_n^n. Perciò esistono $A_1, \ldots A_k \in I$ tali che $I = RA_1 + RA_2 + \cdots + RA_k$. Per ogni $B \in I$ abbiamo allora $B = a_1A_1 + \ldots a_kA_k$ con $a_1, \ldots, a_k \in R$. Ma per ipotesi ciò significa $B = (a_1\delta)A_1 + \ldots (a_k\delta)A_k \in SA_1 + \cdots + SA_k$.

Corollario 3.23. *R sia noetheriano a sinistra ed $n \in \mathbb{N}+1$. Allora R_n^n è un anello noetheriano a sinistra.*

Lemma 3.24. *R sia noetheriano a sinistra e $\varphi : R \longrightarrow S$ un omomorfismo suriettivo di anelli. Allora anche S è noetheriano a sinistra.*

Dimostrazione. Ciò non segue direttamente dall'oss. 3.7, perché φ non è un omomorfismo di moduli, ma di anelli. Possiamo però usare essenzialmente la stessa dimostrazione.

Sia J un ideale di S. Allora, per il punto (1) del lemma 2.30, $\varphi^{-1}(J)$ è un ideale di R. Per ipotesi esistono $e_1, \ldots, e_k \in R$ tali che $\varphi^{-1}(J) = Re_1 + \cdots + Re_k$. Allora J è generato da $\varphi(e_1), \ldots, \varphi(e_k)$. Sia infatti $b \in J$. Allora esiste $x \in R$ con $b = \varphi(x)$. Perciò $x \in \varphi^{-1}(J)$, cosicché $x = a_1e_1 + \cdots + a_ke_k$ per $a_1, \ldots, a_k \in R$. Ciò implica $b = \varphi(x) = \varphi(a_1)\varphi(e_1) + \cdots + \varphi(a_k)\varphi(e_k)$.

Definizione 3.25. Siano A e B anelli. Un *(A,B)-bimodulo* è un gruppo abeliano X che (con l'addizione data) è un A-modulo sinistro e un B-modulo destro in modo che per $a \in A, x \in X, b \in B$ si abbia sempre $(ax)b = a(xb)$.

Definizione 3.26. Siano A, B anelli ed X un (A, B)-bimodulo. Con $\begin{pmatrix} A & X \\ 0 & B \end{pmatrix}$ denotiamo allora l'insieme delle matrici $\begin{pmatrix} a & x \\ 0 & b \end{pmatrix}$ con $a \in A$, $x \in X, b \in B$, dotato della naturale addizione e con la moltiplicazione definita da

$$\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} \begin{pmatrix} c & y \\ 0 & d \end{pmatrix} := \begin{pmatrix} ac & ay + xd \\ 0 & bd \end{pmatrix}$$

Si verifica immediatamente che $\begin{pmatrix} A & X \\ 0 & B \end{pmatrix}$ è un anello con elemento neutro $\begin{pmatrix} 1_A & 0 \\ 0 & 1_B \end{pmatrix}$.

In questa situazione diremo che $\begin{pmatrix} A & X \\ 0 & B \end{pmatrix}$ è un ∇-*anello*.

Osservazione 3.27. Sia $R = \begin{pmatrix} A & X \\ 0 & B \end{pmatrix}$ un ∇-anello. Allora:

(1) Le proiezioni naturali $R \longrightarrow A$ e $R \longrightarrow B$ sono omomorfismi di anelli.

(2) $\begin{pmatrix} 0 & X \\ 0 & 0 \end{pmatrix}$ è un ideale di R.

Dimostrazione. (1) Chiaro.

(2) X è abeliano quindi la somma non presenta problemi.

Per la moltiplicazione definita nella def. 3.26 si ha che

$$\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & y \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & xb \\ 0 & 0 \end{pmatrix} \in \begin{pmatrix} 0 & X \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} a & y \\ 0 & b \end{pmatrix} \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & ax \\ 0 & 0 \end{pmatrix} \in \begin{pmatrix} 0 & X \\ 0 & 0 \end{pmatrix}$$

per ogni $\begin{pmatrix} a & y \\ 0 & b \end{pmatrix} \in R$.

Proposizione 3.28. *Per un ∇-anello $R = \begin{pmatrix} A & X \\ 0 & B \end{pmatrix}$ sono equivalenti:*

(1) R è noetheriano a sinistra.

(2) A e B sono noetheriani a sinistra e X è finitamente generato come A-modulo.

Dimostrazione. Usiamo l'oss. 3.27.

(1) $\Longrightarrow$ (2): Considerando le proiezioni naturali $R \longrightarrow A$ e $R \longrightarrow B$ del lemma 3.24 segue che A e B sono noetheriani a sinistra.

Inoltre $\begin{pmatrix} 0 & X \\ 0 & 0 \end{pmatrix}$ è un ideale e quindi anche un ideale sinistro di R. Ciò implica che esistono $x_1, \ldots, x_m \in X$ tali che

$$\begin{pmatrix} 0 & X \\ 0 & 0 \end{pmatrix} = R \begin{pmatrix} 0 & x_1 \\ 0 & 0 \end{pmatrix} + \cdots + R \begin{pmatrix} 0 & x_m \\ 0 & 0 \end{pmatrix}$$

Se allora $x \in X$, possiamo scrivere

$$\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \xi_1 \\ 0 & \beta_1 \end{pmatrix} \begin{pmatrix} 0 & x_1 \\ 0 & 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 & x_m \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha_m & \xi_m \\ 0 & \beta_m \end{pmatrix}$$

per cui $x = \alpha_1 x_1 + \cdots + \alpha_m x_m$ e ciò mostra che $X = Ax_1 + \cdots + Ax_m$.

(2) $\Longrightarrow$ (1): Dall'isomorfismo naturale $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \cong A \times B$ vediamo che $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ è noetheriano a sinistra. Per ipotesi esistono $x_1, \ldots, x_m \in X$ tali che $X = Ax_1 + \cdots + Ax_m$.

Siano $a \in A, b \in B, x \in X$. Allora esistono $\alpha_1, \ldots, \alpha_m \in A$ con $x = \alpha_1 x_1 + \cdots + \alpha_m x_m$, per cui

$$\begin{pmatrix} a & x \\ 0 & b \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} \alpha_1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & x_1 \\ 0 & 0 \end{pmatrix} + \cdots + \begin{pmatrix} \alpha_m & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & x_m \\ 0 & 0 \end{pmatrix}$$

e vediamo che $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & x_1 \\ 0 & 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 & x_m \\ 0 & 0 \end{pmatrix}$ generano R come modulo su $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$. Dal cor. 3.17 segue che R è noetheriano a sinistra.

Proposizione 3.29. *Per un ∇-anello $R = \begin{pmatrix} A & X \\ 0 & B \end{pmatrix}$ sono equivalenti:*

(1) R è noetheriano a destra.

(2) A e B sono noetheriani a destra e X è finitamente generato come B-modulo destro.

<u>Dimostrazione.</u> Come prop. 3.28.

Esempio 3.30. Il ∇-anello $R := \begin{pmatrix} \mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix}$ è noetheriano a destra, ma non a sinistra.

<u>Dimostrazione.</u> $\mathbb{Z}$ e $\mathbb{Q}$ sono anelli noetheriani e $\mathbb{Q}$ è naturalmente finitamente generato come $\mathbb{Q}$-modulo. Invece $\mathbb{Q}$ non è finitamente generato come $\mathbb{Z}$-modulo. Siano infatti $\alpha_1 = \dfrac{a_1}{b_1}, \ldots, \alpha_m = \dfrac{a_m}{b_m}$ con $a_j, b_j \in \mathbb{Z}$ e $b_j \neq 0$ per ogni j. Allora $\mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_m \subset \dfrac{1}{b_1 \cdots b_m}\mathbb{Z} \subsetneqq \mathbb{Q}$. Pertanto, dalle prop. 3.28 e 3.29, segue direttamente l'enunciato.

Lemma 3.31. *Sia M noetheriano e per ogni $i, j \in \mathbb{N}$ sia dato un sottomodulo M_j^i di M in modo tale che nello schema*

$$\begin{array}{ccccc} M_0^0 & M_1^0 & M_2^0 & M_3^0 & \ldots \\ M_0^1 & M_1^1 & M_2^1 & M_3^1 & \ldots \\ M_0^2 & M_1^2 & M_2^2 & M_3^2 & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots \end{array}$$

ogni riga sia ascendente così come ogni colonna.

Allora esiste $\alpha \in \mathbb{N}$ tale che:

(1) $M_j^i = M_\alpha^i$ per ogni $j \geq \alpha$, per ogni $i \in \mathbb{N}$.

(2) $M_j^i = M_j^\alpha$ per ogni $i \geq \alpha$, per ogni $j \in \mathbb{N}$.

<u>Dimostrazione.</u> Siccome M è noetheriano a sinistra, l'insieme $\{M_k^k \mid k \in \mathbb{N}\}$ contiene un elemento massimale che nel nostro caso evidentemente è anche un massimo, ad esempio M_m^m.

Per $i, j \geq m$ e $t := \max(i, j)$ allora $M_m^m \subset M_j^i \subset M_t^t \subset M_m^m$ e quindi $M_j^i = M_m^m$. Inoltre per ogni $i \in \{0, \dots, m-1\}$ esiste un λ_i tale che $M_j^i = M_{\lambda_i}^i$ per $j \geq \lambda_i$, e similmente, per ogni $j \in \{0, \dots, m-1\}$ esiste un μ_j tale che $M_j^i = M_j^{\mu_j}$ per $i \geq \mu_j$.

Sia $\alpha := \max\{\lambda_0, \dots, \lambda_{m-1}, \mu_0, \dots, \mu_{m-1}, m\}$.
Per $i < m$ e $j \geq \alpha$ allora $j \geq \alpha \geq \lambda_i$ e quindi $M_j^i = M_{\lambda_i}^i = M_\alpha^i$, per $i \geq m$ e $j \geq \alpha$ allora $j \geq \alpha \geq m$ e quindi $M_j^i = M_m^m = M_\alpha^i$.

Ciò mostra il punto (1) dell'enunciato. Il punto (2) si dimostra allo stesso modo.

Proposizione 3.32. *Sia M noetheriano. Allora per ogni sottoinsieme $Z \subset M$ con $Z \neq \emptyset$ esistono $z_1, \dots, z_k \in Z$ tali che $RZ = R\{z_1, \dots, z_k\}$.*

<u>Dimostrazione.</u> Sia, per assurdo, Z un sottoinsieme non vuoto di M per il quale l'enunciato non sia vero. Scegliamo $z_1 \in Z$ in modo arbitrario e poniamo $Z_1 := \{z_1\}$, $N_1 := RZ_1$. Per ipotesi $N_1 \subsetneqq RZ$, quindi $Z \not\subset Z_1$, cosicché possiamo scegliere un elemento $z_2 \in Z \setminus Z_1$; poniamo ora $Z_2 := \{z_1, z_2\} = Z_1 \cup \{z_2\}$ e $N_2 := RZ_2$. Di nuovo troviamo $z_3 \in Z \setminus Z_2$ e possiamo porre $N_3 := RZ_3$ e $Z_3 := Z_2 \cup \{z_3\}$.

Continuando in questo modo otteniamo una catena ascendente infinita $N_1 \subsetneqq N_2 \subsetneqq N_3 \subsetneqq \dots$ di sottomoduli di M, in contraddizione con il punto (4) della prop. 3.3.

4. Il teorema della base di Hilbert

Situazione 4.1. Sia A un anello commutativo.

Definizione 4.2. Per un polinomio $f = a_0x^n + a_1x^{n-1} + \cdots + a_n \in A[x]$ con $a_0 \neq 0$ poniamo

$\operatorname{grad} f := n$ (*grado* di f)

$f[x^i] := a_{n-i}$ per ogni $i = 0, \ldots, n$

$f[x^i] := 0$ per ogni $i > n$

$f\odot := a_0$

Per il polinomio 0 poniamo

$\operatorname{grad} 0 := -\infty$

$0[x^i] := 0$ per ogni $i \in \mathbb{N}$

$0\odot := 0$

Per ogni $f \in A[x]$ l'elemento $f\odot \in A$ si chiama il *coefficiente direttore* di f. Per $n \in \mathbb{N}$ denotiamo con $A[x]_n$ l'insieme dei polinomi di grado n in $A[x]$ insieme al polinomio 0. Quindi $0 \in A[x]_n$ per ogni n.

Osservazione 4.3. Se $A[x]$ è noetheriano, allora anche A è noetheriano.

Dimostrazione. Siccome $A \cong A[x]/x$, l'enunciato segue direttamente dal lemma 3.24.

Definizione 4.4. Siano I un ideale di $A[x]$ ed $n \in \mathbb{N}$. Allora poniamo

$I[n] := \{f\odot \mid f \in I \cap A[x]_n\}$

Lemma 4.5. *Siano I un ideale di $A[x]$ ed $n \in \mathbb{N}$. Allora:*

(1) $I[n]$ è un ideale generalizzato di A.

(2) $I[n] \subset I[n+1]$

È inoltre chiaro che per un ideale J di $A[x]$ con $I \subset J$ si ha $I[n] \subset J[n]$.

Dimostrazione. (1) Osserviamo prima che $0 \in I[n]$, perché $0 \in I \cap A[x]_n$.

Siano $f, g \in I \cap A[x]_n$ ed $a_0 := f\odot \in A$, $b_0 := g\odot \in A$. Se $a_0 + b_0 \neq 0$, allora $f + g \in I \cap A[x]_n$ ed $a_0 + b_0 = (f+g)\odot \in I[n]$. Altrimenti $a_0 + b_0 = 0 \in I[n]$.

Sia $c \in A$. Dobbiamo dimostrare che $ca_0 \in I[n]$. Ciò è chiaro se $c = 0$ oppure $a_0 = 0$. Altrimenti $cf \in I \cap A[x]_n$ e $ca_0 = (cf)\odot \in I[n]$.

(2) Siano ancora $f \in I \cap A[x]_n$ ed $a_0 := f\odot$. Se $a_0 = 0$, allora automaticamente $a_0 \in I[n+1]$. Sia invece $a_0 \neq 0$. Allora $xf \in I \cap A[x]_{n+1}$ ed $a_0 = (xf)\odot \in I[n+1]$.

Teorema 4.6 (teorema della base di Hilbert). *Sia A noetheriano. Allora anche $A[x]$ è noetheriano.*

Dimostrazione. Seguiamo Gabelli, pag 76.

(1) Sia $I_0 \subset I_1 \subset I_2 \subset \dots$ una catena ascendente di ideali di $A[x]$. Per il lemma 4.5 allora otteniamo una tabella di ideali generalizzati di A,

$$\begin{array}{cccc} I_0[0] & I_0[1] & I_0[2] & \dots \\ I_1[0] & I_1[1] & I_1[2] & \dots \\ I_2[0] & I_2[1] & I_2[2] & \dots \\ \dots & \dots & \dots & \dots \end{array}$$

in cui ogni riga è ascendente così come ogni colonna.

