Appunti di

Algebra Superiore

Rosario Strano

A cura di Giuseppe Bilotta.

Dattiloscritti con $\mathcal{AMS}$-LaTeX.

Indice

Parte I

Algebra Commutativa

CAPITOLO I

Anelli ed ideali

1. Richiami

NOTAZIONI Nel seguito, supporremo sempre (tranne quando diversamente specificato) che A sia un anello commutativo con unità; denoteremo con 0 l'elemento nullo e con 1 l'unità.

OSSERVAZIONE 1.1 A priori, non è escluso che $0 = 1$; osserviamo però che ciò si verifica solo se $A = \{0\}$; infatti, se $0 = 1$ si ha, moltiplicando ambo i membri per $x \in A$, $0 = x$, e quindi $x = 0 \ \forall \ x \in A$.

NOTA Imporremo che gli omomorfismi tra anelli portino l'unità nell'unità. Denoteremo poi con

$$\operatorname{Ker} f = \{x \in A \mid f(x) = 0\}$$

il *nucleo* di un omomorfismo $f\colon A \to A'$, con

$$\operatorname{Im} f = \{f(a) \mid a \in A\}$$

la sua *immagine*, e con

$$\operatorname{CoKer} f = {}^{A'}\!/_{\operatorname{Im} f}$$

il suo *conucleo*.

OSSERVAZIONE 1.2 Ricordiamo che un omomorfismo f è iniettivo se e solo se $\operatorname{Ker} f$ è formato dal solo elemento nullo, ed è suriettivo se e solo se $\operatorname{CoKer} f$ è formato dal solo elemento nullo.

NOTAZIONI Seguendo la notazione germanica, denoteremo gli ideali di un anello A con le lettere gotiche $\mathfrak{a}$, $\mathfrak{b}$, ...

OSSERVAZIONE 1.3 Ricordiamo che se $\mathfrak{a}$ è un ideale di A, nasce spontaneamente l'insieme quoziente

$${}^{A}\!/_{\mathfrak{a}} = \{x + \mathfrak{a} \mid x \in A\}$$

costituito dai laterali di $\mathfrak{a}$; esso forma un anello, e vi è l'omomorfismo canonico

$$\pi\colon A \to {}^{A}\!/_{\mathfrak{a}}$$

definito da $\pi(x) = x + \mathfrak{a}$, il cui nucleo è proprio $\mathfrak{a}$; grazie allora al TEOR. di corrispondenza, esiste una biiezione fra gli ideali di A contenenti il nucleo ($\mathfrak{a}$) e gli ideali di ${}^{A}\!/_{\mathfrak{a}}$.

DEFINIZIONE 1.1 Ricordiamo che in un anello A un elemento non nullo a si dice *divisore dello zero* se esiste $b \neq 0$ tale che $ab = 0$.

Un anello privo di divisori dello zero si suole chiamare un *dominio (d'integrità)*.

DEFINIZIONE 1.2 Un elemento $a \in A$ si dice *nilpotente* se esiste $n \in \mathbb{N}$ tale che $x^n = 0$.

OSSERVAZIONE 1.4 Ogni elemento nilpotente è un divisore dello zero.

DEFINIZIONE 1.3 Un elemento $a \in A$ si dice *invertibile* se esiste $b \in A$ tale che $ab = 1$; b si dirà allora l'*inverso* di a e lo si denoterà con a^{-1}.

OSSERVAZIONE 1.5 Un elemento invertibile non può essere divisore dello zero. Infatti, se a è invertibile, da $ab = 0$ segue $a^{-1}ab = 0$ e quindi $b = 0$.

DEFINIZIONE 1.4 Ricordiamo che un anello non banale in cui ogni elemento non nullo è invertibile si dice un *campo*.

PROPOSIZIONE 1.1 *Le seguenti condizioni sono equivalenti:*

(1) *A è un campo;*
(2) *gli unici ideali di A sono (0) ed A;*
(3) *se B è un anello, ogni omomorfismo non nullo $f\colon A \to B$ è iniettivo.*

Dimostrazione. (**1**) $\Rightarrow$ (**2**) Sia $\mathfrak{a}$ un ideale non banale di A; esiste allora $x \in \mathfrak{a}$ non nullo, ed essendo A un campo, x è invertibile; si ha allora $1 = x^{-1}x \in \mathfrak{a}$, e quindi $\mathfrak{a} = A$.

(**2**) $\Rightarrow$ (**3**) Essendo f non nullo, il suo nucleo è distinto da A; ma il nucleo di un omomorfismo è un ideale, e l'unico ideale di A distinto da A è (0), e quindi $\operatorname{Ker} f = (0)$, ossia f è iniettivo.

(**3**) $\Rightarrow$ (**1**) Sia $x \in A$; consideriamo l'omomorfismo canonico $\pi\colon A \to {}^{A}\!/_{(x)}$; se π è nullo, allora, per la suriettvità di π, si ha ${}^{A}\!/_{(x)} = \{0\}$ e quindi $(x) = A$, ossia x è invertibile; se π è non nullo, è per ipotesi iniettivo, e quindi $x = 0$; pertanto, tutti gli elementi non nulli sono invertibili. □

DEFINIZIONE 1.5 Un ideale $\mathfrak{p}$ di A si dice *primo* se $\mathfrak{p} \neq A$ e da $xy \in \mathfrak{p}$ segue $x \in \mathfrak{p}$ oppure $y \in \mathfrak{p}$.

Un ideale $\mathfrak{m}$ di A si dice *massimale* se $\mathfrak{m} \neq A$ e da $\mathfrak{m} \subseteq \mathfrak{a} \subseteq A$ segue $\mathfrak{a} = \mathfrak{m}$ oppure $\mathfrak{a} = A$ (ossia, $\mathfrak{m}$ è massimale nella famiglia degli ideali, ordinata rispetto all'inclusione).

PROPOSIZIONE 1.2 *Un ideale $\mathfrak{p}$ è primo se e solo se ${}^{A}\!/_{\mathfrak{p}}$ è un dominio; un ideale $\mathfrak{m}$ è massimale se e solo se ${}^{A}\!/_{\mathfrak{m}}$ è un campo.*

Poiché ogni campo è un dominio, ogni ideale massimale è primo.

OSSERVAZIONE 1.6 Siano A, A' due anelli commutativi con unità, e sia $f\colon A \to A'$ un omomorfismo; se $\mathfrak{a}'$ è un ideale di A', $\mathfrak{a} = f^{-1}(\mathfrak{a}')$ è un ideale di A.

Tale corrispondenza conserva la primalità; infatti, se $\mathfrak{p}'$ è un ideale primo di A' e $\mathfrak{p} = f^{-1}(\mathfrak{p}')$ è il corrispondente ideale di A, f induce un'immersione di ${}^{A}\!/_{\mathfrak{p}}$ in ${}^{A'}\!/_{\mathfrak{p}'}$; essendo poi $\mathfrak{p}'$ primo, ${}^{A'}\!/_{\mathfrak{p}'}$ è un dominio, ed allora ${}^{A}\!/_{\mathfrak{p}}$ sarà un dominio (in quanto sottoanello di un dominio), ossia $\mathfrak{p}$ sarà primo.

La corrispondenza non conserva però la massimalità, poiché non tutti i sottoanelli di un campo sono campi (basta pensare a $\mathbb{Z} \subseteq \mathbb{Q}$); tuttavia, se f è suriettivo, la massimalità viene conservata, poiché l'immersione ${}^{A}\!/_{\mathfrak{m}} \hookrightarrow {}^{A'}\!/_{\mathfrak{m}'}$ è in realtà un isomorfismo, e pertanto, se il secondo insieme è un campo, anche il primo lo sarà, ossia: se $\mathfrak{m}'$ è massimale, anche $\mathfrak{m}$ lo è.

TEOREMA 1.1 *Ogni anello commutativo non banale con unità A possiede un ideale massimale.*

Dimostrazione. Sia $\mathcal{M}$ la famiglia degli ideali propri di A; $\mathcal{M}$ è non vuota, in quanto $(0) \in \mathcal{M}$, ed è parzialmente ordinata dalla relazione di inclusione; inoltre, un ideale di A è massimale in A se e solo se è un elemento massimale della famiglia $\mathcal{M}$.

Proviamo che ogni catena di $\mathcal{M}$ ammette un maggiorante; sia allora $\{\mathfrak{a}_\alpha\}_{\alpha\in S}$ una catena di $\mathcal{M}$; sia $\mathfrak{a} = \bigcup_{\alpha\in S} \mathfrak{a}_\alpha$; poiché gli ideali $\mathfrak{a}_\alpha$ sono contenuti l'uno nell'altro, $\mathfrak{a}$ è un ideale; inoltre $\mathfrak{a}_\alpha \subseteq \mathfrak{a}\ \forall\ \alpha \in S$; per provare che $\mathfrak{a}$ è un maggiorante della catena, occorre provare che $\mathfrak{a} \in \mathcal{M}$, ossia che $\mathfrak{a} \neq A$. Se, per assurdo, fosse $\mathfrak{a} = A$, si avrebbe $1 \in \mathfrak{a}$, e quindi esisterebbe $\bar\alpha \in S$ tale che $1 \in \mathfrak{a}_{\bar\alpha}$, ossia $\mathfrak{a}_{\bar\alpha} = A \notin \mathcal{M}$, assurdo.

È così provato che $\mathfrak{a}$ è un maggiorante della catena e, per l'arbitrarietà della scelta della catena, risulta provato che ogni catena di $\mathcal{M}$ ha un maggiorante; è allora possibile applicare il LEMMA di Zorn, che assicura che $\mathcal{M}$ ha un elemento massimale; come già osservato, un tale elemento è proprio un ideale massimale di A, e la tesi è così provata. □

COROLLARIO 1.1 *Ogni ideale proprio $\mathfrak{a}$ di un anello commutativo non banale con unità A è contenuto in un ideale massimale.*

Dimostrazione. L'omomorfismo canonico $\pi\colon A \to {}^{A}\!/_{\mathfrak{a}}$ è suriettivo; allora, preso un ideale massimale $\mathfrak{m}'$ di ${}^{A}\!/_{\mathfrak{a}}$ (che esiste per il precedente TEOR.), si ha che $\pi^{-1}(\mathfrak{m}')$ è un ideale massimale di A contenente $\mathfrak{a}$, e quindi la tesi. □

COROLLARIO 1.2 *Ogni elemento non invertibile di un anello commutativo non banale con unità A è contenuto in un ideale massimale.*

Dimostrazione. Sia x un elemento non invertibile di A; allora (x) è un ideale proprio di A, e quindi, per il COR. precedente, esiste un ideale massimale $\mathfrak{m}$ di A che contiene (x), e quindi, in particolare, x. □

NOTA Nel seguito supporremmo, tranne quando diversamente specificato, che gli anelli di cui si parla siano non banali.