Siccome A è noetheriano, per il lemma 3.31 esiste $\alpha \in \mathbb{N}$ tale che $I_j[n] = I_\alpha[n]$ per ogni $n \in \mathbb{N}$ ed ogni $j \geq \alpha$.

(2) Dimostriamo che $I_j = I_\alpha$ per ogni $j \geq \alpha$.

Supponiamo, per assurdo, che per qualche $j \geq \alpha$ si abbia $I_\alpha \subsetneqq I_j$. Sia $f = a_0x^n + a_1x^{n-1} + \dots + a_n$ un polinomio di grado minimo in $I_j \setminus I_\alpha$. Siccome $0 \in I_\alpha$, necessariamente $a_0 \neq 0$. Poiché $a_0 \in I_j[n] = I_\alpha[n]$, esiste un polinomio $g \in I_\alpha \cap A[x]_n$ con $g\odot = a_0$. Allora però $f - g \in I_j \setminus I_\alpha$ possiede grado minore di n, e ciò contraddice la minimalità di n.

Definizione 4.7. Siano B un anello commutativo e $\varphi : A \longrightarrow B$ un omomorfismo di anelli. Allora B si dice un'*algebra commutativa su* A con *omomorfismo di struttura* φ.

Osservazione 4.8. Nella situazione della def. 4.7 φ sarà spesso sottointeso. Da un polinomio $f \in A[x_1, \dots, x_n]$ si ottiene un polinomio $f_\varphi \in B[x_1, \dots, x_n]$ sostituendo ogni coefficiente di f con la sua immagine sotto φ. Per $\alpha_1, \dots, \alpha_n \in B$ è perciò definito

$$f(\alpha_1, \dots, \alpha_n) := f_\varphi(\alpha_1, \dots, \alpha_n) \in B.$$

Definizione 4.9. Siano B un anello commutativo e $\varphi : A \longrightarrow B$ un omomorfismo di anelli. Per $\alpha_1, \dots, \alpha_n \in B$ poniamo

$$A[\alpha_1, \dots, \alpha_n] := \{f(\alpha_1, \dots, \alpha_n) \mid f \in A[x_1, \dots, x_n]\}$$

È immediata la verifica che $A[\alpha_1, \dots, \alpha_n]$ coincide con il più piccolo sottoanello di B che contiene sia $\varphi(A)$ che l'insieme $\{\alpha_1, \dots, \alpha_n\}$.
B si chiama un'*algebra finitamente generata su* A se esistono $\alpha_1, \dots, \alpha_n \in B$ tali che $B = A[\alpha_1, \dots, \alpha_n]$.

Lemma 4.10. *Un anello commutativo B è un'algebra finitamente generata se e solo se esistono $n \in \mathbb{N} + 1$ e un omomorfismo suriettivo di anelli $\theta : A[x_1, \dots, x_n] \longrightarrow B$.*

In tal caso $B = A[\theta(x_1), \dots, \theta(x_n)]$.

Dimostrazione. (1) Siano $\varphi : A \longrightarrow B$ un omomorfismo di anelli ed $\alpha_1, \dots, \alpha_n \in B$ tali che $B = A[\alpha_1, \dots, \alpha_n]$. Allora otteniamo un omomorfismo suriettivo di anelli $\theta : A[x_1, \dots, x_n] \longrightarrow B$ ponendo $\theta(f) := f(\alpha_1, \dots, \alpha_n)$ per ogni $f \in A[x_1, \dots, x_n]$. In particolare si ha $\theta(x_i) = \alpha_i$ per ogni i.

(2) Sia viceversa dato un omomorfismo suriettivo di anelli $\theta : A[x_1, \dots, x_n] \longrightarrow B$. Allora possiamo definire un omomorfismo di anelli $\varphi : A \longrightarrow B$ semplicemente ponendo $\varphi := \theta_{|A}$. È chiaro che

allora con $\alpha_i := \theta(x_i)$ per $i = 1, \dots, n$ si ha $\theta(f) = f(\alpha_1, \dots, \alpha_n)$ per ogni $f \in A[x_1, \dots, x_n]$ e quindi $B = A[\alpha_1, \dots, \alpha_n]$.

Corollario 4.11. *Siano A noetheriano e B un'algebra finitamente generata su A. Allora l'anello B è noetheriano.*

Dimostrazione. Per il lemma 4.10 esistono $n \in \mathbb{N} + 1$ e un omomorfismo suriettivo di anelli $\theta : A[x_1, \dots, x_n] \longrightarrow B$. Per il teorema 4.6 $A[x_1, \dots, x_n]$ è noetheriano, cosicché l'enunciato segue dal lemma 3.24.

Nota 4.12. Seguendo Fieseler/Kaup, pag. 3, diamo una seconda dimostrazione del teorema 4.6.

Dimostrazione. (1) Sia I un ideale di $A[x]$. Per ogni $k \in \mathbb{N}$ esiste allora un sistema di generatori $\{e_{k1}, \dots, e_{km_k}\}$ dell'ideale generalizzato $I[k]$. Per definizione gli e_{kj} sono della forma $e_{kj} = f_{kj}\odot$ con $f_{kj} \in I \cap A[x]_k$. Usando ancora l'ipotesi che A sia noetheriano, vediamo che esiste $\alpha \in \mathbb{N}$ tale che $I[k] = I[\alpha]$ per ogni $k \geq \alpha$.

Sia $J := A[x]\{f_{kj} \mid k \in \{0, \dots, \alpha\}, j \in \{1, \dots, m_k\}\}$. Per costruzione J è finitamente generato ed è chiaro che $J \subset I$. È perciò sufficiente dimostrare che $I \subset J$.

(2) Sia $g \in I$. Dimostriamo, per induzione sul grado n di g, che $g \in J$. I casi $n = 0, 1$ sono banali.

$n-1 \implies n$: Sia $t := \min(n, \alpha)$. Allora $g\odot \in I[n] = I[t] = A\{e_{t1}, \dots, e_{tm_t}\}$ e quindi $g\odot = c_1 e_{t1} + \dots + c_{m_t} e_{tm_t}$ con $c_1, \dots, c_{m_t} \in A$. Ciò implica però che $h := g - x^{n-t} \sum\limits_{k=1}^{m_t} c_k f_{tk} \in I$ possiede grado $< n$. Inoltre allora $h \in I + J \subset I$ e quindi per l'ipotesi di induzione $h \in J$. Ma allora $g \in I + J = J$.

Nota 4.13. La dimostrazione probabilmente più breve del teorema 4.6 è stata data nel 1976 da Heidrun Sarges e si trova anche in Kunz, pag. 11, che seguiamo:

Dimostrazione. Sia I un ideale non finitamente generato di $A[x]$. Allora $I \neq 0$ e per ipotesi esiste $f_1 \in I \setminus 0$ che scegliamo di grado minimo. Similmente, usando l'ipotesi che I non sia finitamente generato, troviamo una successione infinita di polinomi $f_k \in I \setminus A[x]\{f_1, \dots, f_{k-1}\}$, ogni volta di grado minimo. Per ogni k siano $n_k := \operatorname{grad} f_k$ e $a_k := f_k\odot$.

Siccome A è noetheriano, esiste $\alpha \in \mathbb{N}$ tale che $a_{\alpha+1} = c_1 a_1 + \dots + c_\alpha a_\alpha$ con $c_1, \dots, c_\alpha \in A$. Poniamo

$$g := f_{\alpha+1} - x^{n_{\alpha+1} - n_1} c_1 f_1 - \dots - x^{n_{\alpha+1} - n_\alpha} c_\alpha f_\alpha$$

Ma il termine di grado massimo di g è $a_{\alpha+1} x^{n_{\alpha+1}} - \sum\limits_{i=1}^{\alpha} c_i a_i x^{n_{\alpha+1}} = 0$, pertanto $\operatorname{grad} g < n_{\alpha+1}$. D'altra parte $g \in I \setminus A[x]\{f_1, \dots, f_\alpha\}$, che contraddice la minimalità del grado di $f_{\alpha+1}$.

Nota 4.14. L'anello $A[x, xy^2, xy^3, \dots] = A + xA[x, y]$ non è noetheriano. Quindi un sottoanello di un anello commutativo noetheriano non è necessariamente noetheriano.

Dimostrazione. Sia $B := A[x, xy^2, xy^3, \dots]$. Per la prop. 3.32 è sufficiente dimostrare che per ogni $k \in \mathbb{N}$ vale $xy^{k+1} \notin B\{x, xy, \dots, xy^k\}$.

Sia infatti $xy^{k+1} = (a_0 + xf_0)x + (a_1 + xf_1)xy + \cdots + (a_k + xf_k)xy^k$ con $a_0, \dots, a_k \in A$ ed $f_0, \dots, f_k \in A[x, y]$. Allora

$$xy^{k+1} = a_0x + a_1xy + \cdots + a_kxy^k + x^2g$$

per qualche $g \in A[x, y]$ e ciò è impossibile.

Lemma 4.15. *Siano I e J ideali di $A[x]$ con $I \subset J$ e tali che $I[n] = J[n]$ per ogni $n \in \mathbb{N}$. Allora $I = J$.*

Dimostrazione. Sia $f \in J$. Dimostriamo che $f \in I$. Ciò è banale per $f = 0$; lo dimostriamo per induzione sul grado n di f assumendo $f \neq 0$.

$n = 0$: In questo caso $f = f\odot \in I[0] = J[0]$ e quindi $f \in I$.

$n - 1 \implies n$: Abbiamo $f\odot \in J[n] = I[n]$, perciò esiste $g \in I$ tale che $g\odot = f\odot$. Ciò implica $f - g \in J$. Però $\mathrm{grad}(f - g) < n$, per cui $f - g \in I$ e vediamo che $f = g + (f - g) \in I + I = I$.

Nota 4.16. Il lemma 4.15 può essere usato per rendere più trasparente il punto (2) della dimostrazione del teorema 4.6.

Infatti, nel punto (1) di quella dimostrazione abbiamo visto che $I_j[n] = I_\alpha[n]$ per ogni $n \in \mathbb{N}$, per ogni $j \geq \alpha$, cosicché dal lemma 4.15 segue $I_j = I_\alpha$ per ogni $j \geq \alpha$.

Questa variante si trova in Malliavin, pag. 124.

5. Ideali primari

Situazione 5.1. Sia A un anello commutativo.

Osservazione 5.2. P sia un ideale primo di A. Allora $\sqrt{P} = P$.

<u>Dimostrazione.</u> P è un ideale primo, perciò è semiprimo. L'enunciato segue dal cor. 2.50.

Proposizione 5.3. *Sia I un ideale di A. Allora*

$\sqrt{I} = \{a \in A \mid \textit{esiste} \quad n \in \mathbb{N} \quad \textit{con} \quad a^n \in I\}$

<u>Dimostrazione.</u> Ciò segue dalla prop. 2.68 applicata all'anello A/I e può essere dimostrato in modo più diretto così:

(1) Sia $a \in \sqrt{I}$. Per l'oss. 2.58 esiste allora $n \in \mathbb{N}$ tale che $a^n \in I$.

(2) Sia $a \in A$ tale che $a^n \in I$ per qualche $n \in \mathbb{N}$.

Per ogni $P \in \operatorname{Spec} A : I$ vale allora $a \in P$ e ciò implica $a \in I$ per il teorema 2.48.

Definizione 5.4. Un ideale Q di A si dice *primario*, se è soddisfatta la seguente condizione:

Se $a, b \in A$ sono tali che $ab \in Q$ ed $a \notin Q$, allora $b \in \sqrt{Q}$.

Osservazione 5.5. Ogni ideale primo di A è primario.

Osservazione 5.6. Un ideale Q di A è primario se e solo se ogni zero-divisore di A/Q è nilpotente.

Osservazione 5.7. R sia un anello non necessariamente commutativo ed I un ideale di R. Allora $\sqrt{\sqrt{I}} = \sqrt{I}$.

<u>Dimostrazione.</u> Dal cor. 2.49 si ha che $\sqrt{I}$ è il più piccolo ideale semiprimo che contiene I. Pertanto $\sqrt{I}$ è semiprimo, da cui segue, per il cor. 2.50, che $\sqrt{I} = \sqrt{\sqrt{I}}$.

Proposizione 5.8. *Sia Q un ideale primario di A. Allora $\sqrt{Q}$ è primo ed è quindi il più piccolo ideale primo che contiene Q.*

<u>Dimostrazione.</u> Siano $a, b \in A$ tali che $ab \in \sqrt{Q}$. Allora esiste $n \in \mathbb{N}+1$ tale che $a^n b^n = (ab)^n \in Q$. Sia $a \notin \sqrt{Q}$. Allora $a^n \notin Q$. Siccome Q è primario, ciò implica $b^n \in \sqrt{Q}$, ovvero $b \in \sqrt{\sqrt{Q}} = \sqrt{Q}$.

Definizione 5.9. L'anello A si dice *locale* se possiede un unico ideale massimale.

Esempio 5.10. (1) Ogni campo è un anello locale.

(2) Siano p un numero primo, $m \in \mathbb{N} + 1$ ed $A = \mathbb{Z}/p^m$. Allora A possiede un unico ideale primo $(p\mathbb{Z}/p^m)$ ed è quindi in particolare locale. A per $m \geq 2$ non è un campo.

Lemma 5.11. *Le seguenti condizioni sono equivalenti:*

(1) A è locale.

(2) L'insieme degli elementi non invertibili di A è un ideale.

(3) La somma di due elementi non invertibili di A non è invertibile.

(4) Se $a, b \in A$ sono tali che $a+b = 1$, allora almeno uno degli elementi a e b è invertibile.

Dimostrazione. (1) $\Longrightarrow$ (2): Sia $\mathfrak{m}$ l'unico ideale massimale di A. Siano a e b elementi non invertibili di A. Allora Aa e Ab sono ideali di A e quindi entrambi contenuti in $\mathfrak{m}$. Ciò implica $a+b \in \mathfrak{m}$ e $ca \in \mathfrak{m}$ per ogni $c \in A$, per cui gli elementi $a + b$ e ca non possono essere invertibili.

(2) $\Longrightarrow$ (3): Chiaro.

(3) $\Longrightarrow$ (4): Chiaro.

(4) $\Longrightarrow$ (1): Sia $\mathfrak{m}$ l'insieme degli elementi non invertibili di A. Per $a, b \in \mathfrak{m}$ l'ipotesi (4) implica allora $a+b \in \mathfrak{m}$. Inoltre è chiaro che $ca \in \mathfrak{m}$ per ogni $c \in A$. Pertanto $\mathfrak{m}$ è un ideale di A.

Sia ora I un ideale di A. Allora gli elementi di I sono tutti non invertibili, e quindi si ha $I \subset \mathfrak{m}$.

Osservazione 5.12. Sia A un anello locale con ideale massimale $\mathfrak{m}$. Allora $k := A/\mathfrak{m}$ è un campo.

Perciò in tal caso si usa spesso la dizione ,,sia $(A, \mathfrak{m})$ un anello locale" oppure ,,sia $(A, \mathfrak{m}, k)$ un anello locale".

Corollario 5.13. *Sia $(A, \mathfrak{m})$ un anello locale. Allora ogni elemento di $A \setminus \mathfrak{m}$ è invertibile.*

Proposizione 5.14. *Sia $(A, \mathfrak{m})$ un anello locale. Allora per ogni $r \in \mathfrak{m}$ l'elemento $1 + r$ è invertibile.*

Dimostrazione. È chiaro che per $r \in \mathfrak{m}$ si ha $1 + r \notin \mathfrak{m}$. L'enunciato segue quindi dal cor. 5.13.

Proposizione 5.15. *Sia $\mathfrak{m}$ un ideale massimale di A tale che $1 + r$ è invertibile per ogni $r \in \mathfrak{m}$. Allora $\mathfrak{m}$ è l'unico ideale massimale di A.*

Dimostrazione. Sia a un elemento non invertibile di A. Dimostriamo che $a \in \mathfrak{m}$. Assumiamo, per assurdo, che $a \notin \mathfrak{m}$. Allora $aA + \mathfrak{m} = A$, per cui esistono $b \in A$ e $r \in \mathfrak{m}$ tali che $ab + r = 1$. Per ipotesi $ab = 1 - r$ è invertibile, e ciò non è possibile.

Lemma 5.16. *Sia Q un ideale di A tale che $\sqrt{Q} \in \operatorname{Max} A$. Allora:*

(1) $\sqrt{Q}$ è l'unico ideale primo che contiene Q.

(2) Q è primario.

Dimostrazione. (1) Ciò segue dal teorema 2.48.

(2) Siano $a, b \in A$ tali che $ab \in Q$ con $b \notin \sqrt{Q}$. Per il punto (1) A/Q è un anello locale con ideale massimale $\sqrt{Q}/Q$ e dal cor. 5.13 segue che b è invertibile in A/Q. Perciò esistono $c \in A$ e $q \in Q$ tali che $1 = bc + q$. Ma allora $a = abc + aq \in Q + Q = Q$.

Lemma 5.17. *Siano I e J ideali di A. Allora*

$$\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$$

In particolare $\sqrt{I^n} = \sqrt{I}$ *per ogni* $n \in \mathbb{N} + 1$.

Dimostrazione. È chiaro che $\sqrt{IJ} \subset \sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J}$.

Sia $a \in \sqrt{I} \cap \sqrt{J}$. Allora esistono $n, m \in \mathbb{N}$ tali che $a^n \in I$ e $a^m \in J$. Ciò implica $a^{n+m} = a^n a^m \in IJ$.

Osservazione 5.18. Siano I un ideale di A e $P \in \operatorname{Spec} A$ tali che $P^n \subset I \subset P$ per qualche $n \in \mathbb{N} + 1$. Allora $\sqrt{I} = P$.

Dimostrazione. Per ipotesi si ha che $\sqrt{P^n} \subset \sqrt{I} \subset \sqrt{P}$. Dal lemma 5.17 segue che $\sqrt{P^n} = \sqrt{P} = P$, per cui $\sqrt{I} = P$.

Corollario 5.19. *Siano Q un ideale di A ed $\mathfrak{m} \in \operatorname{Max} A$ tali che $\mathfrak{m}^n \subset Q \subset \mathfrak{m}$ per qualche $n \in \mathbb{N} + 1$.*

Allora $\sqrt{Q} = \mathfrak{m}$ e quindi Q è primario per il punto (2) del lemma 5.16.

Corollario 5.20. *Sia $\mathfrak{m} \in \operatorname{Max} A$. Allora $\mathfrak{m}^n$ è primario per ogni $n \in \mathbb{N} + 1$.*

Nota 5.21. Siano K un campo e $I := K[x, y]\{x^2, xy\}$. Allora:

(1) I non è un ideale primario.

(2) $P := K[x, y]\{x\}$ è un ideale primo con $P^2 \subset I \subset P$.

(3) Perciò $\sqrt{I} = P$ è primo.

Dimostrazione. Dobbiamo solo dimostrare il punto (1). Ciò è però evidente, perché $xy \in I$ ed $x \notin I$, mentre $y \notin \sqrt{I} = P$.

Osservazione 5.22. Siano K un campo e $A := K[x, y, z]/(xy - z^2)$. Siano $\bar{x}, \bar{y}, \bar{z}$ le classi di x, y, z in A e $P := A\{\bar{x}, \bar{z}\}$. Allora:

(1) P è primo.

(2) P^2 non è primario.

Dimostrazione. (1) $A/P \cong K[y]$ è integro.

(2) $\bar{x}\bar{y} = \bar{z}^2 \in P^2$, ma $\bar{x} \notin P^2$ e $\bar{y} \notin \sqrt{P^2} = P$.

Definizione 5.23. Sia $P \in \operatorname{Spec} A$. Un *ideale P-primario* è un ideale primario il cui radicale coincide con P.

Lemma 5.24. *Siano $P \in \operatorname{Spec} A$ e $Q_1, \ldots, Q_n$ ideali P-primari. Allora anche $Q_1 \cap \cdots \cap Q_n$ è P-primario.*

Dimostrazione. Sia $Q := Q_1 \cap \cdots \cap Q_n$.

(1) Per il lemma 5.17 $\sqrt{Q} = P$.

(2) Siano $a, b \in A$ tali che $ab \in Q$ ed $a \notin Q$. Allora $a \notin Q_i$ per qualche $i \in \{1, \ldots, n\}$, mentre naturalmente $ab \in Q_i$, per cui $b \in \sqrt{Q_i} = P$.

Osservazione 5.25. Siano $P \in \operatorname{Spec} A$ e Q un ideale P-primario. Sia Q_1 un ideale di A con $Q \subset Q_1 \subset P$. Allora anche Q_1 è P-primario.

Dimostrazione. (1) In primo luogo si ha $P = \sqrt{Q} \subset \sqrt{Q_1} \subset \sqrt{P} = P$, per cui $\sqrt{Q_1} = P$.

(2) Siano $a, b \in A$ con $ab \in Q_1$, ma $a \notin Q_1$. Allora $a \notin Q$ e quindi $b \in P$.

Questa osservazione, di cui la dimostrazione è immediata, viene spesso usata.

Osservazione 5.26. Siano B un anello commutativo, $\varphi : A \longrightarrow B$ un omomorfismo di anelli e Q un ideale primario di B. Allora $\varphi^{-1}(Q)$ è un ideale primario di A.

Dimostrazione. (1) $\varphi^{-1}(Q)$ è un ideale per il lemma 2.30.

(2) Siano $a, b \in A$ tali che $ab \in \varphi^{-1}(Q)$ e $a \notin \varphi^{-1}(Q)$.
Allora $\varphi(a)\varphi(b) \in Q$ e $\varphi(a) \notin Q$, per cui esiste $n \in \mathbb{N}$ tale che $\varphi(b^n) = \varphi(b)^n \in Q$, cosicché $b^n \in \varphi^{-1}(Q)$.

Definizione 5.27. Siano I un ideale generalizzato di A ed $F \subset A$ un sottoinsieme qualsiasi. Allora poniamo

$I : F := \{a \in A \mid aF \subset I\}$

È immediato che $I : F$ è un ideale generalizzato che coincide con A se e solo se $F \subset I$. Si noti che sempre $I \subset I : F$.

In particolare $0 : F = F^{\perp}$ (cfr. def. 2.21).

Osservazione 5.28. Siano I un ideale generalizzato di A ed $a \in I$. Allora $I : a = A$.

Lemma 5.29. *Siano $P \in \operatorname{Spec} A$, Q un ideale P-primario ed $a \in A$. Allora:*

(1) Se $a \notin P$, allora $Q : a = Q$.

(2) Se $a \notin Q$, allora $Q : a$ è P-primario.

In quest'ultimo caso quindi $\sqrt{Q : a} = P$.

Dimostrazione. (1) Abbiamo già osservato che $Q \subset Q : a$. Sia $b \in Q : a$, cioè $ab \in Q$ e $b \notin Q$. Allora $a \in \sqrt{Q} = P$, in contrasto con l'ipotesi.

(2a) Sia $b \in Q : a$. Allora $ab \in Q$, mentre $a \notin Q$, per cui $b \in \sqrt{Q} = P$ perché Q è P-primario. Perciò $Q : a \subset P$. Ciò implica $P = \sqrt{Q} \subset \sqrt{Q : a} \subset \sqrt{P} = P$ e quindi $\sqrt{Q : a} = P$.

(2b) Siano $b, c \in A$ tali che $bc \in Q : a$, ma $b \notin Q : a$. Allora $abc \in Q$ ed $ab \notin Q$ e quindi $c \in \sqrt{Q} = P$.

6. Ideali primi minimali

Situazione 6.1. Sia A un anello commutativo.

Definizione 6.2. Un sottomonoide di A è un sottosemigruppo S di $(A, \cdot)$ tale che $1 \in S$. Il sottomonoide si dice *puro*, se $0 \notin S$.

Proposizione 6.3. *Un ideale P di A è primo se e solo se $A \setminus P$ è un sottomonoide (necessariamente puro) di A.*

Dimostrazione. Ciò è immediato, essendo un ideale primo di un anello commutativo automaticamente completamente primo; cfr. def. 2.29. Si noti che sicuramente $1 \in A \setminus P$.

Definizione 6.4. Sia S un sottoinsieme di A. Allora denotiamo con $S^\sharp$ l'insieme degli ideali I di A per i quali $I \cap S = \emptyset$.

In particolare $1^\sharp$ coincide con l'insieme di tutti gli ideali di A.

Osservazione 6.5. Sia S un sottoinsieme di A. Allora sono equivalenti:

(1) $S^\sharp = \emptyset$

(2) $0 \notin S^\sharp$

(3) $0 \in S$

Dimostrazione. (1) $\Longrightarrow$ (2): Chiaro.

(2) $\Longrightarrow$ (3): Sia $0 \notin S^\sharp$. Allora $0 \cap S \neq \emptyset$ e ciò implica $0 \in S$.

(3) $\Longrightarrow$ (1): Sia $0 \in S$. Siccome ogni ideale I di A contiene 0, si ha $I \cap S \neq \emptyset$, ovvero $I \notin S^\sharp$ e vediamo che $S^\sharp = \emptyset$.

Proposizione 6.6. *Siano $a, b \in A$ ed I un ideale di A tali che $ab \in I$, $a \notin I$, $b \notin I$. Allora $Aa + I \neq A$.*

Dimostrazione. Altrimenti esistono $c \in A$ e $x \in I$ tali che $ac + x = 1$. Allora $b = bac + bx \in I + I = I$, una contraddizione.

Proposizione 6.7. *Sia S un sottomonoide di A. Allora:*

(1) Ogni elemento di $S^\sharp$ è contenuto in un elemento massimale di $S^\sharp$ (il quale non sarà un ideale massimale, ma solo massimale tra gli elementi di $S^\sharp$).

(2) Ogni elemento di $S^\sharp$ è un ideale primo.

In particolare vediamo che, se S è puro, allora $S^\sharp$ contiene un ideale primo.

Dimostrazione. Ciò è un caso speciale del lemma 2.44., perché ogni sottomonoide di A è un m-sistema.

Proposizione 6.8. *Sia S un sottomonoide puro massimale di A. Allora $A \setminus S$ è un ideale primo minimale di A.*

Dimostrazione. Per la prop. 6.3 è sufficiente dimostrare che $A \setminus S$ è un ideale di A. Certamente $A \setminus S \neq A$, perché $1 \in S$.

Inoltre $S^\sharp \neq \emptyset$ per l'oss. 6.5. Per la prop. 6.7 esiste perciò un ideale primo di A con $P \in S^\sharp$.

Allora $A \setminus P$ è un sottomonoide puro di A con $S \subset A \setminus P$. Per la massimalità di S ciò implica $S = A \setminus P$ e vediamo che $A \setminus S$ è un ideale (primo) di A.

Lemma 6.9. *Ogni sottomonoide puro di A è contenuto in un sottomonoide puro massimale di A.*

Dimostrazione. Sia $\mathcal{C}$ una catena $\neq \emptyset$ di sottomonoidi puri di A.
È chiaro allora che anche $\bigcup\limits_{S \in \mathcal{C}} S$ è un sottomonoide puro, cosicché l'enunciato segue dal lemma di Zorn.

Proposizione 6.10. *Sia P un ideale primo minimale di A. Allora $A \setminus P$ è un sottomonoide puro massimale di A.*

Dimostrazione. Dalla prop. 6.3 sappiamo che $A \setminus P$ è un sottomonoide puro di A. Per il lemma 6.9 $A \setminus P$ è contenuto in un sottomonoide puro massimale di S.

Allora $A \setminus S \subset P$. Per la prop. 6.8 però $A \setminus S$ è un ideale primo (minimale) e ciò implica $A \setminus S = P$, perché per ipotesi P è minimale.

Corollario 6.11. *Gli ideali primi minimali di A coincidono con i complementi dei sottomonoidi puri massimali di A.*

Proposizione 6.12. *Sia $a \in A$. Allora sono equivalenti:*

(1) a è nilpotente.

(2) a non appartiene a nessun sottomonoide puro di A.

(3) a non appartiene a nessun sottomonoide puro massimale di A.

Dimostrazione. (1) $\Longrightarrow$ (2): Sia $n \in \mathbb{N}$ tale che $a^n = 0$ e sia S un sottomonoide di A con $a \in S$. Allora $0 = a^n \in S$ e quindi S non è puro.

(2) $\Longrightarrow$ (3): Chiaro.

(3) $\Longrightarrow$ (1): a non sia nilpotente. Allora $\{a^n \mid n \in \mathbb{N}\}$ è un sottomonoide puro di A il quale per il lemma 6.9 è contenuto in un sottomonoide puro massimale S a cui quindi a appartiene.

7. Localizzazione

Situazione 7.1. Siano A un anello commutativo ed S un sottomonoide puro di A.

Definizione 7.2. Un ideale H di S si dice *S-saturo*, se vale l'implicazione

$a \in A, s \in S, as \in H \implies a \in H$

Definizione 7.3. $\Omega := \Omega_S := \{a \in A \mid$ esiste $s \in S$ con $as = 0\}$ si chiama l'*ideale di indeterminazione* di S.

Osservazione 7.4. Ω è un ideale S-saturo di A.

Dimostrazione. (1) È chiaro che $0 \in \Omega$ e che $1 \notin \Omega$.