DEFINIZIONE 1.6 Un anello A si dice *locale* se ha un solo ideale massimale $\mathfrak{m}$; in tal caso, il campo ${}^{A}\!/_{\mathfrak{m}}$ si dice *campo residuo* di A.

PROPOSIZIONE 1.3 *Sia A un anello commutativo con unità e sia $\mathfrak{m}$ un suo ideale; se ogni elemento di $A \setminus \mathfrak{m}$ è invertibile, allora A è locale ed $\mathfrak{m}$ è il suo unico ideale massimale.*

Dimostrazione. Sia $\mathfrak{a}$ un ideale proprio di A; gli elementi di $\mathfrak{a}$ sono allora non invertibili, e quindi $\mathfrak{a} \subseteq \mathfrak{m}$; $\mathfrak{m}$ è allora l'unico massimale, ed A è locale. □

PROPOSIZIONE 1.4 *Sia $\mathfrak{m}$ un ideale massimale di A; se il laterale $1 + \mathfrak{m}$ è formato da soli elementi invertibili, allora A è locale.*

Dimostrazione. Sia $x \notin \mathfrak{m}$; si ha $\mathfrak{m} \subsetneq \mathfrak{m} + (x)$ e quindi $\mathfrak{m} + (x) = A$; in particolare, esistono $m \in \mathfrak{m}$ e $\lambda \in A$ tali che $1 = m + \lambda x$, ossia $\lambda x = 1 - m \in 1 + \mathfrak{m}$, e quindi λx è invertibile; in particolare, x sarà allora invertibile. È così provato che ogni elemento di $A \setminus \mathfrak{m}$ è invertibile, e quindi A è locale. □

PROPRIETÀ degli ideali primi.

Gli ideali primi $\mathfrak{p}$ di un anello commutativo con unità A godono delle seguenti proprietà:

(1) *se* $\bigcap_{i=1}^n \mathfrak{a}_i \subseteq \mathfrak{p}$, *allora* $\mathfrak{a}_i \subseteq \mathfrak{p}$ *per qualche* i;
(2) *se* $\bigcap_{i=1}^n \mathfrak{a}_i = \mathfrak{p}$, *allora* $\mathfrak{a}_i = \mathfrak{p}$ *per qualche* i;
(3) *se* $\mathfrak{a} \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$, *allora* $\mathfrak{a} \subseteq \mathfrak{p}_i$ *per qualche* i.

Dimostrazione. Proviamo la **(1)**, ragionando per assurdo. Supponiamo che, per ogni $i = 1, 2, \ldots, n$, esista $a_i \in \mathfrak{a}_i \setminus \mathfrak{p}$; risultando $\prod_{i=1}^n a_i \in \mathfrak{a}_j \ \forall\ j = 1, 2, \ldots, n$, si ha $\prod_{i=1}^n a_i \in \bigcap_{i=1}^n \mathfrak{a}_i \subseteq \mathfrak{p}$ e quindi deve esistere un i tale che $a_i \in \mathfrak{p}$, contro la scelta degli elementi a_i.

Proviamo ora la **(2)**; per la **(1)**, esiste $\mathfrak{a}_i \subseteq \mathfrak{p}$;ma $\mathfrak{p} \subseteq \bigcap_{j=1}^n \mathfrak{a}_j \subseteq \mathfrak{a}_i$, e quindi $\mathfrak{p} \subseteq \mathfrak{a}_i$; si ha quindi l'uguaglianza $\mathfrak{a}_i = \mathfrak{p}$.

Proviamo infine la **(3)**, provando che se $\mathfrak{a} \nsubseteq \mathfrak{p}_i \ \forall\ i = 1, 2, \ldots, n$, allora $\mathfrak{a} \nsubseteq \bigcup_{i=1}^n \mathfrak{p}_i$.

Ragioniamo per induzione sul numero n di ideali primi $\mathfrak{p}_i$. La tesi è banalmente vera nel caso si abbia un unico ideale primo $\mathfrak{p}$ (base dell'induzione); supponiamo ora la tesi vera per $n-1$ ($n > 1$), e proviamo la tesi per n.

Fissiamo $i = 1, 2, \ldots, n$; avendosi in particolare $\mathfrak{a} \nsubseteq \mathfrak{p}_j$ per $j \neq i$, ed essendo la proprietà vera nel caso di $n-1$ ideali, possiamo dire che $\mathfrak{a} \nsubseteq \bigcup_{j\neq i} \mathfrak{p}_j$, e quindi esiste $x_i \in \mathfrak{a}$ tale che $x_i \notin \mathfrak{p}_j \ \forall\ j \neq i$. Al variare di $i = 1, 2, \ldots, n$ otteniamo n elementi $x_1, x_2, \ldots, x_n$ di $\mathfrak{a}$. Se esiste i tale che $x_i \notin \mathfrak{p}_i$, si ha $x_i \notin \mathfrak{p}_j \ \forall\ j = 1, 2, \ldots, n$, e quindi $\mathfrak{a} \nsubseteq \bigcup_{j=1}^n \mathfrak{p}_j$, che è quanto volevamo provare. Se invece $x_i \in \mathfrak{p}_i \ \forall\ i = 1, 2, \ldots, n$, consideriamo l'elemento

$$y = \sum_{i=1}^{n} \left(\prod_{j\neq i} x_j \right) \in \mathfrak{a};$$

e proviamo che $y \notin \mathfrak{p}_i \ \forall\ i = 1, 2, \ldots, n$ (da cui seguirà la tesi).

Supponiamo per assurdo che ciò non sia vero; esisterà allora un $\mathfrak{p}_i$ contente y; per la scelta degli x_j, si ha $\prod_{j\neq i} x_j \notin \mathfrak{p}_i$ e $\prod_{j\neq h} x_j \in \mathfrak{p}_i \ \forall\ h \neq i$; si ha d'altra parte

$$y - \sum_{h\neq i} \left(\prod_{j\neq h} x_j \right) = \prod_{j\neq i} x_j,$$

ed il primo membro è un elemento di $\mathfrak{p}_i$, mentre il secondo no; ciò è evidentemente un assurdo, e la tesi è quindi vera. □

OSSERVAZIONE 1.7 La proprietà **(3)** continua a valere anche se al più due ideali non sono primi.

1.1. Alcuni ideali particolari.

DEFINIZIONE 1.7 L'insieme $\mathcal{N}$ degli elementi nilpotenti di A si suole chiamare il *nilradicale* di A.

PROPOSIZIONE 1.5 *$\mathcal{N}$ è un ideale.*

Dimostrazione. Occorre provare che $\mathcal{N}$ è chiuso rispetto alla somma e che $\mathcal{N}$ gode della proprietà d'assorbimento.

Proviamo che $\mathcal{N}$ è chiuso rispetto alla somma; se $x, y \in \mathcal{N}$, esistono $n, m \in \mathbb{N}$ tali che $x^n = y^m = 0$; proviamo che $x+y$ è nilpotente con potenza $n+m-1$; si ha infatti

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

e la somma a secondo membro è tutta costituita da zeri in quanto, se $i \geq n$, si ha $x^i = 0$; se $i < n$, si ha $n+m-1-i > m-1 \geq m$ e quindi $y^{n+m-1-i} = 0$; si ha allora $(x+y)^{n+m-1} = 0$, e quindi $x+y \in \mathcal{N}$, ed è così provata la chiusura di $\mathcal{N}$ rispetto alla somma.

La proprietà di assorbimento degli ideali è pure banalmente verificata, in quanto, se $x \in \mathcal{N}$, con esponente di nilpotenza n, ed $\alpha \in A$, si ha $(\alpha x)^n = \alpha^n x^n = 0$, e quindi $\alpha x \in \mathcal{N}$. □

PROPOSIZIONE 1.6 *Il nilradicale di A è l'intersezione di tutti gli ideali primi di A.*

Dimostrazione. Proviamo innanzi tutto che $\mathcal{N}$ è contenuto nell'intersezione degli ideali primi. Fissato $x \in \mathcal{N}$, sia n il suo esponente di nilpotenza; per ogni ideale primo $\mathfrak{p}$ di A si ha $0 \in \mathfrak{p}$, ossia $x^n \in \mathfrak{p}$, e quindi $x \in \mathfrak{p}$ (per la definizione di ideale primo).

Viceversa, proviamo che $\mathcal{N}$ contiene l'intersezione degli ideali primi; equivalentemente, proviamo che se $x \notin \mathcal{N}$, allora esiste un ideale primo $\mathfrak{p}$ di A che non contiene x.

Sia $x \notin \mathcal{N}$. Sia $\mathcal{M}$ la famiglia degli ideali $\mathfrak{a} \subseteq A$ tali che $x^n \notin \mathfrak{a}\ \forall\, n \in \mathbb{N}$; essendo $x \notin \mathcal{N}$, si ha $x^n \notin (0)\ \forall\, n \in \mathbb{N}$; quindi $\mathcal{M}$ è non vuota, in quanto $(0) \in \mathcal{M}$.