(2) Siano $a, b \in \Omega$, ad esempio $as = 0$ e $bt = 0$ con $s, t \in S$. Siccome S è un sottomonoide di A si ha $st \in S$. Inoltre $ast = 0$ e $bts = 0$ e quindi $(a + b)st = 0$.

(3) Siano $a \in \Omega$ e $b \in A$. Allora ad esempio $as = 0$ per qualche $s \in S$, per cui allora segue che $abs = 0$.

Ciò mostra che Ω è un ideale di A.

(4) Dimostriamo che Ω è S-saturo.

Siano $a \in A, s \in S$ tali che $as \in \Omega$. Allora esiste $r \in S$ tale che $asr = 0$. Ma ciò implica $a \in \Omega$, essendo $sr \in S$.

Definizione 7.5. Sull'insieme $A \times S$ introduciamo la relazione

$(a, s) \sim (b, t) :\iff at - bs \in \Omega$

Lemma 7.6. *La relazione $\sim$ introdotta nell'oss. 7.5 è una relazione di equivalenza su $A \times S$.*

Dimostrazione. (1) Riflessività e simmetria di $\sim$ sono evidenti.

(2) Dimostriamo la transitività: Si abbia $(a, s) \sim (b, t) \sim (c, u)$. Allora $at - bs \in \Omega$ e $bu - ct \in \Omega$, per cui $atu - bsu \in \Omega$ e $bus - cts \in \Omega$, cosicché $(au - cs)t = atu - cts \in \Omega$.

Siccome Ω è S-saturo, ciò implica $au - cs \in \Omega$ e quindi $(a, s) \sim (c, u)$.

Definizione 7.7. $S^{-1}A := (A \times S)/\sim$ si chiama la *localizzazione* di A rispetto al sottomonoide S.

Definizione 7.8. Per $a \in A$ ed $s \in S$ denotiamo con a_S la classe di equivalenza di $(a, 1)$ in $S^{-1}A$, con $\dfrac{a_S}{s}$ la classe di equivalenza di (a, s).

Vedremo che questa notazione è legittima, perché gli elementi di S sono, come dimostreremo, invertibili in $S^{-1}A$.

Osservazione 7.9. La def. 7.5 può essere riformulata così : Per $a, b \in A$ ed $s, t \in S$ si ha

$\dfrac{a_S}{s} = \dfrac{b_S}{t} \iff$ esiste $u \in S$ tale che $(at - bs)u = 0$

Se S non contiene zerodivisori, si ha

$$\frac{a_S}{s} = \frac{b_S}{t} \iff at = bs$$

Osservazione 7.10. Siano $a, b \in A$. Allora

$$a_S = b_S \iff a - b \in \Omega$$

Se S non contiene zerodivisori, allora $a_S = b_S \iff a = b$.

Osservazione 7.11. Sia $a \in A$. Allora $a_S = 0 \iff a \in \Omega$.

Osservazione 7.12. $1_S \neq 0$.

Dimostrazione. Infatti $1 \notin \Omega$.

Osservazione 7.13. Siano $a, b, a', b' \in A$ ed $s, t, s', t' \in S$ tali che

$$\frac{a_S}{s} = \frac{a'_S}{s'} \text{ e } \frac{b_S}{t} = \frac{b'_S}{t'}$$

Allora

$$\frac{(at + bs)_S}{st} = \frac{(a't' + b's')_S}{s't'}$$

$$\frac{(ab)_S}{st} = \frac{(a'b')_S}{s't'}$$

Dimostrazione. (1) Per ipotesi si ha che $as' - a's \in \Omega$ e $bt' - b't \in \Omega$. D'altra parte Ω è un ideale di A, perciò

$$\begin{aligned}(at + bs)s't' - (a't' + b's')st &= as'(tt') + bt'(ss') - a's(tt') - b't(ss') \\ &= (as' - a's)(tt') + (bt' - b't)(ss') \in \Omega\end{aligned}$$

che equivale a dire che $(at + bs, st) \sim (a't' + b's', s't')$, ciò che dovevamo dimostrare.

(2) Similmente

$$\begin{aligned}abs't' - a'b'st &= as'(bt') - a's(bt') + a's(bt') - a's(b't) \\ &= (as' - a's)(bt') + (bt' - b't)(a's) \in \Omega\end{aligned}$$

da cui la tesi.

Osservazione 7.14. Siano $a \in A$ ed $s, t \in S$. Allora $\dfrac{a_S}{s} = \dfrac{(at)_S}{st}$

Proposizione 7.15. *Su $S^{-1}A$ introduciamo le operazioni*

$$\frac{a_S}{s} + \frac{b_S}{t} := \frac{(at + bs)_S}{st}$$

$$\frac{a_S}{s}\frac{b_S}{t} := \frac{(ab)_S}{st}$$

Allora $S^{-1}A$ diventa un anello commutativo in cui 0_S è l'elemento neutro dell'addizione e 1_S è l'elemento neutro della moltiplicazione.

Dimostrazione. (1) Le operazioni sono ben definite per l'oss. 7.13.

(2) Si verifica facilmente che $(S^{-1}A, +)$ è un gruppo abeliano con elemento neutro 0_S e che $(S^{-1}A, \cdot)$ è un monoide commutativo con elemento neutro 1_S.

(3) Dimostriamo la legge di distributività: Usando l'oss. 7.14 per $a, b, c \in A$ ed $s, t, r \in S$ abbiamo

$$\begin{aligned}\frac{a_S}{s}\left(\frac{b_S}{t}+\frac{c_S}{r}\right) &= \frac{a_S}{s}\frac{(br+ct)_S}{tr} = \frac{(abr+act)_S}{str} \\ &= \frac{(abrs+acts)_S}{strs} = \frac{(ab)_S}{st}+\frac{(ac)_S}{rs} \\ &= \frac{a_S}{s}\frac{b_S}{t}+\frac{a_S}{s}\frac{c_S}{r}\end{aligned}$$

Osservazione 7.16. Siano $a, b \in A$. Allora

$(a+b)_S = a_S + b_S$

$(ab)_S = a_S b_S$

Dimostrazione. (1) Infatti

$a_S + b_S = \dfrac{a_S}{1} + \dfrac{b_S}{1} = \dfrac{(a+b)_S}{1} = (a+b)_S$

(2) Similmente

$a_S b_S = \dfrac{a_S}{1}\dfrac{b_S}{1} = \dfrac{(ab)_S}{1} = (ab)_S$

Proposizione 7.17. *L'applicazione $i_S := \bigcirc_a a_S : A \longrightarrow S^{-1}A$ è un omomorfismo di anelli con nucleo Ω.*

Dimostrazione. Ciò segue dalle oss. 7.16 e 7.11 e dalla prop. 7.15.

Corollario 7.18. *Se S non contiene zerodivisori, possiamo considerare A come sottoanello di $S^{-1}A$ tramite l'omomorfismo $i_S : A \longrightarrow S^{-1}A$.*

Osservazione 7.19. Gli elementi di S siano invertibili in A. Allora per ogni $a \in A$ e per ogni $s \in S$ si ha $\dfrac{a_S}{s} = (as^{-1})_S$.

Dimostrazione. $a = as^{-1}s$ implica $\dfrac{a_S}{s} = (as^{-1})_S$.

Osservazione 7.20. L'applicazione $i_S : A \longrightarrow S^{-1}A$ è un isomorfismo se e solo se ogni elemento di S è invertibile.

Dimostrazione. (1) Sia i_S un isomorfismo. Allora $\Omega = \operatorname{Ker} i_S = 0$. Per la suriettività di i_S, dato $s \in S$ deve esistere $e \in A$ tale che $\dfrac{1_S}{s} = e_S$.

Ciò significa che $1 - es \in \Omega = 0$, per cui s è invertibile.

(2) Ogni elemento di S sia invertibile, ciò implica che S non contiene zerodivisori. Dall'oss. 7.9 segue che $\operatorname{Ker} i_S = \Omega = 0$ pertanto i_S è iniettivo.

Sia ora $\dfrac{a_S}{s} \in S^{-1}A$. Dall'oss. 7.19 segue che $\dfrac{a_S}{s} = (as^{-1})_S = i_S(as^{-1})$, e vediamo che i_S è suriettivo.

Definizione 7.21. Per un anello integro A denotiamo con $\mathcal{K}(A)$ il suo campo dei quozienti.

Nel caso che A sia sottoanello di un campo E, spesso identifichiamo $\mathcal{K}(A)$ con il sottocampo $\left\{ \dfrac{a}{b} \mid a \in A, b \in A \setminus 0 \right\}$ di E.

Nota 7.22. A sia un anello integro. Allora l'applicazione

$$\begin{aligned} \varphi : S^{-1}A &\longrightarrow \mathcal{K}(A) \\ \frac{a_S}{s} &\longmapsto \frac{a}{s} \end{aligned}$$

è ben definita e costituisce un omomorfismo di anelli che rende commutativo il diagramma

$$\begin{tikzcd} A \arrow[r, "i_S"] \arrow[dr, "j"'] & S^{-1}A \arrow[d, "\varphi"] \\ & \mathcal{K}(A) \end{tikzcd}$$

in cui j è l'inclusione $\underset{a}{\bigcirc}\, \dfrac{a}{1}$ di A nel suo campo dei quozienti.

Nel caso che A sia integro possiamo quindi identificare $S^{-1}A$ con il sottoanello $\left\{ \dfrac{a}{s} \mid a \in A, s \in S \right\}$ di $\mathcal{K}(A)$.

<u>Dimostrazione.</u> (1) Dimostriamo che φ è ben definito.

Osserviamo che $\Omega = 0$. Sia $\dfrac{a_S}{s} = \dfrac{b_S}{t}$. Allora $at - bs = 0$ e ciò implica che $\dfrac{a}{s} = \dfrac{b}{t}$ in $\mathcal{K}(A)$.

(2) Dimostriamo che φ è iniettivo.

Sia $\dfrac{a_S}{s} = 0$ in $\mathcal{K}(A)$. Ciò implica però $a = 0$ e quindi $\dfrac{a_S}{s} = 0$.

(3) Per $a \in A$ abbiamo $\varphi(i_S(a)) = \varphi(a_S) = \dfrac{a}{1} = j(a)$.

(4) Si verifica facilmente che φ è un omomorfismo di anelli.

Definizione 7.23. Siano f un elemento non nilpotente di A ed $S := \{f^n \mid n \in \mathbb{N}\}$. Allora S è un sottomonoide puro di A.

In questo caso scriviamo A_f per $S^{-1}A$, a_f per a_S e quindi $\dfrac{a_f}{s}$ per $\dfrac{a_S}{s}$.

Nota 7.24. A sia un anello integro, $f \in A \setminus 0$ ed $S := \{f^n \mid n \in \mathbb{N}\}$. Allora il sottoanello $\left\{ \dfrac{a}{s} \mid a \in A, s \in S \right\} = \left\{ \dfrac{a}{f^n} \mid a \in A, n \in \mathbb{N} \right\}$ coincide con il sottoanello $A\left[\dfrac{1}{f}\right]$ di $\mathcal{K}(A)$.

Se A è integro, possiamo quindi identificare A_f con $A\left[\dfrac{1}{f}\right]$, con quest'ultimo anello formato in $\mathcal{K}(A)$.

Esempio 7.25. Sia $b \in \mathbb{Z} \setminus 0$. Per la proposizione 7.24 possiamo identificare $\mathbb{Z}_b$ con il sottoanello $\left\{ \frac{a}{b^k} \mid a \in \mathbb{Z}, k \in \mathbb{N} \right\}$ di $\mathbb{Q}$.

Corollario 7.26. *Siano K un campo ed $f \in K[x_1, \ldots, x_n]$ con $f \neq 0$. Allora $K[x_1, \ldots, x_n]_f$ può essere identificato con il sottoanello $K[x_1, \ldots, x_n, \frac{1}{f}]$ di $K(x_1, \ldots, x_n)$.*

Osservazione 7.27. Per ogni $s \in S$ si ha $s_S \frac{1_S}{s} = 1_S$.

Dimostrazione. Infatti si ha $s_S \frac{1_S}{s} = \frac{s_S}{s}$ ed è chiaro che l'ultima frazione coincide con 1_S (cfr. oss. 7.14).

Teorema 7.28. *Per ogni $s \in S$ l'elemento s_S è invertibile nell'anello $S^{-1}A$ e si ha $(s_S)^{-1} = \frac{1_S}{s}$.*

Dimostrazione. Ciò è una conseguenza immediata dell'oss. 7.27.

Osservazione 7.29. L'oss. 7.27 e il teorema 7.28 giustificano la nostra notazione introdotta nella def. 7.8. Infatti, per $a \in A$ ed $s \in S$, in $S^{-1}A$ si ha

$$\frac{a_S}{s} = \frac{a_S 1_S}{s} = a_S (s_S)^{-1}$$

Lemma 7.30. *Siano f un elemento non nilpotente di A ed $S := \{f^n \mid n \in \mathbb{N}\}$. Definiamo un omomorfismo di anelli $\psi : A[x] \longrightarrow A_f$ ponendo, per $u = a_0 x^n + \cdots + a_n \in A[x]$,*

$$\begin{aligned} \psi(u) := u\left(\frac{1_f}{f}\right) &= \frac{(a_0)_f}{f^n} + \frac{(a_1)_f}{f^{n-1}} + \cdots + (a_n)_f \\ &= \frac{(a_0 + a_1 f + \cdots + a_n f^n)_f}{f^n} \end{aligned}$$

Allora $\operatorname{Ker} \psi = A[x](fx - 1)$.

Dimostrazione. (1) È chiaro che ψ è un omomorfismo di anelli, ad esempio considerando A_f come A-modulo, cosicché ψ diventa semplicemente l'operatore di valutazione di un polinomio in $\frac{1_f}{f}$.

(2) È chiaro anche che $fx - 1 \in \operatorname{Ker} \psi$.

Infatti $\psi(fx - 1) = f \frac{1_f}{f} - 1 = 0_f$.

(3) Sia $u \in \operatorname{Ker} \psi$, dove $u = a_0 x^n + \cdots + a_n$. Dimostriamo prima che esiste un $k \in \mathbb{N}$ tale che $f^k u \in A[x](fx - 1)$. Allora abbiamo $(a_0 + a_1 f + \cdots + a_n f^n)_f = 0$, per cui esiste $m \in \mathbb{N}$ tale che

$$0 = f^m (a_0 + a_1 f + \cdots + a_n f^n) = a_0 f^m + a_1 f^{m+1} + \cdots + a_n f^{m+n} \qquad (*)$$

Allora

$$f^{m+n} u = a_0 f^m f^n x^n + a_1 f^{m+1} f^{n-1} x^{n-1} + \cdots + a_{n-1} f^{m+n-1} fx + a_n f^{m+n}$$

e quindi $f^{m+n}u = v(fx)$ con

$$v := a_0 f^m x^n + a_1 f^{m+1} x^{n-1} + \cdots + a_{n-1} f^{m+n-1} x + a_n f^{m+n} \in A[x]$$

Per la relazione (*) abbiamo $v(1) = 0$, cosicché esiste un polinomio $q \in A[x]$ tale che $v = (x-1)q$. Allora però

$$f^{m+n}u = v(fx) = (fx-1)qf(x) \in A[x](fx-1).$$

(4) Siano $u \in \operatorname{Ker}\psi$ ed $m, n \in \mathbb{N}$ come al punto (3). Con $k := m+n$ abbiamo allora $f^k u \in A[x](fx-1) =: J$. Dobbiamo dimostrare che $u \in J$. Però $1 = fx - (fx-1)$ e con $I := A[x]f$ abbiamo $A = I + J$. Ciò implica (come si vede facilmente) $A = I^k + J$ e siccome $uf^k \in J$ si ha $uI^k \subset J$. Per ipotesi esistono $d \in I^k$ ed $e \in J$ tali che $1 = d + e$. Ciò implica $u = ud + ue \in J + J = J$.

Proposizione 7.31. *L'omomorfismo ψ del teorema 7.30 induce un isomorfismo naturale $A_f \cong A[x]/(fx-1)$.*

Dimostrazione. Siccome $\operatorname{Ker}\psi = A[x](fx-1)$, è sufficiente verificare che ψ è suriettiva. Ma ciò è ovvio, perché per ogni $a \in A$ ed ogni $n \in \mathbb{N}$ abbiamo $\dfrac{a_f}{f^n} = \psi(ax^n)$.

Esempio 7.32. Sia $b \in \mathbb{Z} \setminus 0$. Allora esistono isomorfismi naturali

$$\left\{ \frac{a}{b^k} \mid a \in \mathbb{Z}, k \in \mathbb{N} \right\} \cong \mathbb{Z}_b \cong \mathbb{Z}[x]/(bx-1)$$

Esempio 7.33. Siano K un campo ed $f \in K[x_1, \ldots, x_n] \setminus 0$.
Allora esiste un isomorfismo naturale

$$K[x_1, \ldots, x_n]_f \cong K[x_1, \ldots, x_{n+1}]/(fx_{n+1} - 1)$$

Teorema 7.34. *Siano B un anello commutativo e $\varphi : A \longrightarrow B$ un omomorfismo di anelli tale che ogni elemento di $\varphi(S)$ sia invertibile. Allora esiste un unico omomorfismo di anelli $\overline{\varphi} : S^{-1}A \longrightarrow B$ che rende commutativo il diagramma*

$$\begin{tikzcd} A \arrow[r, "i_S"] \arrow[dr, "\varphi"'] & S^{-1}A \arrow[d, "\bar\varphi"] \\ & B \end{tikzcd}$$

Per $a \in A$ ed $s \in S$ si ha $\overline{\varphi}\left(\dfrac{a_S}{s}\right) = \varphi a(\varphi s)^{-1}$

Dimostrazione. (1) Se $\overline{\varphi}$ esiste, per $a \in A$ ed $s \in S$ dall'uguaglianza $\dfrac{a_S}{s} s_S = a_S$ valida in $S^{-1}A$ dobbiamo avere $\overline{\varphi}\left(\dfrac{a_S}{s}\right) \overline{\varphi} s_S = \overline{\varphi} a_S$ ovvero $\overline{\varphi}\left(\dfrac{a_S}{s}\right) \varphi s = \varphi a$. D'altra parte ogni elemento di $\varphi(S)$ è invertibile in B, pertanto $\overline{\varphi}\left(\dfrac{a_S}{s}\right) = \varphi a(\varphi s)^{-1}$.

(2) Dobbiamo ancora dimostrare che in questo modo $\overline{\varphi}$ è ben definita. Sia $\dfrac{a_S}{s} = \dfrac{b_S}{t}$ con $a, b \in A$ ed $s, t \in S$. Allora esiste $u \in S$ tale che $(at - bs)u = 0$. Ciò implica $\varphi u(\varphi a \varphi t - \varphi b \varphi s) = 0$ e, siccome φu è invertibile, si ha $\varphi a \varphi t = \varphi b \varphi s$. Poiché anche φs e φt sono invertibili si ha $\varphi a(\varphi s)^{-1} = \varphi b(\varphi t)^{-1}$.

(3) È chiaro adesso che $\overline{\varphi}$ è un omomorfismo di anelli.

(4) Per $a \in A$ abbiamo infine $\overline{\varphi} a_S = \overline{\varphi}\left(\dfrac{a_S}{1}\right) = \varphi a(\varphi 1)^{-1} = \varphi a$, cosicché $\overline{\varphi}$ rende commutativo il diagramma.

Definizione 7.35. Per un sottoinsieme $E \subset A$ sia
$S^{-1}E := \left\{\dfrac{e_S}{s} \mid e \in E, s \in S\right\}$

Osservazione 7.36. Nella situazione del teorema 7.34 si ha $\operatorname{Ker}\overline{\varphi} = S^{-1}\operatorname{Ker}\varphi$.

Dimostrazione. Infatti $\varphi a(\varphi s)^{-1} = 0 \iff \varphi a = 0$.

Osservazione 7.37. Per un A-modulo M si può definire $S^{-1}M$ in modo analogo alla def. 7.7 (come faremo nel capitolo 8). Si dimostra facilmente che per un ideale generalizzato I di A questa costruzione è equivalente a quella data nella def. 7.35; cfr. Atiyah/Macdonald, pag. 70, e Reid, pag. 87.

Lemma 7.38. *Sia I un ideale generalizzato di A. Allora:*

(1) $S^{-1}I$ è un ideale generalizzato di $S^{-1}A$.

(2) $S^{-1}I$ è un ideale di $S^{-1}A \iff I \cap S = \emptyset$.

Dimostrazione. (1) Siano $a, b \in I$ ed $s, t \in S$.

Allora $\dfrac{a_S}{s} + \dfrac{b_S}{t} = \dfrac{(at+bs)_S}{st} \in S^{-1}I$.

Inoltre per $c \in A$ ed $s \in S$ si ha $\dfrac{c_S}{r}\dfrac{a_S}{s} = \dfrac{(ca)_S}{rs} \in S^{-1}I$

(2a) Sia $I \cap S \neq \emptyset$, ad esempio $s \in I \cap S$. Allora $1_S = \dfrac{s_S}{s} \in S^{-1}I$.

(2b) Sia $S^{-1}I = S^{-1}A$. Allora esistono $a \in I$ ed $s \in S$ tali che $\dfrac{a_S}{s} = 1_S$. Ciò significa che esiste $u \in S$ con $u(a-s) = 0$ ovvero $us = ua$. Ma allora $us \in S \cap I$.

Definizione 7.39. Per un ideale generalizzato J di $S^{-1}A$ usiamo la notazione

$S^*J := i_S^{-1}(J) = \{a \in A \mid a_S \in J\}$

S^*J si chiama la *contrazione di J ad A.*

Osservazione 7.40. (1) Sia J un ideale di $S^{-1}A$. Allora S^*J è un ideale di A.

(2) Sia $Q \in \operatorname{Spec} S^{-1}A$. Allora $S^*Q \in \operatorname{Spec} A$.

Dimostrazione. Siccome i_S è un omomorfismo di anelli, l'enunciato segue dal lemma 2.30.

Nel punto (2) qui usiamo che un ideale primo in un anello commutativo è completamente primo.

Lemma 7.41. *Sia J un ideale generalizzato di $S^{-1}A$. Allora $S^{-1}S^*J = J$.*

Dimostrazione. (1) Sia $q \in S^{-1}S^*J$. Allora esistono $e \in S^*J$ ed $s \in S$ tali che $q = \dfrac{e_S}{s} = e_S(s_S)^{-1}$. Per ipotesi J è un ideale generalizzato di $S^{-1}A$ ed $e_S \in J$, perciò $q \in J$.

(2) Sia $q \in J$, ad esempio $q = \dfrac{a_S}{s}$ con $a \in A$ ed $s \in S$. Allora $a_S = qs_S \in J$ e quindi $a \in S^*J$. Da ciò segue direttamente che $q \in S^{-1}S^*J$.

Lemma 7.42. *Sia I un ideale generalizzato di A. Allora*
$S^*S^{-1}I = \{a \in A \mid$ *esiste* $s \in S$ *con* $as \in I\}$

Dimostrazione. (1) Sia $a \in S^*S^{-1}I$. Ciò significa $a_S \in S^{-1}I$, perciò esistono $b \in I$ ed $s \in S$ con $a_S = \dfrac{b_S}{s}$, ovvero $sa_S = b_S$. Pertanto esiste $t \in S$ con $tsa = tb \in I$.

(2) Siano $a \in A$ ed $s \in S$ con $as \in I$. Allora $a_S = \dfrac{(as)_S}{s} \in S^{-1}I$ e quindi $a \in S^*S^{-1}I$.

Proposizione 7.43. *Sia $P \in \operatorname{Spec} A$ tale che $P \cap S = \emptyset$.*
Allora $S^{-1}P \in \operatorname{Spec} S^{-1}A$.

Dimostrazione. (1) Dal lemma 7.38 sappiamo che $S^{-1}P$ è un ideale di $S^{-1}A$.

(2) Siano $u, v \in S^{-1}A$ tali che $uv \in S^{-1}P$. Allora esistono $a, b \in A$, $p \in P$ ed $s, t, x \in S$ tali che $u = \dfrac{a_S}{s}$, $v = \dfrac{b_S}{t}$ e $uv = \dfrac{(ab)_S}{st} = \dfrac{p_S}{x}$, cosicché esiste $y \in S$ con $(abx - pst)y = 0$. Ciò significa che $abxy = psty \in P$, cosicché necessariamente $ab \in P$, cioè $a \in P$ oppure $b \in P$. Se ad esempio $a \in P$, allora $u = \dfrac{a_S}{s} \in S^{-1}P$.

Corollario 7.44. *Per un ideale generalizzato I di A sono equivalenti:*

(1) $S^*S^{-1}I = I$.

(2) I è S-saturo.

Dimostrazione. (1) $\Longrightarrow$ (2): Per il lemma 7.42
$I = \{a \in A \mid$ esiste $s \in S$ con $as \in I\}$, quindi la tesi segue direttamente dalla def. 7.2.

(2) $\Longrightarrow$ (1): Sia $a \in S^*S^{-1}I$. Allora esiste $s \in S$ tale che $as \in I$ e, poiché I è S-saturo, $a \in I$.

Teorema 7.45. *Esiste una biiezione canonica*

$$\{\textit{ideali generalizzati } S\textit{-saturi di } A\} \longleftrightarrow \{\textit{ideali generalizzati di } S^{-1}A\}$$
$$I \longmapsto S^{-1}I$$
$$S^*J \longleftarrow\!\shortmid\ J$$

Dimostrazione. (1) Per ogni ideale generalizzato J di $S^{-1}A$, S^*J è S-saturo, come si vede dal cor. 7.44: $S^*S^{-1}S^*J \overset{7.41}{=} S^*J$.

(2) Le due applicazioni indicate sono perciò ben definite e una l'inversa dell'altra, come segue dal lemma 7.41 e dal cor. 7.44.

Osservazione 7.46. Siano I un ideale generalizzato di A ed $e_1, \ldots, e_m \in A$ tali che $I = Ae_1 + \cdots + Ae_m$.

Allora $S^{-1}I = (S^{-1}A)(e_1)_S + \cdots + (S^{-1}A)(e_m)_S$.

<u>Dimostrazione.</u> (1) Sia $x \in S^{-1}I$. Allora $x = \dfrac{b_S}{s}$ per qualche $b \in I$ ed $s \in S$. Esistono dunque $a_1, \ldots, a_m \in A$ tali che $b = a_1e_1 + \cdots + a_me_m$. Da ciò segue che

$$\begin{aligned} x &= \frac{(a_1e_1 + \cdots + a_me_m)_S}{s} \\ &= \frac{(a_1e_1)_S}{s} + \cdots + \frac{(a_me_m)_S}{s} \\ &= \frac{(a_1)_S}{s}(e_1)_S + \cdots + \frac{(a_m)_S}{s}(e_m)_S \in (S^{-1}A)(e_1)_S + \cdots + (S^{-1}A)(e_m)_S \end{aligned}$$

(2) Sia $x \in (S^{-1}A)(e_1)_S + \cdots + (S^{-1}A)(e_m)_S$. Allora esistono $a_1, \ldots, a_m \in A$ e $s_1, \ldots, s_m \in S$ tali che

$$\begin{aligned} x &= \frac{(a_1)_S}{s_1}(e_1)_S + \cdots + \frac{(a_m)_S}{s_m}(e_m)_S \\ &= \frac{(a_1s_2 \ldots s_me_1 + \cdots + a_ms_1 \ldots s_{m-1}e_m)_S}{s_1 \ldots s_m} \in S^{-1}I \end{aligned}$$

Corollario 7.47. *Se A è noetheriano, allora anche $S^{-1}A$ è noetheriano.*

Osservazione 7.48. Per un ideale generalizzato I di A sono equivalenti:

(1) $S^*S^{-1}I = A$.

(2) $S^{-1}I = S^{-1}A$.

(3) $I \cap S \neq \emptyset$.

<u>Dimostrazione.</u> (1) $\Longrightarrow$ (2): Infatti, dalla prop. 7.41 abbiamo

$S^{-1}A = S^{-1}S^*S^{-1}I = S^{-1}I$.

(2) $\Longrightarrow$ (1): Nell'ipotesi (2) si ha

$S^*S^{-1}I = S^*S^{-1}A = i_S^{-1}(S^{-1}A) = A$.

(2) $\Longleftrightarrow$ (3): Segue direttamente dalla prop. 7.38.

Osservazione 7.49. Sia $P \in \operatorname{Spec} A \cap S^\sharp$, cioè $P \in \operatorname{Spec} A$ e $P \cap S = \emptyset$. Allora P è S-saturo.

<u>Dimostrazione.</u> Siano $a \in A$ ed $s \in S$ tali che $as \in P$. Poiché $s \notin P$, ciò implica $a \in P$.

Osservazione 7.50. I sia un ideale S-saturo di A. Allora $I \cap S = \emptyset$, cioè $I \in S^\sharp$.

Dimostrazione. Sia $s \in S \cap I$. Allora $s = 1s \in I$ e quindi $1 \in I$, una contraddizione.

Corollario 7.51. *Per $P \in \operatorname{Spec} A$ sono equivalenti:*

(1) P è S-saturo.

(2) $P \in S^\sharp$, cioè $P \cap S = \emptyset$.

Teorema 7.52. *La biiezione del teorema 7.45 induce una biiezione canonica* $\operatorname{Spec} A \cap S^\sharp \longleftrightarrow \operatorname{Spec} S^{-1}A$.