Verifichiamo che $\mathcal{M}$ soddisfa le ipotesi del LEMMA di Zorn. Sia $\mathcal{C} = \{\mathfrak{a}_\alpha\}_{\alpha \in S}$ una catena di $\mathcal{M}$; l'insieme $\mathfrak{a} = \bigcup_{\alpha \in S} \mathfrak{a}_\alpha$ è un ideale, e risulta $\mathfrak{a} \in \mathcal{M}$ (ciò si prova come nel TEOR. 1.1); $\mathfrak{a}$ è allora un maggiorante della catena $\mathcal{C}$; data l'arbitrarietà della scelta di $\mathcal{C}$, possiamo affermare che ogni catena di $\mathcal{M}$ ha un maggiorante, e quindi $\mathcal{M}$ soddisfa il LEMMA di Zorn, che assicura l'esistenza in $\mathcal{M}$ di un elemento massimale $\mathfrak{p}$; per provare la tesi basta provare che $\mathfrak{p}$ è primo e che $x \notin \mathfrak{p}$.

Essendo $\mathfrak{p} \in \mathcal{M}$, si ha $x^n \notin \mathfrak{p}\ \forall\, n \in \mathbb{N}$, e quindi in particolare $x \notin \mathfrak{p}$.

Proviamo infine che $\mathfrak{p}$ è primo; essendo $x \notin \mathfrak{p}$, si ha $\mathfrak{p} \neq A$; siano ora $y, z \in A$ tali che $yz \in \mathfrak{p}$; proviamo che $y \in \mathfrak{p}$ oppure $z \in \mathfrak{p}$. Se per assurdo si avesse $y \notin \mathfrak{p}$ e $z \notin \mathfrak{p}$, i due ideali $\mathfrak{p}+(y)$ e $\mathfrak{p}+(z)$ conterrebbero propriamente $\mathfrak{p}$; per la massimalità di $\mathfrak{p}$ in $\mathcal{M}$ si avrebbe allora $\mathfrak{p}+(y) \notin \mathcal{M}$ e $\mathfrak{p}+(z) \notin \mathcal{M}$; esisterebbero allora $n, m \in \mathbb{N}$ tali che $x^n \in \mathfrak{p}+(y)$ e $x^m \in \mathfrak{p}+(z)$, e sarebbe quindi possibile determinare $p_1, p_2 \in \mathfrak{p}$ e $\lambda, \mu \in A$ tali che $x^n = p_1 + \lambda y$ e $x^m = p_2 + \mu z$; allora

$$x^{n+m} = (p_1 + \lambda y)(p_2 + \mu z) = p_3 + \lambda\mu yz \in \mathfrak{p}$$

(con $p_3 = p_1 p_2 + \lambda y p_2 + \mu z p_1 \in \mathfrak{p}$), in contrasto con il fatto che $\mathfrak{p} \in \mathcal{M}$. Risulta così provato che $\mathfrak{p}$ è primo, e ciò completa la dimostrazione. □

DEFINIZIONE 1.8 Sia A un anello commutativo con unità; dicesi *radicale di Jacobson* l'intersezione $\mathcal{R}$ di tutti gli ideali massimali di A.

PROPOSIZIONE 1.7 *Sia A un anello commutativo con unità, e sia U il sottoinsieme degli elementi invertibili di A; si ha allora la seguente caratterizzazione del radicale*

di Jacobson di A:

$$\mathcal{R} = \{x \in A \mid 1 + \lambda x \in U \ \forall\ \lambda \in A\}.$$

Dimostrazione. Proviamo che $\mathcal{R} \subseteq \{x \in A \mid 1 + \lambda x \in U \ \forall\ \lambda \in A\}$. Sia $x \in \mathcal{R}$; proviamo che $1+\lambda x$ è invertibile per ogni $\lambda \in A$. Supponiamo per assurdo che esista $\bar\lambda \in A$ per cui $1+\bar\lambda x$ non sia invertibile; esiste allora un ideale massimale $\mathfrak{m}$ per cui $1+\lambda x \in \mathfrak{m}$; ma $x \in \mathfrak{m}$, e quindi $1 \in \mathfrak{m}$, ossia $\mathfrak{m} = A$, assurdo.

Proviamo l'inclusione inversa. Sia allora $x \in A$ tale che $1 + \lambda x$ è invertibile per ogni $\lambda \in A$; proviamo che $x \in \mathcal{R}$, ossia che $x \in \mathfrak{m}$ per ogni ideale massimale $\mathfrak{m}$ di A. Supponiamo per assurdo che esista $\mathfrak{m}$ massimale per cui $x \notin \mathfrak{m}$; allora $\mathfrak{m} \subsetneq \mathfrak{m} + (x)$, e quindi $\mathfrak{m} + (x) = A$; esistono allora $\mu \in A$ ed $m \in \mathfrak{m}$ tali che $1 = m + \mu x$, ossia $m = 1-\mu x$; ma $1-\mu x$ è invertibile (in quanto nella forma $1+\lambda x$, con $\lambda = -\mu \in A$) e quindi m sarebbe invertibile; $\mathfrak{m}$ conterrebbe allora un elemento invertibile, e quindi $\mathfrak{m} = A$, contro la massimalità di $\mathfrak{m}$. L'assurdo assicura allora la tesi. □

2. Operazioni con gli ideali

Definizione 2.1 Siano $\mathfrak{a}, \mathfrak{b}$ due ideali di un anello commutativo con unità A; si definiscono le seguenti operazioni sugli ideali:

$$\mathfrak{a} \cap \mathfrak{b} \qquad (\textit{intersezione})$$

$$\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\} \qquad (\textit{somma})$$

$$\mathfrak{a} \cdot \mathfrak{b} = \left\{ \sum_{i=1}^{n} a_i \cdot b_i \mid n \in \mathbb{N},\ a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\ \forall\ i = 1, 2, \ldots, n \right\} \qquad (\textit{prodotto})$$

in particolare

$$\mathfrak{a}^n = \overbrace{\mathfrak{a} \cdot \mathfrak{a} \cdot \cdots \cdot \mathfrak{a}}^{n} \qquad (\textit{potenza})$$

Proprietà *Le operazioni sui radicali godono delle seguenti proprietà di immediata verifica:*

(1) $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}\ \forall\ \mathfrak{a}, \mathfrak{b}$*; in particolare,* $\mathfrak{a}^n \subseteq \mathfrak{a}\ \forall\ n \in \mathbb{N},\ \forall\ \mathfrak{a}$*;*
(2) $\mathfrak{a} \cdot (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cdot \mathfrak{b} + \mathfrak{a} \cdot \mathfrak{c} \quad \forall\ \mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ *(proprietà distributiva);*
(3) $\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c} \iff \mathfrak{b} \subseteq \mathfrak{a} \ \vee\ \mathfrak{c} \subseteq \mathfrak{a}$ *(proprietà di modularità);*
(4) $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{a} \cdot \mathfrak{b} \quad \forall\ \mathfrak{a}, \mathfrak{b}$.

(def) Osservazione 2.1 In particolare, dalla **(3)** segue che, se $\mathfrak{a}, \mathfrak{b}$ sono *coprimi*, ossia se $\mathfrak{a} + \mathfrak{b} = A$, allora $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a} \cdot \mathfrak{b}$, e quindi, essendo sempre (per **(1)**) $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$, si ha $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a} \cdot \mathfrak{b}$.

Definizione 2.2 Siano $\mathfrak{a}, \mathfrak{b}$ due ideali di un anello commutativo con unità A; si definisce *quoziente* dei due ideali l'insieme

$$\mathfrak{a} : \mathfrak{b} = \{x \in A \mid x \cdot \mathfrak{b} \subseteq \mathfrak{a}\}$$

Notazioni Se $\mathfrak{a} = (0)$, scriveremo $0 : \mathfrak{b}$ invece di $(0) : \mathfrak{b}$. Tale insieme viene detto
(def) *annullatore* di $\mathfrak{b}$, e lo si indica anche con $\operatorname{Ann}(\mathfrak{b})$; esso è

$$\operatorname{Ann}(\mathfrak{b}) = \{x \in A \mid xb = 0\ \forall\ b \in \mathfrak{b}\};$$

in particolare, se $\mathfrak{b} = (x)$, scriveremo $0 : x$ invece di $0\colon (x)$; tale insieme si dirà *annullatore* di x, e viene indicato con $\operatorname{ann}(x)$; esso è l'insieme (DEF)

$$\operatorname{ann}(x) = \{y \in A \mid yx = 0\}.$$

OSSERVAZIONE 2.2 Osserviamo che l'insieme $\bigcup_{x\in A} \operatorname{ann}(x)$ è l'insieme $\mathcal{D}$ dei divisori dello zero di A.

PROPRIETÀ *Siano $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ ideali di un anello commutativo commutativo con unità; valgono allora le seguenti relazioni:*

(1) $\mathfrak{a} \subseteq \mathfrak{a} : \mathfrak{b}$*;*
(2) $(\mathfrak{a} : \mathfrak{b}) \cdot \mathfrak{b} \subseteq \mathfrak{a}$*;*
(3) $(\mathfrak{a} : \mathfrak{b}) : \mathfrak{c} = \mathfrak{a} : (\mathfrak{b} \cdot \mathfrak{c}) = (\mathfrak{a} : \mathfrak{c}) : \mathfrak{b}$*;*
(4) $\left(\bigcap_{i\in I} \mathfrak{a}_i\right) : \mathfrak{b} = \bigcap_{i\in I} (\mathfrak{a}_i : \mathfrak{b})$*;*
(5) $\mathfrak{a} : \left(\sum_{i\in I} \mathfrak{b}_i\right) = \bigcap_{i\in I} (\mathfrak{a} : \mathfrak{b}_i)$.

Dimostrazione. Le prime tre proprietà sono banali; proviamo **(4)** e **(5)**.