Proposizione 7.53. *Sia anche T un sottomonoide puro di A con $S \subset T$. Allora esiste un unico omomorfismo $i_{S,T} : S^{-1}A \longrightarrow T^{-1}A$ che rende commutativo il diagramma*

$$\begin{tikzcd} A \arrow[r, "i_S"] \arrow[dr, "i_T"'] & S^{-1}A \arrow[d, "i_{S,T}"] \\ & T^{-1}A \end{tikzcd}$$

$i_{S,T}$ è dato da $i_{S,T}\left(\dfrac{a_S}{s}\right) = \dfrac{a_T}{s}$.

Dimostrazione. Applichiamo il teorema 7.34 al caso $B = T^{-1}A$ e $\varphi = i_T$.

Allora $i_{S,T}\left(\dfrac{a_S}{s}\right) = \overline{i_T}\left(\dfrac{a_S}{s}\right) = i_T(a)(i_T(s))^{-1} = a_T\dfrac{1_S}{s} = \dfrac{a_T}{s}$.

Proposizione 7.54. *Sia I un ideale generalizzato di A.*

Allora $\sqrt{S^{-1}I} = S^{-1}\sqrt{I}$.

Dimostrazione. (1) Siano $a \in A$, $s \in S$ ed $n \in \mathbb{N}$ tali che $\left(\dfrac{a_S}{s}\right)^n \in S^{-1}I$. Allora esistono $b \in I$ e $t \in T$ tali che $\left(\dfrac{a_S}{s}\right)^n = \dfrac{b_S}{t}$ e quindi esiste $u \in S$ con $a^n tu = bsu \in I$. Ciò implica $(atu)^n \in I$, per cui $aut \in I$. Dal lemma 7.42 segue $a \in S^*S^{-1}\sqrt{I}$. Ma allora $\dfrac{a_S}{s} \in S^{-1}S^*S^{-1}\sqrt{I} \overset{7.41}{=} S^{-1}\sqrt{I}$.

(2) Sia $q \in S^{-1}\sqrt{I}$. Allora esistono $a \in \sqrt{I}$ ed $s \in S$ tali che $q = \dfrac{a_S}{s}$. Sia ad esempio $a^n \in I$. Allora $q^n = \dfrac{(a^n)_S}{s^n} \in S^{-1}I$, quindi $q \in \sqrt{S^{-1}I}$.

8. Localizzazione di moduli

Situazione 8.1. Siano A un anello commutativo ed S un sottomonoide puro di A.

$M, N, \ldots$ siano A-moduli, quando non indicato diversamente.

Definizione 8.2. Un sottomodulo H di M si chiama un *sottomodulo S-saturo* di M, se vale l'implicazione

$x \in M, s \in S, sx \in H \implies x \in H$

Definizione 8.3. $\Omega_{S,M} := \{x \in M \mid \text{esiste } s \in S \text{ con } sx = 0\}$.

Osservazione 8.4. $\Omega_{S,M}$ è un sottomodulo S-saturo di M.

Dimostrazione. (1) Siano $x, y \in \Omega_{S,M}$. Allora esistono $s, t \in S$ tali che $sx = 0$ e $ty = 0$. Siccome S è un sottomonoide di A, si ha allora $st \in S$. Inoltre $stx = 0$ e $sty = 0$ e quindi $st(x + y) = 0$, perciò $x + y \in \Omega_{S,M}$.

(2) Siano $x \in \Omega_{S,M}$ ed $a \in A$. Allora $sx = 0$ per qualche $s \in S$, per cui $sax = asx = 0$ e vediamo che $\Omega_{S,M}$ è un sottomodulo di M.

(3) Siano $x \in M$ ed $s \in S$ tali che $sx \in \Omega_{S,M}$. Allora esiste $t \in S$ tale che $tsx = 0$, e poiché $ts \in S$ ciò implica $x \in \Omega_{S,M}$.

Definizione 8.5. Sull'insieme $M \times S$ introduciamo la relazione

$(x, s) \sim (y, t) :\iff tx - sy \in \Omega_{S,M}$

Lemma 8.6. *La relazione $\sim$ introdotta nella nota 8.5 è una relazione di equivalenza su $M \times S$.*

Dimostrazione. (1) Riflessività e simmetria di $\sim$ sono evidenti.

(2) Dimostriamo la transitività: Si abbia $(x, s) \sim (y, t) \sim (z, u)$. Allora $tx - sy \in \Omega_{S,M}$ e $uy - tz \in \Omega_{S,M}$, per cui $tux - suy \in \Omega_{S,M}$ e $usy - tsz \in \Omega_{S,M}$. Quindi $t(ux - sz) = tux - tsz \in \Omega_{S,M}$ da cui segue che $ux - sz \in \Omega_{S,M}$ e quindi $(x, s) \sim (z, u)$.

Definizione 8.7. $S^{-1}M := (M \times S)/\sim$ si chiama la *localizzazione* di M rispetto al sottomonoide S. Verificheremo fra poco che nel caso che M sia un ideale di A la nuova definizione è equivalente a quella data nella def. 7.35.

Definizione 8.8. Per $x \in M$ ed $s \in S$ denotiamo con x_S la classe di equivalenza di $(x, 1)$ in $S^{-1}M$, con $\dfrac{x_S}{s}$ la classe di equivalenza di (x, s).

Osservazione 8.9. Siano $x, y \in M$. Allora

$x_S = y_S \iff x - y \in \Omega_{S,M}$

In particolare

$x_S = 0 \iff x \in \Omega_{S,M}$

Osservazione 8.10. Siano $x, y, x', y' \in M$ ed $s, t, s', t' \in S$ tali che

$\dfrac{x_S}{s} = \dfrac{x'_S}{s'}$ e $\dfrac{y_S}{t} = \dfrac{y'_S}{t'}$

Allora

$$\frac{(tx+sy)_S}{st} = \frac{(t'x'+s'y')_S}{s't'}$$

(2) Siano $x, x' \in M$, $a, a' \in A$ ed $s, t, s', t' \in S$ tali che

$\dfrac{x_S}{s} = \dfrac{x'_S}{s'}$ e $\dfrac{a_S}{t} = \dfrac{a'_S}{t'}$

Allora

$$\frac{(ax)_S}{st} = \frac{(a'x')_S}{s't'}$$

Dimostrazione. Ciò segue facilmente dall'oss. 8.9.

Proposizione 8.11. *Su $S^{-1}M$ definiamo le operazioni*

$$\frac{x_S}{s} + \frac{y_S}{t} := \frac{(tx+sy)_S}{st}$$

$$\frac{a_S}{s}\frac{x_S}{t} := \frac{(ax)_S}{st}$$

Allora $S^{-1}M$ diventa un $S^{-1}A$-modulo (e quindi un A-modulo) in cui 0_S è l'elemento neutro dell'addizione.

Dimostrazione. (1) Le operazioni sono ben definite per l'oss. 8.10.

(2) Si verifica facilmente che $(S^{-1}M, +)$ è un gruppo abeliano con elemento neutro 0_S ed è chiaro che $1_S\dfrac{x_S}{s} = \dfrac{x_S}{s}$ per ogni $x \in M, s \in S$.

(3) La distributività si dimostra come nella prop. 7.15.

Osservazione 8.12. Siano $x, y \in M$ ed $a \in A$. Allora

$$(x+y)_S = x_S + y_S$$

$$(ay)_S = a_S y_S$$

Dimostrazione. Segue direttamente dalla prop. 8.11 utilizzando lo stesso procedimento dell'oss. 7.16.

Proposizione 8.13. *L'applicazione $i_{S,M} := \underset{x}{\bigcirc} x_S : M \longrightarrow S^{-1}M$ è un omomorfismo di A-moduli con nucleo $\Omega_{S,M}$.*

Dimostrazione. (1) Dall'oss. 8.12 segue che $i_{S,M}$ è un omomorfismo di gruppi abeliani.

(2) Siano $a \in A$ ed $x \in M$. Allora

$$i_{S,M}(ax) = (ax)_S \overset{8.12}{=} a_S x_S = a x_S = a i_{S,M}(x)$$

(3) Dall'oss. 8.9 abbiamo $\operatorname{Ker} i_{S,M} = \Omega_{S,M}$.

Proposizione 8.14. *Sia $\varphi : M \longrightarrow N$ un omomorfismo di A-moduli. Allora esiste un unico omomorfismo $S^{-1}\varphi$ di $S^{-1}A$-moduli $S^{-1}M \longrightarrow S^{-1}N$ che rende commutativo il diagramma (di A-moduli):*

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "i_{S,M}"'] & N \arrow[d, "i_{S,N}"] \\ S^{-1}M \arrow[r, "S^{-1}\varphi"] & S^{-1}N \end{tikzcd}$$

$S^{-1}\varphi$ è dato da $(S^{-1}\varphi)\dfrac{x_S}{s} = \dfrac{(\varphi x)_S}{s}$.

Dimostrazione. (1) La costruzione del diagramma implica che per $x \in M$ dobbiamo avere $(S^{-1}\varphi)x_S = (\varphi x)_S$. Siccome $S^{-1}\varphi$ deve essere un omomorfismo di $S^{-1}A$-moduli, per $s \in S$ dobbiamo avere

$$(S^{-1}\varphi)\frac{x_S}{s} = \frac{1_S}{s}(S^{-1}\varphi)x_S = \frac{1_S}{s}(\varphi x)_S = \frac{(\varphi x)_S}{s}$$

(2) Dimostriamo che $S^{-1}\varphi$ in questo modo è ben definito.

Siano $\dfrac{x_S}{s} = \dfrac{y_S}{t}$ dove $s, t \in S$ e $x, y \in M$. Allora esiste $u \in S$ tale che $u(tx - sy) = 0$. Ma ciò implica $u(t\varphi x - s\varphi y) = 0$.

(3) È immediato adesso che $S^{-1}\varphi$ è un omomorfismo di $S^{-1}A$-moduli.

Definizione 8.15. Una successione $M_1 \xrightarrow{\varphi} M \xrightarrow{\psi} M_2$ di omomorfismi di moduli su un anello si dice *esatta*, se $\operatorname{Ker}\psi = \operatorname{Im}\varphi$.

Teorema 8.16. *La successione $M_1 \xrightarrow{\varphi} M \xrightarrow{\psi} M_2$ (di A-moduli) sia esatta. Allora anche la successione*

$$S^{-1}M_1 \xrightarrow{S^{-1}\varphi} S^{-1}M \xrightarrow{S^{-1}\psi} S^{-1}M_2$$

di $S^{-1}A$-moduli è esatta.

Dimostrazione. (1) Siano $x \in M_1$ ed $s \in S$. Allora

$$(S^{-1}\psi)(S^{-1}\varphi)\frac{x_S}{s} = (S^{-1}\psi)\frac{(\varphi x)_S}{s} = \frac{(\psi(\varphi x))_S}{s} = \frac{0_S}{s} = 0$$

Perciò $\operatorname{Im}\varphi \subset \operatorname{Ker}\psi$.

(2) Siano $x \in M$ ed $s \in S$ tali che $(S^{-1}\psi)\dfrac{x_S}{s} = 0$. Ciò significa che $\dfrac{(\psi x)_S}{s} = 0$. Pertanto esiste $t \in S$ tale che $0 = t\psi x = \psi tx$. Per ipotesi esiste $y \in M_1$ tale che $tx = \varphi y$. Allora $x_S = \dfrac{(\varphi y)_S}{t}$, per cui

$\dfrac{x_S}{s} = \dfrac{(\varphi y)_S}{st} = (S^{-1}\varphi)\dfrac{y_S}{st}$.

Ciò mostra $\operatorname{Ker}\psi \subset \operatorname{Im}\varphi$.

Corollario 8.17. *$\varphi : M \longrightarrow N$ sia un omomorfismo di A-moduli.*

(1) Se φ è iniettivo, allora anche $S^{-1}\varphi : S^{-1}M \longrightarrow S^{-1}N$ è iniettivo.

(2) Se φ è suriettivo, allora anche $S^{-1}\varphi : S^{-1}M \longrightarrow S^{-1}N$ è suriettivo.

Osservazione 8.18. Siano N un sottomodulo di M ed $i : N \longrightarrow M$ l'inclusione. Per il cor. 8.17 l'omomorfismo $S^{-1}i : S^{-1}N \longrightarrow S^{-1}M$ è iniettivo e ci permette di considerare $S^{-1}N$ come sottomodulo di $S^{-1}M$, come faremo nel seguito.

Nota 8.19. Sia N un sottomodulo di M. Dalla successione esatta

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

otteniamo allora una successione esatta

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

che ci fornisce un isomorfismo $S^{-1}(M/N) \cong (S^{-1}M)/(S^{-1}N)$.

Proposizione 8.20. *Siano N_1 ed N_2 sottomoduli di M. Allora*

(1) $S^{-1}(N_1 + N_2) = S^{-1}N_1 + S^{-1}N_2$.

(2) $S^{-1}(N_1 \cap N_2) = S^{-1}N_1 \cap S^{-1}N_2$.

Dimostrazione. (1) Siano $x \in N_1$, $y \in N_2$ ed $s, t \in S$. Allora $\frac{x_S}{s} + \frac{y_S}{t} = \frac{tx_S + sy_S}{st}$ e ciò mostra che $S^{-1}N_1 + S^{-1}N_2 \subset S^{-1}(N_1 + N_2)$. L'inclusione in senso opposto è ovvia.

(2) Anche qui è sufficiente dimostrare che $S^{-1}N_1 \cap S^{-1}N_2 \subset S^{-1}(N_1 \cap N_2)$:

Siano $x \in N_1$, $y \in N_2$ ed $s, t \in S$ tali che $\frac{x_S}{s} = \frac{y_S}{t}$. Allora esiste $u \in S$ con $utx = usy =: p$. In particolare $p \in N_1 \cap N_2$, quindi $\frac{x_S}{s} = \frac{utx_S}{uts} = \frac{p_S}{uts} \in S^{-1}(N_1 \cap N_2)$.

9. Localizzazione in un ideale primo

Situazione 9.1. Siano A un anello commutativo e $P \in \operatorname{Spec} A$.

Osservazione 9.2. $A \setminus P$ è un sottomonoide puro di A.

Definizione 9.3. Per un A-modulo M poniamo $M_P := (A \setminus P)^{-1}M$ e in particolare $A_P := (A \setminus P)^{-1}A$.

Per $x \in M$ risp. $a \in A$ ed $s \in A \setminus P$ poniamo $x_P := x_{A \setminus P}$ risp. $a_P := a_{A \setminus P}$, $\dfrac{x_P}{s} := \dfrac{x_{A\setminus P}}{s}$, $\dfrac{a_P}{s} := \dfrac{a_{A\setminus P}}{s}$.

Questa notazione è comunemente usata e non ambigua, perché, essendo $0 \in P$, P non è mai un sottomonoide puro di A.