Per la **(4)**, consideriamo la seguente catena di equivalenze:

$$x \in \left(\bigcap_{i\in I} \mathfrak{a}_i\right) : \mathfrak{b} \iff x \cdot \mathfrak{b} \subseteq \bigcap_{i\in I} \mathfrak{a}_i \iff x \cdot \mathfrak{b} \subseteq \mathfrak{a}_i \ \forall\, i \in I \iff$$
$$\iff x \in \mathfrak{a}_i : \mathfrak{b} \ \forall\, i \in I \iff x \in \bigcap_{i\in I} (\mathfrak{a}_i : \mathfrak{b}).$$

Per la **(5)**, si ha, da un lato:

$$x \in \mathfrak{a} : \left(\sum_{i\in I} \mathfrak{b}_i\right) \implies xc \in \mathfrak{a} \ \forall\, c \in \sum_{i\in I} \mathfrak{b}_i \implies$$
$$\implies xb \in \mathfrak{a} \ \forall\, b \in \mathfrak{b}_i,\ \forall\, i \in I \implies$$
$$\implies x \in \mathfrak{a} : \mathfrak{b}_i \ \forall\, i \in I \implies x \in \bigcap_{i\in I} (\mathfrak{a} : \mathfrak{b}_i),$$

e quindi $\mathfrak{a} : \left(\sum_{i\in I} \mathfrak{b}_i\right) \subseteq \bigcap_{i\in I} (\mathfrak{a} : \mathfrak{b}_i)$; d'altra parte,

$$x \in \bigcap_{i\in I} (\mathfrak{a} : \mathfrak{b}_i) \implies xb \in \mathfrak{a} \ \forall\, b \in \mathfrak{b}_i,\ \forall\, i \in I \implies$$
$$\implies xc = x \sum_{i\in I} b_i = \sum_{i\in I} xb_i \in \mathfrak{a} \ \forall\, c = \sum_{i\in I} b_i \in \sum_{i\in I} \mathfrak{b}_i \implies$$
$$\implies xc \in \mathfrak{a} \ \forall\, c \in \sum_{i\in I} \mathfrak{b}_i \implies x \in \mathfrak{a} : \left(\sum_{i\in I} \mathfrak{b}_i\right),$$

ed è così provata l'inclusione $\mathfrak{a} : \left(\sum_{i\in I} \mathfrak{b}_i\right) \supseteq \bigcap_{i\in I} (\mathfrak{a} : \mathfrak{b}_i)$; si ha allora in definitiva l'eguaglianza della tesi **(5)**. □

DEFINIZIONE 2.3 Sia $\mathfrak{a}$ un ideale[1] di un anello commutativo con unità A; dicesi *radicale* di $\mathfrak{a}$, e si indica con uno dei simboli $\mathfrak{r}(\mathfrak{a})$, $\sqrt{\mathfrak{a}}$, l'insieme

$$\mathfrak{r}(\mathfrak{a}) = \{x \in A \mid \exists\, n \in \mathbb{N} \mid x^n \in \mathfrak{a}\}.$$

OSSERVAZIONE 2.3 $\mathfrak{r}(\mathfrak{a})$ è l'ideale intersezione degli ideali primi di A contenenti $\mathfrak{a}$.

[1] in realtà, il radicale può essere definito per un qualunque sottoinsieme di A, ma non è in tal caso garantito che sia un ideale.

Dimostrazione. Consideriamo l'omomorfismo canonico suriettivo $\pi\colon A \to {}^{A}\!/_{\mathfrak{a}}$; si vede immediatamente che $x \in \mathsf{r}(\mathfrak{a})$ se e solo se $\pi(x)$ sta nel nilradicale di ${}^{A}\!/_{\mathfrak{a}}$, e quindi $\mathsf{r}(\mathfrak{a})$ è la retroimmagine, secondo π, del nilradicale di ${}^{A}\!/_{\mathfrak{a}}$, che è un ideale ed è l'intersezione di tutti i primi di ${}^{A}\!/_{\mathfrak{a}}$; ne segue allora che $\mathsf{r}(\mathfrak{a})$ è un ideale, e che $\mathsf{r}(\mathfrak{a})$ è l'intersezione di tutti gli ideali primi contenenti $\mathfrak{a}$. □

Proprietà del radicale.

(1) $\mathfrak{a} \subseteq \mathfrak{b} \implies \mathsf{r}(\mathfrak{a}) \subseteq \mathsf{r}(\mathfrak{b})$;
(2) $\mathfrak{a} \subseteq \mathsf{r}(\mathfrak{a})$;
(3) $\mathsf{r}(\mathsf{r}(\mathfrak{a})) = \mathsf{r}(\mathfrak{a})$;
(4) $\mathsf{r}(\mathfrak{a} \cdot \mathfrak{b}) = \mathsf{r}(\mathfrak{a} \cap \mathfrak{b}) = \mathsf{r}(\mathfrak{a}) \cap \mathsf{r}(\mathfrak{b})$;
(5) $\mathsf{r}(\mathfrak{a} + \mathfrak{b}) = \mathsf{r}(\mathsf{r}(\mathfrak{a}) + \mathsf{r}(\mathfrak{b}))$;
(6) $\mathsf{r}(\mathfrak{a}) = (1) \iff \mathfrak{a} = (1)$;
(7) *se* $\mathfrak{p}$ *è primo, allora* $\mathsf{r}(\mathfrak{p}^n) = \mathfrak{p}\ \forall\ n \in \mathbb{N}$.

Dimostrazione. Proviamo la **(4)**. Avendosi $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$, per **(1)** si ha $\mathsf{r}(\mathfrak{a} \cdot \mathfrak{b}) \subseteq \mathsf{r}(\mathfrak{a} \cap \mathfrak{b})$; ma $\mathfrak{a} \cap \mathfrak{b}$ è contenuto sia in $\mathfrak{a}$, sia in $\mathfrak{b}$, e quindi, sempre per **(1)**, $\mathsf{r}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathsf{r}(\mathfrak{a})$ e $\mathsf{r}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathsf{r}(\mathfrak{b})$, e quindi $\mathsf{r}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathsf{r}(\mathfrak{a}) \cap \mathsf{r}(\mathfrak{b})$; è quindi provata la catena di inclusioni

$$\mathsf{r}(\mathfrak{a} \cdot \mathfrak{b}) \subseteq \mathsf{r}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathsf{r}(\mathfrak{a}) \cap \mathsf{r}(\mathfrak{b});$$

per provare che sussistono le uguaglianze, basta allora provare che $\mathsf{r}(\mathfrak{a}) \cap \mathsf{r}(\mathfrak{b}) \subseteq \mathsf{r}(\mathfrak{a} \cdot \mathfrak{b})$; ed infatti, se $x \in \mathsf{r}(\mathfrak{a}) \cap \mathsf{r}(\mathfrak{b})$, esistono $n, m \in \mathbb{N}$ tali che $x^n \in \mathfrak{a}, x^m \in \mathfrak{b}$; allora $x^{n+m} \in \mathfrak{a} \cdot \mathfrak{b}$, e quindi $x \in \mathsf{r}(\mathfrak{a} \cdot \mathfrak{b})$.

Proviamo ora la **(6)**. Si ha banalmente

$$\mathsf{r}(\mathfrak{a}) = (1) \iff 1 \in \mathsf{r}(\mathfrak{a}) \iff 1^n = 1 \in \mathfrak{a} \iff 1 \in \mathfrak{a} \iff \mathfrak{a} = (1)$$

Proviamo infine la **(7)**. Si ha $\mathsf{r}(\mathfrak{p}^n) \subseteq \mathfrak{p}$ poiché $\mathfrak{p}$ è un primo contenente $\mathfrak{p}^n$; l'inclusione inversa è sempre vera, ed quindi verificata l'uguaglianza della tesi. □

Osservazione 2.4 Due ideali $\mathfrak{a}, \mathfrak{b}$ sono coprimi se e solo se lo sono $\mathsf{r}(\mathfrak{a})$ ed $\mathsf{r}(\mathfrak{b})$.

Dimostrazione. $\mathfrak{a}, \mathfrak{b}$ sono coprimi se e solo se $\mathfrak{a} + \mathfrak{b} = (1)$, ovvero (per la **(6)**) se e solo se $\mathsf{r}(\mathfrak{a} + \mathfrak{b}) = (1)$, che equivale a $\mathsf{r}(\mathsf{r}(\mathfrak{a}) + \mathsf{r}(\mathfrak{b})) = (1)$ (per la **(5)**), che per la **(6)** equivale a $\mathsf{r}(\mathfrak{a}) + \mathsf{r}(\mathfrak{b}) = (1)$, ossia se e solo se $\mathsf{r}(\mathfrak{a}), \mathsf{r}(\mathfrak{b})$ sono coprimi. □

3. Ideali ed omomorfismi

Sia $f\colon A \to B$ un omomorfismo tra anelli commutativi con unità. Abbiamo già visto che, per ogni ideale $\mathfrak{b}$ di B, l'insieme $f^{-1}(\mathfrak{b})$ è un ideale di A; esso si suole (DEF) chiamare *contrazione* di $\mathfrak{b}$ (in A, secondo f), e lo si denota con $\mathfrak{b}^c$.

Viceversa, fissato un ideale $\mathfrak{a}$ di A, possiamo considerare, in B, l'ideale generato da $f(\mathfrak{a})$ (poiché, in generale, $f(\mathfrak{a})$ *non* è un ideale); esso si suole indicare con $\mathfrak{a}^e$, o con $\mathfrak{a}B$, e si suole chiamare *esteso* di $\mathfrak{a}$ (in B); si ha:

$$\mathfrak{a}^e = \mathfrak{a}B = \left\{ \sum_{i=1}^{n} f(a_i)b_i \mid n \in \mathbb{N}, a_i \in \mathfrak{a}, b_i \in B\ \forall\ i = 1, 2, \ldots, n \right\}$$

Se f è suriettiva, $f(\mathfrak{a})$ è un ideale e risulta $\mathfrak{a}^e = f(\mathfrak{a})$.

Proprietà dell'estensione e contrazione di ideali.

(1) $\mathfrak{a}^{ec} \supseteq \mathfrak{a}$, $\mathfrak{b}^{ce} \subseteq \mathfrak{b}$;
(2) $\mathfrak{a}^{ece} = \mathfrak{a}^e$, $\mathfrak{b}^{cec} = \mathfrak{b}^c$;
(3) *detto C l'insieme degli ideali contratti di A (cioè tali che $\mathfrak{a}^{ec} = \mathfrak{a}$), e detto E l'inseme degli ideali estesi di B (cioè tali che $\mathfrak{b}^{ce} = \mathfrak{b}$), si ha una biiezione tra C ed E associando ad ogni ideale $\mathfrak{a} \in C$ l'ideale $\mathfrak{a}^e$, ed ad ogni ideale $\mathfrak{b} \in E$ l'ideale $\mathfrak{b}^c$.*

PROPRIETÀ dell'estensione e contrazione di ideali. *Rispetto alle operazioni di somma, intersezione, prodotto, quoziente e radicale, l'estensione e la contrazione di ideali si comportano secondo la seguente tabella:*

Operazione	Estensione	Contrazione
somma	$(\mathfrak{a}_1 + \mathfrak{a}_2)^e = {\mathfrak{a}_1}^e + {\mathfrak{a}_2}^e$	$(\mathfrak{b}_1 + \mathfrak{b}_2)^c \subseteq {\mathfrak{b}_1}^c + {\mathfrak{b}_2}^c$
intersezione	$(\mathfrak{a}_1 \cap \mathfrak{a}_2)^e \subseteq {\mathfrak{a}_1}^e \cap {\mathfrak{a}_2}^e$	$(\mathfrak{b}_1 \cap \mathfrak{b}_2)^c = {\mathfrak{b}_1}^c \cap {\mathfrak{b}_2}^c$
prodotto	$(\mathfrak{a}_1 \cdot \mathfrak{a}_2)^e = {\mathfrak{a}_1}^e \cdot {\mathfrak{a}_2}^e$	$(\mathfrak{b}_1 \cdot \mathfrak{b}_2)^c \subseteq {\mathfrak{b}_1}^c \cdot {\mathfrak{b}_2}^c$
quoziente	$(\mathfrak{a}_1 : \mathfrak{a}_2)^e \subseteq {\mathfrak{a}_1}^e : {\mathfrak{a}_2}^e$	$(\mathfrak{b}_1 : \mathfrak{b}_2)^c \subseteq {\mathfrak{b}_1}^c : {\mathfrak{b}_2}^c$
radicale	$(\mathfrak{r}(\mathfrak{a}))^e \subseteq \mathfrak{r}(\mathfrak{a}^e)$	$(\mathfrak{r}(\mathfrak{b}))^c = \mathfrak{r}(\mathfrak{b}^c)$

Dimostrazione. Proviamo alcune delle suddette relazioni, per dare un metodo; le altre sono lasciate per esercizio.

Proviamo, ad esempio, che $(\mathfrak{r}(\mathfrak{a}))^e \subseteq \mathfrak{r}(\mathfrak{a}^e)$.

Per definizione, $(\mathfrak{r}(\mathfrak{a}))^e$ è il più piccolo ideale contenente $f(\mathfrak{r}(\mathfrak{a}))$; ma essendo $f(\mathfrak{a}) \subseteq \mathfrak{a}^e$, si ha $f(\mathfrak{r}(\mathfrak{a})) \subseteq \mathfrak{r}(f(\mathfrak{a})) \subseteq \mathfrak{r}(\mathfrak{a}^e)$, e quindi $\mathfrak{r}(\mathfrak{a}^e)$ è un'ideale contenente $f(\mathfrak{r}(\mathfrak{a}))$;da ciò segue allora che $(\mathfrak{r}(\mathfrak{a}))^e$ è contenuto in $\mathfrak{r}(\mathfrak{a}^e)$.

Proviamo anche che $(\mathfrak{b}_1 : \mathfrak{b}_2)^c \subseteq {\mathfrak{b}_1}^c : {\mathfrak{b}_2}^c$.

Sia $x \in (\mathfrak{b}_1 : \mathfrak{b}_2)^c$; allora $f(x) \in \mathfrak{b}_1 : \mathfrak{b}_2$, ossia $f(x)\mathfrak{b}_2 \subseteq \mathfrak{b}_1$. Proviamo che $x{\mathfrak{b}_2}^c \subseteq \mathfrak{b}_1$. Sia $y \in {\mathfrak{b}_2}^c$; allora $f(y) \in \mathfrak{b}_2$, e quindi $f(xy) = f(x)f(y) \in \mathfrak{b}_1$, ossia $xy \in {\mathfrak{b}_1}^c$, che è quanto volevamo provare. □

CAPITOLO II

Moduli

1. Prime definizioni

DEFINIZIONE 1.1 Sia A un anello commutativo con unità; un insieme M si dice un A-modulo se sono definite due operazioni $+\colon M \times M \to M$ e $\cdot\colon A \times M \to M$ tali che $(M,+)$ sia un gruppo abeliano e

(1) $1 \cdot m = m \ \forall\ m \in M$;
(2) $(ab)m = a(bm) \ \forall\ a,b \in A,\ \forall\ m \in M$;
(3) $(a+b)m = am + bm \ \forall\ a,b \in A,\ \forall\ m \in M$;
(4) $a(m_1+m_2) = am_1 + am_2 \ \forall\ a \in A,\ \forall\ m_1,m_2 \in M$.

Vediamo tre importanti esempi di A-moduli.

ESEMPIO 1.1 Se $A = \mathbb{K}$ è un campo, gli A-moduli sono tutti e soli i $\mathbb{K}$-spazi vettoriali.

ESEMPIO 1.2 A è un A-modulo, i cui sottomoduli sono tutti e soli gli ideali.

ESEMPIO 1.3 Se $A = \mathbb{Z}$, i $\mathbb{Z}$-moduli sono tutti e soli i gruppi abeliani G; in tal caso, il prodotto esterno è definito con

$$ng = \begin{cases} \overbrace{g+g+\cdots+g}^{n} & \forall\ n > 0 \\ 0_G & \text{se } n = 0 \\ -(\underbrace{g+g+\cdots+g}_{n}) & \forall\ n < 0 \end{cases}$$

La teoria dei moduli può allora essere vista come un'estensione della teoria dei gruppi, comprendente anche la teoria degli anelli e la teoria degli spazi vettoriali (Algebra Lineare).

Ad esempio, il

TEOREMA 1.1 (fondamentale sui gruppi abeliani) *Ogni gruppo abeliano finitamente generato è somma diretta di gruppi ciclici.*

si estende naturalmente nel

TEOREMA 1.2 *Se A è PID, ogni A-modulo finitamente generato è somma diretta di moduli ciclici.*

Per i moduli, si possono ripetere le nozioni generali[1] già viste per gli spazi vettoriali e per le altre strutture algebriche; ad esempio, un *omomorfismo* di A-moduli (DEF)
è una applicazione lineare $f\colon M \to N$, ossia una funzione $f\colon M \to N$ tale che

$$f(m_1+m_2) = f(m_1) + f(m_2) \quad \forall\ m_1,m_2 \in M;$$
$$f(am) = af(m) \quad \forall\ a \in A,\ m \in M.$$

[1] ciò che gli inglesi chiamano *common nonsense*.

(DEF) Si definisce immediatamente la nozione di *sotto-A-modulo* N di un modulo M, come sottoinsieme $N \subseteq M$ che costituisce un A-modulo (cioè un sottogruppo (DEF) additivo di M, che sia chiuso rispetto al prodotto esterno); si parla poi di *laterali* di un sottomodulo (come insiemi del tipo $m+N$, con $m \in M$), e di modulo quoziente, come insieme delle classi di equivalenza nella famiglia dei laterali; si definisce quindi l'omomorfismo canonico

$$\pi \colon M \to {}^{M}\!/_{N},$$

che risulta essere suriettivo, ed il cui nucleo è proprio N, e così via.

Una scrittura del tipo

$$a_1 m_1 + a_2 m_2 + \cdots + a_n m_n,$$

(DEF) con $m_i \in M, a_i \in A \ \forall\ i = 1, 2, \ldots, n$, si dice una *combinazione lineare (c.l.)* (DEF) degli elementi $m_1, m_2, \ldots, m_n$ secondo i *coefficienti* $a_1, a_2, \ldots, a_n$. Si definiscono allora *generatori* di un A-modulo M, nel seguente modo: un insieme $\mathcal{G} \subseteq M$ si (DEF) dice un *insieme di generatori* di M (su A) se ogni elemento di M si può scrivere come combinazione lineare di elementi di $\mathcal{G}$ (a coefficienti in A); gli elementi di $\mathcal{G}$ (DEF) si diranno allora *generatori* di M (su A).

(DEF) Un modulo si dice *finitamente generato* se ammette un insieme di generatori finito.

2. Il modulo degli omomorfismi

DEFINIZIONE 2.1 Siano M, N due A-moduli; l'insieme degli omomorfismi da M in N si suole indicare con $\mathrm{Hom}_A(M, N)$; definiamo su di esso le due operazioni nel seguente modo

- per ogni $f, g \in \mathrm{Hom}_A(M, N)$, definiamo $f + g \in \mathrm{Hom}_A(M, N)$ ponendo

$$(f+g)(m) = f(m) + g(m) \quad \forall\ m \in M;$$

- per ogni $f \in \mathrm{Hom}_A(M, N)$, per ogni $a \in A$, definiamo $af \in \mathrm{Hom}_A(M, N)$ ponendo

$$(af)(m) = af(m) = f(am) \quad \forall\ m \in M;$$

si vede immediatamente che $\mathrm{Hom}_A(M, N)$, con le operazioni ora definite è un A-modulo.

OSSERVAZIONE 2.1 Supponiamo di avere tre A-moduli M, N, N', e supponiamo che esista un omomorfismo $u \colon N \to N'$; possiamo allora definire un omomorfismo $\bar{u} \colon \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M, N')$ con la legge $\bar{u}(f) = u \circ f \ \forall\ f \in \mathrm{Hom}_A(M, N)$.

Se invece si hanno tre A-moduli M, M', N, e $v \colon M \to M'$ è un omomorfismo, è possibile definire un omomorfismo $\bar{v} \colon \mathrm{Hom}_A(M', N) \to \mathrm{Hom}_A(M, N)$ ponendo $\bar{v}(f) = f \circ v \ \forall\ f \in \mathrm{Hom}_A(M', N)$.

In teoria delle categorie, $\mathrm{Hom}(\cdot, \cdot)$ è un *funtore*; le suddette relazioni tra gli omomorfismi fra le variabili (ossia i moduli) e gli omomorfismi tra gli Hom si esprimono dicendo che Hom è un operatore covariante sulla seconda variabile e controvariante sulla prima.