Osservazione 9.4. $PA_P = (A \setminus P)^{-1}P = P_P$.

Lemma 9.5. *Siano $a \in A$ ed $s \in A \setminus P$. Allora sono equivalenti:*

(1) $\dfrac{a_S}{s} \in PA_P$.

(2) $a \in P$.

Dimostrazione. (1) $\Longrightarrow$ (2): Sia $\dfrac{a_S}{s} = \dfrac{b_S}{t}$ con $b \in P$ e $t \in A \setminus P$. Allora esiste $u \in A \setminus P$ tale che $u(at - bs) = 0$ e quindi $atu = bsu \in P$. Poiché $tu \notin P$, allora si ha $a \in P$.

(2) $\Longrightarrow$ (1): Chiaro.

Lemma 9.6. *Siano $a \in A$ ed $s \in A \setminus P$. Allora sono equivalenti:*

(1) $\dfrac{a_S}{s}$ *è invertibile in* A_P.

(2) $a \notin P$.

(3) $\dfrac{a_S}{s} \notin PA_P$.

Dimostrazione. (1) $\Longrightarrow$ (2): Sia $\dfrac{a_S}{s}\dfrac{b_S}{t} = 1_S$ con $b \in A$, $t \in A \setminus P$. Allora esiste $u \in A \setminus P$ tale che $abu = stu \in A \setminus P$. Necessariamente si ha $a \notin P$.

(2) $\Longrightarrow$ (1): Se $a \notin P$, allora $\dfrac{a_S}{s}\dfrac{s_S}{a} = 1_S$ in A_P.

(2) $\Longleftrightarrow$ (3): Segue direttamente dal lemma 9.5.

Teorema 9.7. *A_P è un anello locale con ideale massimale PA_P.*

Dimostrazione. Per il lemma 9.6 l'insieme degli elementi non invertibili di A_P coincide con l'ideale PA_P. Per il lemma 5.11 A_P è un anello locale il cui ideale massimale è uguale a PA_P per il cor. 5.13.

Osservazione 9.8. $(A \setminus P)^\sharp$ è l'insieme degli ideali di A contenuti in P.

Teorema 9.9. *La biiezione del teorema 7.44 induce una biiezione naturale*

$$\{Q \in \operatorname{Spec} A \mid Q \subset P\} \longleftrightarrow \operatorname{Spec} A_P$$
$$Q \longmapsto (A \setminus P)^{-1}Q = QA_P$$

Dimostrazione. Teorema 7.52.

Proposizione 9.10. *P sia un ideale primo minimale. Allora:*

(1) PA_P è l'unico ideale primo di A_P.

(2) Ogni elemento di P è uno zerodivisore.

Dimostrazione. Seguiamo Brüske/Ischebeck/Vogel, pag. 26.

(1) Per il teorema 9.9 PA_P è un ideale primo minimale di A_P e per il teorema 9.7 è anche l'unico ideale massimale. È chiaro che ciò implica che non ci possono essere altri ideali primi di A_P.

(2) Sia $a \in P$. Vogliamo dimostrare che a è uno zerodivisore. Possiamo assumere che $a \neq 0$. Il punto (1) implica che in A_P si ha $\sqrt{0} = PA_P$, perciò per il cor. 2.59 esiste $n \in \mathbb{N} + 1$ tale che $a_P^n = 0$. Scegliamo n in modo minimale, cosicché $a_P^{n-1} \neq 0$. Allora esiste $s \in S = A \setminus P$ tale che $a^n s = 0$. Per ipotesi su n si ha $sa^{n-1} \neq 0$, perché altrimenti si avrebbe $a_P^{n-1} = 0$.

Osservazione 9.11. $A_P/PA_P \cong \mathcal{K}(A/P)$.

Dimostrazione. Ciò è una facile conseguenza della nota 8.19.

Teorema 9.12. *Per un A-modulo sono equivalenti:*

(1) $M = 0$.

(2) $M_P = 0$ per ogni $P \in \operatorname{Spec} A$.

(3) $M_\mathfrak{m} = 0$ per ogni $\mathfrak{m} \in \operatorname{Max} A$.

Dimostrazione. (1) $\Longrightarrow$ (2): Chiaro.

(2) $\Longrightarrow$ (3): Chiaro.

(3) $\Longrightarrow$ (1): Assumiamo, per assurdo, che $M \neq 0$. Sia $x \in M$ con $x \neq 0$. Allora $\operatorname{Ann}(x)$ è un ideale contenuto in un ideale massimale $\mathfrak{m}$. Per ipotesi si ha $\dfrac{x_\mathfrak{m}}{1} = 0$. Ciò significa che esiste $y \in A \setminus \mathfrak{m}$ tale che $xy = 0$, che è una contraddizione perché $\operatorname{Ann}(x) \subset \mathfrak{m}$.

10. Decomposizione primaria

Situazione 10.1. Sia A un anello commutativo.

Seguiamo Atiyah/Macdonald, pagg. 81-87 e 125-127.

Definizione 10.2. Sia I un ideale di A. Una *decomposizione primaria* di I è un insieme *finito* Δ di ideali primari tale che $I = \bigcap\limits_{Q \in \Delta} Q$.

I si dice *decomponibile*, se possiede una decomposizione primaria.

Definizione 10.3. Sia I un ideale di A. Una decomposizione primaria Δ di I si dice *minimale*, se sono soddisfatte le seguenti due condizioni:

(1) Elementi distinti di Δ hanno radicali distinti.

(2) Per ogni $Q \in \Delta$ si ha $\bigcap\limits_{Q' \in \Delta, Q' \neq Q} Q' \not\subset Q$.

Nota 10.4. Sia I un ideale di A. Allora da ogni decomposizione primaria Δ di I si può ottenere una decomposizione primaria minimale essenzialmente equivalente di I nel modo seguente:

(1) Se $Q_1, \ldots, Q_m \in \Delta$ possiedono tutti lo stesso radicale P, allora sostituiamo $Q_1, \ldots, Q_m$ in Δ con $Q_1 \cap \cdots \cap Q_m$. Quest'ultimo ideale è ancora P-primario per il lemma 5.24.

(2) Adesso da Δ (un insieme finito) togliamo successivamente tutti gli elementi superflui, in modo che alla fine sia soddisfatta la condizione (2) della def. 10.3.

Definizione 10.5. Sia Δ un insieme di ideali primari di I. Allora poniamo

$$\sqrt{\Delta} := \{\sqrt{Q} \mid Q \in \Delta\}$$

$\sqrt{\Delta}$ si chiama il *radicale di* Δ. Per la prop. 5.8 si ha $\sqrt{\Delta} \subset \operatorname{Spec} A$.

Osservazione 10.6. Siano $\mathcal{I}$ un insieme di ideali generalizzati di A ed $a \in A$. Allora

$$\left(\bigcap_{I \in \mathcal{I}} I\right) : a = \bigcap_{I \in \mathcal{I}} (I : a) = \bigcap_{I \in \mathcal{I}, a \notin I} (I : a)$$

Lemma 10.7. *Siano I un ideale di A e Δ una decomposizione primaria di I. Sia $a \in A$. Allora:*

(1) $I : a = \bigcap\limits_{Q \in \Delta, a \notin Q} (Q : a)$

(2) $\sqrt{I : a} = \bigcap\limits_{Q \in \Delta, a \notin Q} \sqrt{Q : a} = \bigcap\limits_{Q \in \Delta, a \notin Q} \sqrt{Q}$

(3) Se $Q \in \Delta$ è tale che $a \notin Q$ ed $a \in \bigcap\limits_{Q' \in \Delta, Q' \neq Q} Q'$, allora $I : a = Q : a$ e $\sqrt{I : a} = \sqrt{Q}$.

Dimostrazione. Ciò segue dai lemmi 5.17 e 5.29 e dall'oss. 10.6.

Lemma 10.8. *Siano I un ideale di A e Δ una decomposizione primaria minimale di I.*

Allora per ogni $P \in \sqrt{\Delta}$ esiste $a \in A$ tale che $I : a$ è P-primario.

Dimostrazione. Sia $P \in \sqrt{\Delta}$. Allora esiste $Q \in \Delta$ tale che $P = \sqrt{Q}$. Siccome Δ è minimale si ha $\bigcap\limits_{Q' \in \Delta, Q' \neq Q} Q' \not\subset Q$. Perciò esiste $a \in \bigcap\limits_{Q' \in \Delta, Q' \neq Q} Q' \setminus Q$. Per il lemma 10.7 allora $I : a = Q : a$. Per il lemma 5.29 $I : a$ è P-primario.

Lemma 10.9. *Siano $P \in \operatorname{Spec} A$ ed $I_1, \ldots, I_m$ ideali generalizzati di A.*

(1) Se $I_1 \cap \cdots \cap I_m \subset P$, allora esiste j tale che $I_j \subset P$.

(2) Se $I_1 \cap \cdots \cap I_m = P$, allora esiste j tale che $I_j = P$.

Dimostrazione. (1) Si ha $I_1 I_2 \ldots I_m \subset I_1 \cap \cdots \cap I_m \subset P$, allora, poiché P è primo, esiste j tale che $I_j \subset P$.

(2) Dal punto (1) segue che esiste j tale che $I_j \subset P$. D'altra parte $P \subset I_1 \cap \cdots \cap I_m$ implica $P \subset P_j$.

Teorema 10.10 (teorema di unicità). *Siano I un ideale di A e Δ una decomposizione primaria minimale di I. Allora*

$\sqrt{\Delta} = \{P \in \operatorname{Spec} A \mid$ *esiste* $a \in A$ *con* $P = \sqrt{I : a}\}$

Dimostrazione. (1) Sia $P \in \sqrt{\Delta}$. Per il lemma 10.8 esiste $a \in A$ tale che $I : a$ è P-primario, per cui $P = \sqrt{I : a}$.

(2) Sia $a \in A$ tale che $\sqrt{I : a} =: P$ sia primo. Per il lemma 10.7 abbiamo allora $P = \bigcap\limits_{Q \in \Delta, a \notin Q} \sqrt{Q}$. Per il lemma 10.9 esiste $Q \in \Delta$ tale che $P = \sqrt{Q}$ e quindi $P \in \sqrt{\Delta}$.

Corollario 10.11. *Se un ideale di A possiede una decomposizione primaria, allora i radicali di tutte le sue decomposizioni primarie minimali coincidono.*

Esempio 10.12. Siano K un campo, $A := K[x, y]$ ed $I := A\{x^2, xy\}$. Con $P_1 := Ax$ e $P_2 := A\{x, y\}$ si ha allora $I = P_1 \cap P_2^2$. Siccome P_2 è massimale, dal lemma 5.16 segue che P_2^2 è primario.

$\Delta := \{P_1, P_2^2\}$ è quindi una decomposizione primaria (minimale) di I.

Si noti però che $P_1 \subset P_2$. Inoltre $\sqrt{I} = \sqrt{P_1 \cap P_2^2} = \sqrt{P_1} \cap \sqrt{P_2^2} = P_1 \cap P_2 = P_1$. Nonostante ciò I non è primario.

Definizione 10.13. Per un ideale I di A sia

$\operatorname{Ass} A/I := \{P \in \operatorname{Spec} A \mid$ esiste $a \in A$ con $P = \sqrt{I : a}\}$

Gli elementi di $\operatorname{Ass} A/I$ sono detti *ideali primi associati ad* I.

La notazione è scelta in modo da renderla compatibile con quella comunemente usata per moduli M invece di A/I. Vedremo fra poco che nel caso di anelli noetheriani gli elementi di $\operatorname{Ass} A/I$ coincidono con gli ideali primi della forma $I : a$.

Osservazione 10.14. Un ideale decomponibile Q di A è primario se e solo se $\operatorname{Ass} A/Q$ consiste di esattamente un elemento.

Dimostrazione. (1) Sia Q primario. Allora $\Delta := \{Q\}$ è una decomposizione primaria minimale di Q e si ha $\operatorname{Ass} A/Q = \sqrt{\Delta} = \{\sqrt{Q}\}$.

(2) Sia $\operatorname{Ass} A/Q = \{P\}$. Per ipotesi esiste una decomposizione primaria minimale Δ di Q, necessariamente della forma $\Delta = \{Q\}$, per il lemma 5.24.

Definizione 10.15. Sia I un ideale di A. Gli elementi minimali di $\operatorname{Ass} A/I$ si chiamano *ideali primi minimali di I.*

Gli elementi di $\operatorname{Ass} A/I \setminus \operatorname{Min} \operatorname{Ass} A/I$ sono detti *ideali primi immersi di I.*

Proposizione 10.16. *Sia I un ideale decomponibile di A. Allora ogni ideale primo che contiene I contiene un elemento di* $\operatorname{Min} \operatorname{Ass} A/I$. *Perciò*

$$\operatorname{Min} \operatorname{Ass} A/I = \operatorname{Min} \operatorname{Spec} A : I$$

Dimostrazione. Siano Δ una decomposizione primaria minimale di I e $P' \in \operatorname{Spec} A : I$. Allora

$$P' = \sqrt{P'} \supset \sqrt{\bigcap_{Q\in\Delta} Q} \overset{5.17}{=} \bigcap_{Q\in\Delta} \sqrt{Q} = \bigcap_{P\in\sqrt{\Delta}} P = \bigcap_{P\in\operatorname{Min}\sqrt{\Delta}} P.$$

Per il lemma 10.9 esiste $P \in \operatorname{Min} \sqrt{\Delta}$ con $P \subset P'$.

Qui abbiamo usato che, per definizione, Δ è un insieme finito e quindi ogni elementi di $\sqrt{\Delta}$ contiene un elemento minimale di $\sqrt{\Delta}$.

Proposizione 10.17. *Siano I un ideale di A e Δ una decomposizione primaria minimale di I. Allora*

$$\bigcup_{P\in\sqrt{\Delta}} P = \{a \in A \mid I : a \neq I\}$$

Dimostrazione. (1) Siano $P \in \sqrt{\Delta}$ ed $a \in P$. Per il teorema 10.10 esiste $b \in A$ tale che $P = \sqrt{I : b}$. Perciò esiste $n \in \mathbb{N}+1$ tale che $a^n b \in I$; se scegliamo n in modo minimale , possiamo ottenere che $a^{n-1}b \notin I$. Allora $a \cdot a^{n-1}b \in I$, sicché $a^{n-1}b \in (I : a) \setminus I$.

(2) Sia $a \in A$ e assumiamo che esiste $b \notin I$ tale che $ab \in I$. Supponiamo, per assurdo, che $a \notin P$ per ogni $P \in \sqrt{\Delta}$. Ma $ab \in \bigcap\limits_{Q\in\Delta} Q$, quindi $b \in Q$ per ogni $Q \in \Delta$ per la definizione di ideale primario. Ciò implica $b \in I$, una contraddizione.