DEFINIZIONE 2.2 Se M è un A-modulo, $\mathrm{Hom}_A(M, A)$ prende il nome di *duale (algebrico)* di M, e si suole indicare con il simbolo M'.

OSSERVAZIONE 2.2 Se N è un A-modulo, allora $\mathrm{Hom}_A(A, N)$ è isomorfo ad N.

Dimostrazione. Fissato un omomorfismo $f \in \mathrm{Hom}_A(A, N)$, si ha $f(a) = af(1)\ \forall\ a \in A$. Quindi ogni omomorfismo di $\mathrm{Hom}_A(A, N)$ è determinato dal suo valore sull'unità di A; viene quindi naturale definire l'isomorfismo $\varphi\colon \mathrm{Hom}_A(A, N) \to N$ ponendo $\varphi(f) = f(1)\ \forall\ f \in \mathrm{Hom}_A(A, N)$. □

3. Operazioni con i moduli

Sia A un anello commutativo con unità e sia M un modulo.

Fissato un ideale $\mathfrak{a}$ di A, ed un sotto-A-modulo N di M, si vede facilmente che $\mathfrak{a}N$ è non solo un sotto-A-modulo, ma anche un $\mathfrak{a}$-modulo.

Fissati poi due sotto-A-moduli N_1, N_2 di M, anche $N_1 \cap N_2$ ed $N_1 + N_2$ risultano essere sotto-A-moduli di M. Possiamo poi considerare l'insieme

$$N_1 : N_2 = \{a \in A \mid a \cdot N_2 \subseteq N_1\},$$

che è un ideale di A. In particolare, si dice *annullatore* di N_2 l'ideale

$$0 : N_2 = \{a \in A \mid a \cdot n = 0\ \forall\ n \in N_2\};$$

se risulta $0 : N_2 = \{0\}$, N_2 si dice un modulo *fedele*; in tal caso, da $a \cdot N_2 = 0$ segue $a = 0$.

3.1. Prodotto diretto e somma diretta. Sia $\{M_i\}_{i \in I}$ una famiglia di A moduli; si definisce *prodotto diretto* dei moduli M_i l'insieme (DEF)

$$\prod_{i \in I} M_i = \{(\ldots, m_i, \ldots) \mid m_i \in M_i\ \forall\ i \in I\};$$

i suoi elementi vengono detti *uple*, e vengono indicati con il simbolo $(m_i)_{i \in I}$; m_i sarà allora la i-esima *componente* della upla $(m_i)_{i \in I}$.

Rigorosamente, il prodotto diretto si definisce come l'insieme delle funzioni $f\colon I \to \bigcup_{i \in I} M_i$ tali che $f(i) \in M_i\ \forall\ i \in I$. La definizione da noi data è equivalente a quella formale, facendo corrispondere alla funzione f l'elemento $\big(f(i)\big)_{i \in I}$, e viceversa associando all'elemento $(m_i)_{i \in I}$ la funzione f definita da $f(i) = m_i\ \forall\ i \in I$. La differenza è quindi per lo più una differenza formale, tranne in alcune questioni tecniche. La prossima osservazione spiega anche perché si preferisce in genere la definizione non rigorosa a quella formale.

Nel caso in cui I sia un insieme finito con n elementi (in particolare, per $I = \{1, 2, \ldots, n\}$), gli elementi di $M_1 \times M_2 \times \cdots \times M_n$ sono n-uple di elementi (sempre con la condizione $m_i \in M_i\ \forall\ i = 1, 2, \ldots, n$).

Osserviamo subito che $\prod_{i \in I} M_i$ è un A-modulo, dove le operazioni sono definite componente per componente.

Un importante sottomodulo di $\prod_{i \in I} M_i$ è la cosiddetta *somma diretta*, ossia il modulo $\oplus_{i \in I} M_i$ delle uple del tipo $(\ldots, m_i, \ldots)$, in cui solo un numero finito di componenti sono non nulle; ovviamente, nel caso finito si ha $\prod M_i = \oplus M_i$. Negli altri casi, la somma diretta è propriamente contenuta nel prodotto diretto; ad esempio, se $I = \mathbb{N}$ ed $M_n = A\ \forall\ n \in N$, il prodotto diretto è l'insieme delle successioni di elementi di A, mentre la somma diretta è l'insieme delle successioni definitivamente nulle.

Nel caso in cui M_i sia isomorfo ad A per ogni $i \in I$, la somma diretta si indicherà con il simbolo A^I o $A^{\oplus I}$, e verrà detta un *modulo libero*.

NOTAZIONI Nel caso in cui $M_i \cong A \ \forall \ i \in I$, gli elementi del prodotto diretto verranno indicati con notazione di n-uple ordinate, nella forma $(\dots, a_i, \dots)$, mentre gli elementi della somma diretta verranno indicati con notazione additiva, cioè nella forma $\sum a_i$; nel caso finito, la differenza è solo di notazione.

PROPOSIZIONE 3.1 *Ogni modulo è quoziente di un modulo libero.*

Dimostrazione. Sia M un A-modulo e sia $\mathcal{M} = \{m_i\}_{i \in I}$ una famiglia di generatori (potendo eventualmente anche essere $\mathcal{M} = M$). Consideriamo allora l'omomorfismo $\varphi\colon A^{\oplus I} \to M$ definito da

$$\sum a_i \mapsto \sum_{i \in I} a_i m_i;$$

osserviamo innanzi tutto che φ è ben definito, in quanto la somma ad ultimo membro è sempre una somma finita (in quanto gli m_i non nulli sono in numero finito). Si vede immediatamente che φ è suriettivo, poiché ogni elemento di M è nella forma $\sum_{i \in I} a_i m_i$; risulta allora $M \cong {}^{A^{\oplus I}}\!/_{\operatorname{Ker} \varphi}$, e si ha quindi la tesi. □

COROLLARIO 3.1 *Ogni A-modulo finitamente generato M è quoziente di A^n, dove n è il numero di generatori di M.*

3.2. Il Lemma di Nakayama.

LEMMA 3.1 (Nakayama) *Sia M un A-modulo finitamente generato e sia $\mathfrak{a}$ un ideale di A contenuto nel radicale di Jacobson $\mathcal{R}$ di A; se $\mathfrak{a}M = M$ allora $M = 0$.*

Dimostrazione. Supponiamo per assurdo che si abbia $M \neq 0$, e sia $\{m_1, m_2, \dots, m_n\}$ un insieme di generatori avente il minimo numero di elementi; essendo $m_1 \in M = \mathfrak{a}M$, è possibile trovare $a_1, a_2, \dots, a_n \in \mathfrak{a}$ tali che $m_1 = \sum_{i=1}^n a_i m_i$, e quindi

$$(1 - a_1)m_1 = \sum_{i=2}^{n} a_i m_i;$$

allora $a_1 \in \mathfrak{a} \subseteq \mathcal{R} = \{x \in A \mid 1 + \lambda x \in U \ \forall \ \lambda \in A\}$, e quindi $1 - a_1$ è invertibile; allora

$$m_1 = \sum_{i=2}^{n} a_i (1 - a_1)^{-1} m_i$$

è c.l. di $\{m_2, \dots, m_n\}$, e quindi $\{m_2, \dots, m_n\}$ è un insieme di generatori di M, con $n - 1$ generatori; ciò è assurdo per la minimalità del numero di generatori scelti inizialmente, e quindi $M = 0$. □

COROLLARIO 3.2 *Sia M un A-modulo finitamente generato e sia N un suo sottomodulo; sia poi $\mathfrak{a}$ un ideale di A contenuto in $\mathcal{R}$ tale che $M = \mathfrak{a}M + N$; allora si ha $M = N$.*

Dimostrazione. Dal fatto che M è f.g. segue che anche ${}^{M}\!/_{N}$ lo è; inoltre dall'ipotesi $M = \mathfrak{a}M + N$ segue che ${}^{M}\!/_{N} = \mathfrak{a}\,{}^{M}\!/_{N}$, e quindi, per il LEMMA di Nakayama, si ha ${}^{M}\!/_{N} = 0$, ossia $M = N$. □

OSSERVAZIONE 3.1 Sia A un anello locale ed $\mathfrak{m}$ il suo unico massimale; sappiamo allora che $k = {}^{A}\!/_{\mathfrak{m}}$ è un campo; inoltre, se M è un A-modulo, $\mathfrak{m}M$ è un sotto-A-modulo di M; ${}^{M}\!/_{\mathfrak{m}M}$ è ancora un A-modulo, ed è anche in ${}^{A}\!/_{\mathfrak{m}}$-modulo, ossia un k-spazio vettoriale.

Infatti, gli elementi di $A/\mathfrak{m}$ sono laterali del tipo $\bar{a} = a + \mathfrak{m}$, con $a \in A$; consideriamo allora un elemento $a+m \in \bar{a}$ (con $m \in \mathfrak{m}$), e sia poi $n+\mathfrak{m}M \in M/\mathfrak{m}M$ (con $n \in M$). Osserviamo che risulta

$$(a + m)(n + \mathfrak{m}M) = an + \mathfrak{m}M + nm + \mathfrak{m}M = an + \mathfrak{m}M,$$

con $an \in M$; allora, il prodotto del laterale $a + \mathfrak{m}$ per un elemento di $M/\mathfrak{m}M$ è indipendente dalla scelta del rappresentate del laterale (infatti m non compare nel risultato), ed è quindi un'operazione ben definita, che dà come risultato un elemento di $M/\mathfrak{m}M$; ha quindi senso definire il prodotto degli elementi di $A/\mathfrak{m}$ per gli elementi di $M/\mathfrak{m}M$, che dà a $M/\mathfrak{m}M$ la struttura di $A/\mathfrak{m}$-modulo.

Supponiamo ora che M sia un A-modulo finitamente generato; allora anche $M/\mathfrak{m}M$ è finitamente generato, ed è quindi un k-spazio vettoriale di dimensione finita n; esistono in particolare n laterali di $\mathfrak{m}M$ $x_1+\mathfrak{m}M$, $x_2+\mathfrak{m}M$, …, $x_n+\mathfrak{m}M$ tali che $\bar{x}_1$, $\bar{x}_2$, …, $\bar{x}_n$ generano $M/\mathfrak{m}M$ su k; proviamo che, scelto un rappresentate x_i in ogni laterale $\bar{x}_i$, M viene generato, come A-modulo, da x_1, x_2, …, x_n.

Sia N il sottomodulo di M generato da x_1, x_2, …, x_n; proviamo che $N = M$; sia $\bar{N}$ la classe di N in $M/\mathfrak{m}M$; per la scelta di N si ha $N = M/\mathfrak{m}M$, e quindi $\mathfrak{m}M + N = M$, ossia, per il Cor. 3.2, $M = N$.

4. Sequenze

Definizione 4.1 Sia A un anello commutativo con unità e sia $\{M_n\}$ una successione di A-moduli; supponiamo che fra gli elementi della successione agiscano degli omomorfismi $f_n\colon M_n \to M_{n+1}$; $\{M_n\}$ si dirà una *sequenza*, e verrà scritta nel seguente modo:

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} \dots \xrightarrow{f_n} M_{n+1} \xrightarrow{f_{n+1}} \dots$$

La sequenza $\{M_n\}$ si dirà un *complesso* se, per ogni $n \in \mathbb{N}$, $f_n \circ f_{n-1}$ è l'omomorfismo nullo, ossia se $\operatorname{Im} f_{n-1} \subseteq \operatorname{Ker} f_n$.

La sequenza $\{M_n\}$ si dirà una *sequenza esatta* se per ogni $n \in \mathbb{N}$ risulta $\operatorname{Im} f_{n-1} = \operatorname{Ker} f_n$.

Una sequenza si dirà *esatta a destra* se la sequenza ottenuta togliendo il primo modulo (ed il primo omomorfismo) è esatta. Analogamente, una sequenza finita si dirà *esatta a sinistra* se la sequenza ottenuta togliendo l'ultimo modulo (e l'ultimo omomorfismo) è esatta.

Notazioni Per semplicità di notazione, verrà soppressa l'indicazione dell'omomorfismo ove non sia necessario.

Esempio 4.1 Una sequenza del tipo

$$0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$$

si dice una *sequenza corta*; gli omomorfismi $0 \longrightarrow M'$ e $M'' \longrightarrow 0$ sono gli unici definibili; una tale sequenza è esatta se e solo se u è iniettiva, v è suriettiva e $\operatorname{Ker} v = \operatorname{Im} u$, condizione che equivale a $M/\operatorname{Im} u \cong M''$. (def)

Se manca l'iniettività di u, la sequenza è esatta solo a destra; se invece manca la suriettività di v, la sequenza è esatta solo a sinistra.

ESEMPIO 4.2 Una *sequenza corta spezzata* è una sequenza nella forma

$$0 \longrightarrow M' \xrightarrow{i} M' \oplus M'' \xrightarrow{p} M'' \longrightarrow 0,$$

dove i, p sono la iniezione e suriezione naturali definite da

$$\begin{aligned} i(m') &= (m', 0) \quad \forall\ m' \in M', \\ p(m', m'') &= m'' \quad \forall\ (m', m'') \in M' \oplus M''; \end{aligned}$$

ovviamente, la sequenza è esatta se e solo se lo è anche se letta al contrario (basta invertire i ruoli di M' ed M''); devono quindi esistere $q \in \mathrm{Hom}_A(M'', M' \oplus M'')$ e $j \in \mathrm{Hom}_A(M' \oplus M'', M')$ tali che $j \circ i = \mathrm{id}_{M'}$ e $p \circ q = \mathrm{id}_{M''}$.

Il precedente esempio può essere così generalizzato:

PROPOSIZIONE 4.1 *Sia* $0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{p} M'' \longrightarrow 0$ *una sequenza esatta; sono condizioni equivalenti:*

(1) *la sequenza è spezzata (ossia,* $M \cong M' \oplus M''$*);*
(2) *esiste* $j \in \mathrm{Hom}_A(M, M')$ *tale che* $j \circ i = \mathrm{id}_{M'}$*;*
(3) *esiste* $q \in \mathrm{Hom}_A(M'', M)$ *tale che* $p \circ q = \mathrm{id}_{M''}$*.*

Dimostrazione. Le implicazioni (**1**) $\Rightarrow$ (**2**) e (**1**) $\Rightarrow$ (**3**) sono state viste nel precedente esempio.

Proviamo ora che (**2**) $\Rightarrow$ (**1**). $K = \mathrm{Im}\, i$ e $H = \mathrm{Ker}\, j$ (dove j è l'omomorfismo della ipotesi **(2)**) sono sottomoduli di M.

Risulta $K \cap H = \{0\}$; infatti, se $m \in H \cap K$, deve esistere $m' \in M'$ tale che $m = i(m')$, ed inoltre $0 = j(m) = (j \circ i)(m') = m'$, e quindi $m' = 0$, da cui $m = 0$.

Risulta anche $M = K + H$; poiché banalmente $K + H \subseteq M$, occorre provare l'inclusione inversa; ora, se $m \in M$, si ha $(i \circ j)(m) = i\big(j(m)\big) \in K$; basta allora vedere che $m - (i \circ j)(m) \in H$; ma ciò segue dal fatto che $j\big(m - (i \circ j)(m)\big) = j(m) - j(i(j(m))) = j(m) - j(m) = 0$.

In definitiva, risulta $M = K \oplus H$; la tesi **(1)** è allora provata se proviamo che $K \cong M'$ e $H \cong M''$; ma il primo isomorfismo è ovvio, in quanto $i\colon M' \to M$ è iniettivo, la sua immagine è proprio K, e quindi $i\colon M' \to K$ è un isomorfismo; proviamo infine che $p_{|H}\colon H \to M''$ è un isomorfismo; per l'esattezza della sequenza, $\mathrm{Ker}\, p = \mathrm{Im}\, i$, e quindi $\mathrm{Ker}\, p_{|H} = \mathrm{Ker}\, p \cap H = \mathrm{Im}\, i \cap H = K \cap H = \{0\}$; quindi $p_{|H}$ è iniettiva; per la suriettività, fissiamo $m'' \in M''$; essendo p suriettiva, esiste $m \in M$ tale che $p(m) = m''$; ma $m = h + k$ con $h \in H, k \in K$, e quindi $p(m) = p(h) + p(k) = p(h)$ in quanto $k \in K = \mathrm{Im}\, i = \mathrm{Ker}\, p$; m'' è allora immagine secondo $p_{|H}$ di h; per l'arbitrarietà di $m'' \in M''$ si ha che ogni elemento di M'' proviene allora da un elemento $h \in H$, e quindi $p_{|H}$ è suriettiva; $p_{|H}$ è allora un isomorfismo, e ciò completa la dimostrazione.

Con tecnica analoga si prova che (**3**) $\Rightarrow$ (**1**). □

4.1. Esattezza e moduli Hom.

OSSERVAZIONE 4.1 Sia $0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{p} M'' \longrightarrow 0$ una sequenza corta e sia N un A-modulo; possiamo allora considerare la sequenza

$$0 \longrightarrow \mathrm{Hom}_A(M'', N) \xrightarrow{\bar{p}} \mathrm{Hom}_A(M, N) \xrightarrow{\bar{\imath}} \mathrm{Hom}_A(M', N) \longrightarrow 0$$

dove $\bar{\imath}$ e $\bar{p}$ sono definiti dalle leggi

$$\bar{\imath}(f) = f \circ i \qquad \forall\ f \in \mathrm{Hom}_A(M, N),$$
$$\bar{p}(g) = g \circ p \qquad \forall\ g \in \mathrm{Hom}_A(M'', N).$$

Possiamo anche considerare la sequenza

$$0 \longrightarrow \mathrm{Hom}_A(N, M') \xrightarrow{\tilde{\imath}} \mathrm{Hom}_A(N, M) \xrightarrow{\tilde{p}} \mathrm{Hom}_A(N, N'') \longrightarrow 0.$$

dove $\tilde{\imath}$ e $\tilde{p}$ sono definiti dalle leggi

$$\tilde{\imath}(f) = i \circ f \qquad \forall\ f \in \mathrm{Hom}_A(N, M'),$$
$$\tilde{p}(g) = p \circ g \qquad \forall\ g \in \mathrm{Hom}_A(N, M).$$

Sorge allora il problema di vedere quando le due sequenze sono esatte, in rapporto all'esattezza della sequenza originaria.

PROPOSIZIONE 4.2 *Sia*

(1) $$M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$$

una sequenza; condizione necessaria e sufficiente affinché la sequenza

(2) $$0 \longrightarrow \mathrm{Hom}_A(M'', N) \xrightarrow{\bar{v}} \mathrm{Hom}_A(M, N) \xrightarrow{\bar{u}} \mathrm{Hom}_A(M', N)$$

sia esatta per ogni A-modulo N è che sia esatta la sequenza (1).

Sufficienza. Supponiamo che sia esatta la (1), e proviamo l'esattezza di (2). Occorre provare che $\bar{v}$ è iniettiva e che $\mathrm{Im}\,\bar{v} = \mathrm{Ker}\,\bar{u}$.

Per l'esattezza di (1), v è suriettiva; quindi, per ogni $m'' \in M''$ esiste $m \in M$ tale che $v(m) = m''$; proviamo dunque la iniettività di $\bar{v}$; da $\bar{v}(f) = 0$ segue $f\big(v(m)\big) = 0\ \forall\ m \in M$, e quindi, per quanto appena osservato su v, $f(m'') = 0\ \forall\ m'' \in M''$; allora $f = 0$. Ciò prova l'iniettività di $\bar{v}$.

Proviamo ora che $\mathrm{Im}\,\bar{v} = \mathrm{Ker}\,\bar{u}$, provando le due inclusioni.

Per provare che $\mathrm{Im}\,\bar{v} \subseteq \mathrm{Ker}\,\bar{u}$ basta provare che $\bar{u} \circ \bar{v} = 0$; per ogni $f \in \mathrm{Hom}_A(M'', N)$, si ha $\bar{u} \circ \bar{v}(f) = f \circ v \circ u$; ma $v \circ u = 0$ in quanto la sequenza (1) è esatta, e quindi $f \circ v \circ u = 0$ per ogni $f \in \mathrm{Hom}_A(M'', N)$, ossia $\bar{u} \circ \bar{v}(f) = 0$ per ogni $f \in \mathrm{Hom}_A(M'', N)$, cioè $\bar{u} \circ \bar{v} = 0$, come volevasi.