Corollario 10.18. *L'ideale 0 sia decomponibile . Allora $\bigcup\limits_{P\in\operatorname{Ass} A} P$ coincide con l'insieme degli zerodivisori di A.*

Lemma 10.19. *Siano $P \in \operatorname{Spec} A$, Q un ideale P-primario di A ed S un sottomonoide puro di A.*

(1) Se $S \cap P = \emptyset$, allora $S^{-1}P$ è primo ed $S^{-1}Q$ è $S^{-1}P$-primario con $S^*S^{-1}Q = Q$.

(2) Se $S \cap P \neq \emptyset$, allora $S^{-1}Q = S^{-1}A$.

Dimostrazione. (1) Dalla prop. 7.43 si ha $S^{-1}P \in \operatorname{Spec} S^{-1}A$.

Dimostriamo che $S^{-1}Q$ è $S^{-1}P$-primario: In primo luogo $\sqrt{S^{-1}Q} \overset{7.54}{=} S^{-1}\sqrt{Q} = S^{-1}P$.

Siano $a, b \in A$, $s, t \in S$ tali che $\frac{ab}{st} \in S^{-1}Q$, ad esempio $\frac{ab}{st} = \frac{q}{u}$ con $q \in Q$ ed $u \in S$, e sia $\frac{a}{s} \notin Q$. Allora esiste $r \in S$ tale che $abur = qstr \in Q$ e quindi $bur \in P$. Ciò implica $b \in P$, per cui $\frac{b}{t} \in S^{-1}P$.

Dobbiamo ancora dimostrare che $S^*S^{-1}Q = Q$. Sia $a \in S^*S^{-1}Q$. Per il lemma 7.42 allora esiste $s \in S$ con $as \in Q$. Siccome $s \notin P = \sqrt{Q}$, ciò implica $a \in Q$.

(2) Si ha ancora $\sqrt{S^{-1}Q} \overset{7.54}{=} S^{-1}\sqrt{Q} = S^{-1}P \overset{7.48}{=} S^{-1}A$. Ciò è possibile solo se $S^{-1}Q = S^{-1}A$.

Definizione 10.20. Siano Δ un insieme di ideali generalizzati di A ed S un sottomonoide puro di A. Poniamo

$$S^{-1}\Delta := \{S^{-1}Q \mid Q \in \Delta\}$$

Osservazione 10.21. Siano $J_1, \dots, J_m$ ideali generalizzati di A ed S un sottomonoide puro di A. Allora

$$S^*(J_1 \cap \dots \cap J_m) = S^*J_1 \cap \dots \cap S^*J_m$$

Dimostrazione. Ciò è chiaro perché $S^*J = i_S^{-1}(J)$ per ogni ideale generalizzato J.

Proposizione 10.22. *Siano I un ideale di A e Δ una decomposizione primaria minimale di I. Sia S un sottomonoide puro di A e siano*

$$\Delta_1 := \{Q \in \Delta \mid \sqrt{Q} \cap S = \emptyset\}$$

$$\Delta_2 := \Delta \setminus \Delta_1$$

Allora

(1) $S^{-1}\Delta_1$ è una decomposizione primaria minimale di $S^{-1}I$.

(2) Δ_1 è una decomposizione primaria minimale di $S^*S^{-1}I$.

Dimostrazione. (1) In primo luogo abbiamo $S^{-1}I = S^{-1} \bigcap\limits_{Q \in \Delta} Q \overset{8.20}{=} \bigcap\limits_{Q \in \Delta} S^{-1}Q \overset{10.19}{=} \bigcap\limits_{Q \in \Delta_1} S^{-1}Q$. Per il lemma 10.19 $S^{-1}\Delta$ è una decomposizione primaria di $S^{-1}I$ ed è immediato che si tratta di una decomposizione primaria minimale.

(2) $S^*S^{-1}I = S^* \bigcap\limits_{Q \in \Delta_1} S^{-1}Q \overset{10.21}{=} \bigcap\limits_{Q \in \Delta_1} S^*S^{-1}Q \overset{10.19}{=} \bigcap\limits_{Q \in \Delta_1} Q$.
Anche qui è immediato che la decomposizione primaria è minimale.

Osservazione 10.23. Sia $\mathcal{R} \subset \operatorname{Spec} A$ ed $\mathcal{R} \neq \emptyset$. Allora $S := A \setminus \bigcup\limits_{R \in \mathcal{R}} R$ è un sottomonoide puro di A.

Dimostrazione. $A \setminus \bigcup\limits_{R \in \mathcal{R}} R = \bigcap\limits_{R \in \mathcal{R}} (A \setminus R)$ dove $A \setminus R$ è un sottomonoide puro di A. Ma un'intersezione di sottomonoidi puri è un sottomonoide puro.

Lemma 10.24. *Siano I un ideale di A e $P_1, \dots, P_n \in \operatorname{Spec} A$ tali che $I \subset P_1 \cup \dots \cup P_n$. Allora esiste k tale che $I \subset P_k$.*

Dimostrazione. Facile per induzione su n.
Cfr. Atiyah/Macdonald, pag. 26.

Definizione 10.25. Siano I un ideale di A ed $\mathcal{R} \subset \operatorname{Ass} A/I$. $\mathcal{R}$ si dice *isolato rispetto ad I* se per $P \in \operatorname{Ass} A/I$ ed $R \in \mathcal{R}$ con $P \subset R$ si ha sempre $P \in \mathcal{R}$.

Osservazione 10.26. Siano I un ideale di A e $P \in \operatorname{Spec} A$. Allora sono equivalenti:

(1) $P \in \operatorname{Min} \operatorname{Ass} A/I$.

(2) $\{P\}$ è isolato rispetto ad I.

Osservazione 10.27. Siano I un ideale di A ed $\mathcal{R} \subset \operatorname{Ass} A/I$ isolato rispetto ad I. $\mathcal{R}$ sia finito e $\neq \emptyset$. Sia $S := A \setminus \bigcup\limits_{R \in \mathcal{R}} R$. Allora:

(1) S è un sottomonoide puro di A.

(2) $R \in \mathcal{R} \implies R \cap S = \emptyset$.

(3) $P' \in \operatorname{Ass} A/I \setminus \mathcal{R} \implies P' \cap S \neq \emptyset$.

Dimostrazione. (1) Oss. 10.23.

(2) Chiaro.

(3) Assumiamo, per assurdo, che $P' \cap S = \emptyset$. Allora $P' \subset \bigcup\limits_{R \in \mathcal{R}} R$. Per il lemma 10.24 esiste quindi $R \in \mathcal{R}$ tale che $P' \subset R$, e poiché $\mathcal{R}$ è isolato rispetto ad I, si ha $P' \in \mathcal{R}$, una contraddizione.

Teorema 10.28. *Siano I un ideale di A e $P \in \operatorname{Min} \operatorname{Ass} A/I$. Siano Δ e Δ' due decomposizioni primarie minimali di I e Q risp. Q' gli elementi P-primari di Δ risp. Δ' (univocamente determinati per la minimalità della decomposizione). Allora $Q = Q'$.*

Dimostrazione. Sia $S := A \setminus P$. Allora S è un sottomonoide puro di A e per $P' \in \operatorname{Spec} A$ si ha $P' \cap S = \emptyset \iff P' \setminus P = \emptyset \iff P' \subset P$.

Siccome P è minimale in $\operatorname{Ass} A/I$, per il teorema 10.10 si ha $P' \cap S \neq \emptyset$ per ogni $P' \in \sqrt{\Delta}$ con $P' \neq P$. Dalla prop. 10.22 segue $S^* S^{-1} I = Q$, ma anche $S^* S^{-1} I = Q'$, per cui $Q = Q'$.

Osservazione 10.29. Usando i risultati precedenti si può, in modo immediato, generalizzare il teorema 10.28 a sottoinsiemi isolati di $\operatorname{Ass} A/I$.

Definizione 10.30. Un ideale I di A si dice *irriducibile*, se dati ideali J ed L di A tali che $I = J \cap L$ si ha $I = J$ o $I = L$.

Proposizione 10.31. *Siano A un anello noetheriano ed I un ideale* *di A. Allora esistono ideali irriducibili $Q_1, \dots, Q_m$ tali che $I = Q_1 \cap \dots \cap Q_m$.*

Dimostrazione. Assumiamo, per assurdo, che l'insieme $\mathcal{B}$ degli ideali di A che non sono intersezione di un numero finito di ideali irriducibili di A sia $\neq \emptyset$. Allora $\mathcal{B}$ ammette un elemento massimale J.

Siccome allora J non è irriducibile, esistono due ideali L, M di A tali che $J \neq L$, $J \neq M$ e $J = L \cap M$. Per la minimalità di J necessariamente $L, M \notin \mathcal{B}$, perciò esistono ideali irriducibili $Q_1, \dots, Q_m$ di A tali che $L = Q_1 \cap \dots \cap Q_j$ e $M = Q_{j+1} \cap \dots \cap Q_m$. Ciò implica che $J = Q_1 \cap \dots \cap Q_m$, una contraddizione.

Lemma 10.32. *A sia noetheriano e l'ideale 0 sia irriducibile. Allora 0 è un ideale primario.*

Dimostrazione. Siano $a, b \in A$ tali che $ab = 0$ e sia ad esempio $a \neq 0$. Consideriamo la catena di ideali $\operatorname{Ann} b \subset \operatorname{Ann}(b^2) \subset \dots$. Tale catena è stazionaria, pertanto esiste $n \in \mathbb{N}$ tale che $\operatorname{Ann}(b^n) = \operatorname{Ann}(b^{n+1})$. Ne segue che $Ab^n \cap Aa = 0$; infatti, se $x \in Aa$ allora $xb = 0$, e se $x \in Ab^n$ allora $x = yb^n$ per un certo y. Pertanto $yb^{n+1} = 0$ da cui segue che $y \in \operatorname{Ann}(b^{n+1}) = \operatorname{Ann}(b^n)$ e quindi $a = yb^n = 0$. Poiché 0 è irriducibile e $Ay \neq 0$ necessariamente $x^n = 0$, cioè 0 è primario.

Proposizione 10.33. *A sia noetheriano e Q un ideale irriducibile di A. Allora Q è primario.*

Dimostrazione. Ciò segue dal cor. 10.32, considerando l'anello A/Q, anch'esso noetheriano.

Teorema 10.34. *Sia A noetheriano ed I un ideale di A.*

Allora I possiede una decomposizione primaria.

Dimostrazione. Segue direttamente dalla prop. 10.31, poiché per la prop. 10.33 ogni ideale irriducibile in un anello noetheriano è anche primario.

Lemma 10.35. *Siano A noetheriano ed I un ideale di A. Allora esiste $n \in \mathbb{N}$ tale che $(\sqrt{I})^n \subset I$.*

Dimostrazione. È sufficiente applicare la prop. 2.63 all'anello A/I.

Corollario 10.36. *Siano A noetheriano, Q un ideale di A ed $\mathfrak{m} \in \operatorname{Max} A$. Allora sono equivalenti:*

(1) Q è $\mathfrak{m}$-primario.

(2) $\sqrt{Q} = \mathfrak{m}$.

(3) Esiste $n \in \mathbb{N} + 1$ tale che $\mathfrak{m}^n \subset Q \subset \mathfrak{m}$.

Dimostrazione. (1) $\Longrightarrow$ (2): Chiaro.

(2) $\Longrightarrow$ (1): Ciò segue direttamente dal lemma 5.16.

(2) $\Longrightarrow$ (3): Per il lemma 10.35 esiste $n \in \mathbb{N}$ tale che $\mathfrak{m}^n \subset Q$. Inoltre naturalmente $Q \subset \sqrt{Q} = \mathfrak{m}$.

(3) $\Longrightarrow$ (2): Cor. 5.19.

Proposizione 10.37. *Siano A noetheriano ed I un ideale di A. Allora* $\operatorname{Ass} A/I := \{P \in \operatorname{Spec} A \mid$ ***esiste*** $a \in A$ ***con*** $P = I : a\}$

Dimostrazione. Considerando l'anello A/I possiamo supporre $I = 0$. Sia $\bigcap\limits_{Q \in \Delta} Q = 0$ una decomposizione primaria minimale dell'ideale 0. Siano inoltre $P_i = \sqrt{Q_i}$ per ogni $Q_i \in \Delta$. Sia $I_i = \bigcap\limits_{i \neq j} Q_i \neq 0$. Allora $\sqrt{\operatorname{Ann} Aa} = P_i$ per ogni elemento $a \neq 0$ in I_i, cosicché $\operatorname{Ann} Aa \subset P_i$.

Q_i è P_i-primario, quindi esiste $m \in \mathbb{N}$ tale che $P_i^m \subset Q_i$ e
$I_i P_i^m \subset I_i \cap P_i^m \subset I_i \cap Q_i = 0$. Sia $m \in \mathbb{N} + 1$ il più piccolo intero tale che $I_i P_i^m = 0$ e sia a un elemento non nullo in $I_i P_i^{m-1}$. Allora $P_i a = 0$, cioè $\operatorname{Ann} Aa \supset P_I$, quindi $\operatorname{Ann} Aa = P_i$.

Viceversa se $\operatorname{Ann} Aa$ è un ideale primo P, allora $\sqrt{\operatorname{Ann} Aa} = P$ cosicché $P \in \operatorname{Ass} A$ per il teorema 10.10.

Bibliografia

M. Atityah/I. Macdonald: Introduzione all'algebra commutativa. Feltrinelli 1981.

R. Brüske/F. Ischebeck/F. Vogel: Kommutative Algebra. Bibl. Inst. 1989.

J. Dauns: Modules and rings. Cambridge UP 2008.

D. Dummit/R. Foote: Abstract algebra. Wiley 2004.

K. Fieseler/L. Kaup: Algebraische Geometrie. Heldermann 2005.

S. Gabelli: Teoria delle equazioni e teoria di Galois. Springer 2008.

K. Goodearl/R. Warfield: An introduction to noncommutative noetherian rings. Cambridge UP 2004.

J. Kuipers: Quaternions and rotation sequences. Princeton UP 2002.

E. Kunz: Introduction to commutative algebra and algebraic geometry. Birkhäuser 1985.

M. Malliavin: Algèbre commutative. Masson 1985.

R. Pierce: Associative algebras. Springer 1982.

H. Pottmann/J. Wallner: Computational line geometry. Springer 2001.

J. Rotman: An introduction to homological algebra. Springer 2009.

M. Reid: Undergraduate commutative algebra. Cambridge UP 2002.

H. Sarges: Ein Beweis des Hilbertschen Basissatzes. J. reine u. angew. Math. 283/284 (1976), 436-437.

G. Scarpone: Moduli proiettivi e moduli iniettivi su anelli di Dedekind. Tesi LT, Ferrara 2011.

R. Sharp: Steps in commutative algebra. Cambridge UP 2000.