Proviamo infine l'inclusione inversa; sia $f \in \mathrm{Ker}\,\bar{u}$; si ha allora $f \circ u = 0$, e quindi $\mathrm{Im}\,u \subseteq \mathrm{Ker}\,f$; ma $\mathrm{Im}\,u = \mathrm{Ker}\,v$, per l'esattezza di (1), e quindi $\mathrm{Ker}\,v \subseteq \mathrm{Ker}\,f$; esiste allora, per un COR. del TEOR. dell'omomorfismo, $g \in \mathrm{Hom}_A(M'', N)$ tale che $f = g \circ v$, ossia $f = \bar{v}(g)$ e quindi $f \in \mathrm{Im}\,\bar{v}$; per l'arbitrarietà della scelta di $f \in \mathrm{Ker}\,\bar{u}$ si ha allora $\mathrm{Ker}\,\bar{u} \subseteq \mathrm{Im}\,\bar{v}$, e quindi l'inclusione che mancava per completare la dimostrazione. □

Necessità. Proviamo che se (2) è esatta per ogni A-modulo N, allora (1) è pure esatta.

Cominciamo con il provare la suriettività di v; supponiamo per assurdo che v non sia suriettiva; si avrebbe allora $\mathrm{Im}\,v \subsetneq M''$, e pertanto l'omomorfismo canonico $g\colon M'' \to {}^{M''}\!/_{\mathrm{Im}\,v}$ sarebbe non nullo; si avrebbe però $g \circ v = 0$; prendendo $N = {}^{M''}\!/_{\mathrm{Im}\,v}$, si avrebbe allora che $\bar{v}$ non sarebbe iniettivo (in quanto $g \neq 0$ e $\bar{v}(g) = 0$), contro l'esattezza di (2); l'assurdo assicura allora la suriettività di v.

Proviamo ora che $\mathrm{Im}\,u = \mathrm{Ker}\,v$, provando le due inclusioni.

Proviamo che $\operatorname{Im} u \subseteq \operatorname{Ker} v$ provando che $v \circ u = 0$. Prendiamo $N = M''$; per l'esattezza di (2) si ha $\bar{u} \circ \bar{v} = 0$ e quindi in particolare $\bar{u} \circ \bar{v}(\mathrm{id}) = 0$, ossia $\mathrm{id} \circ v \circ u = 0$, ossia $v \circ u = 0$, come volevasi.

Proviamo infine l'inclusione inversa; consideriamo $N = {}^{M}\!/_{\operatorname{Im} u}$; l'omomorfismo canonico $\varphi\colon M \to {}^{M}\!/_{\operatorname{Im} u}$ sarà allora un elemento di $\operatorname{Hom}_A(M, N)$; si ha $\operatorname{Ker} \varphi = \operatorname{Im} u$ e risulta anche $\varphi \circ u = 0$, ossia $\varphi \in \operatorname{Ker} \bar{u} = \operatorname{Im} \bar{v}$; esiste allora $\psi \in \operatorname{Hom}_A(M'', N)$ tale che $\psi \circ v = \varphi$; quindi $\operatorname{Ker} v \subseteq \operatorname{Ker} \varphi = \operatorname{Im} u$, e quindi $\operatorname{Ker} v \subseteq \operatorname{Im} u$, che è l'inclusione che rimaneva per completare la dimostrazione. □

Analogamente si prova il seguente risultato.

PROPOSIZIONE 4.3 *Sia*

$$0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \tag{3}$$

una sequenza; condizione necessaria e sufficiente affinché la sequenza

$$0 \longrightarrow \operatorname{Hom}_A(N, M') \xrightarrow{\bar{u}} \operatorname{Hom}_A(N, M) \xrightarrow{\bar{v}} \operatorname{Hom}_A(N, M'')$$

sia esatta per ogni A-modulo N è che sia esatta la sequenza (3).

OSSERVAZIONE 4.2 In entrambi i casi, l'esattezza a destra non è garantita, nemmeno nel caso in cui la sequenza di partenza sia esatta sia a destra sia a sinistra. Infatti, nelle ipotesi della PROP. 4.2, dall'iniettività di u non segue la suriettività di $\bar{u}$; analogamente, nelle ipotesi della PROP. 4.3, dalla suriettività di v non segue l'iniettività di $\tilde{v}$. Vediamolo con un esempio.

ESEMPIO 4.3 Consideriamo la sequenza di $\mathbb{Z}$-moduli

$$0 \longrightarrow \mathbb{Z} \xrightarrow{i} \mathbb{Z} \xrightarrow{p} \mathbb{Z}_2 \longrightarrow 0,$$

dove i moduli sono gruppi additivi, p è la usuale applicazione che associa ad ogni intero il suo resto modulo 2, ed i è l'applicazione definita da $i(m) = 2m$; la sequenza è esatta. Possiamo poi considerare, componendo con $\operatorname{Hom}_{\mathbb{Z}}(\cdot, \mathbb{Z})$ e con $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}_2, \cdot)$, le sequenze

$$0 \longleftarrow \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \xleftarrow{\bar{\imath}} \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \xleftarrow{\bar{p}} \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}) \longleftarrow 0;$$

e

$$0 \longrightarrow \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}_2) \xrightarrow{\tilde{p}} \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}_2) \xrightarrow{\tilde{\imath}} \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}_2) \longrightarrow 0.$$

Entrambe le sequenze sono esatte a sinistra (ciò è garantito dalle precedenti PROP.). Vediamo ora che non sono esatte a destra.

Proviamo che $\bar{\imath}$ non è suriettiva; per definizione, $\bar{\imath}(f) = f \circ i$ e quindi $\bar{\imath}(f)(m) = f(2m)$ per ogni $m \in \mathbb{Z}$; l'identità, che appartiene all'insieme d'arrivo di $\bar{\imath}$, non è allora immagine secondo $\bar{\imath}$ di alcun elemento; quindi $\bar{\imath}$ non è suriettiva.

Proviamo che $\tilde{\imath}$ non è suriettiva. Osserviamo che, per definizione, $\tilde{\imath}(f) = i \circ f$, e quindi $\tilde{\imath}(f)(m) = 2f(m) = 0$ per ogni $m \in \mathbb{Z}$; quindi l'immagine di $\tilde{\imath}$ è costituita dal solo omomorfismo nullo; $\tilde{\imath}$ non è allora suriettiva.

4.2. Il Lemma del Serpente.

OSSERVAZIONE 4.3 Siano M, N due A-moduli e sia $f\colon M \to N$ un omomorfismo; la sequenza

$$0 \longrightarrow \operatorname{Ker} f \longrightarrow M \xrightarrow{f} N \longrightarrow \operatorname{CoKer} f \longrightarrow 0$$

è esatta.

Dimostrazione. Infatti, banalmente:

- $\operatorname{Ker} f \longrightarrow M$ è iniettiva, e la sua immagine è proprio $\operatorname{Ker} f$, ossia il nucleo dell'omomorfismo $M \xrightarrow{f} N$;
- $N \longrightarrow \operatorname{CoKer} f$ è suriettiva, e la sua immagine è proprio $\operatorname{CoKer} f$, ossia il nucleo dell'omomorfismo $\operatorname{CoKer} f \longrightarrow 0$.

□

LEMMA 4.1 (del serpente) *Se nel diagramma*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\
0 & \longrightarrow & N' & \xrightarrow{u'} & N & \xrightarrow{v'} & N'' & \longrightarrow & 0
\end{array}$$

le righe sono esatte ed i quadrati

$$\begin{array}{ccc} M' & \xrightarrow{u} & M \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} \\ N' & \xrightarrow{u'} & N \end{array}, \qquad \begin{array}{ccc} M & \xrightarrow{v} & M'' \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} \\ N & \xrightarrow{v'} & N'' \end{array}$$

commutano[2]*, allora dal diagramma*

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \operatorname{Ker} f & & \operatorname{Ker} g & & \operatorname{Ker} h & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\
0 & \longrightarrow & N' & \xrightarrow{u'} & N & \xrightarrow{v'} & N'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \operatorname{CoKer} f & & \operatorname{CoKer} g & & \operatorname{CoKer} h & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

è possibile costruire una sequenza esatta

$$0 \longrightarrow \operatorname{Ker} f \longrightarrow \operatorname{Ker} g \longrightarrow \operatorname{Ker} h \longrightarrow \operatorname{CoKer} f \longrightarrow \operatorname{CoKer} g \longrightarrow \operatorname{CoKer} h \longrightarrow 0$$

[2] cioè se $u' \circ f = g \circ u$ e $v' \circ g = h \circ v$.

Dimostrazione. Gli omomorfismi tra i nuclei sono banalmente definiti a partire dagli omomorfismi $M' \xrightarrow{u} M \xrightarrow{v} M''$; analogamente, a partire dagli omomorfismi $N' \xrightarrow{u'} N \xrightarrow{v'} N''$ si definiscono gli omomorfismi tra i conuclei; si vede subito che queste sottosequenze della sequenza della tesi sono esatte; rimane ora da verificare l'esattezza per l'omomorfismo $\operatorname{Ker} h \longrightarrow \operatorname{CoKer} f$. Chiamiamo d detto omomorfismo; vediamo innanzi tutto come è definito.

Fissiamo $m'' \in \operatorname{Ker} h$; per la suriettività di $v\colon M \to M''$, esiste $m \in M$ tale che $m'' = v(m)$; si ha quindi $h \circ v(m) = 0$; per la commutatività del quadrato di lati v, g, h, v', ciò equivale a $v' \circ g(m) = 0$, e quindi $g(m) \in \operatorname{Ker} v' = \operatorname{Im} u'$; esiste allora $n' \in N'$ tale che $u'(n') = g(m)$; possiamo allora definire $d(m'') = \bar{n'} \in \operatorname{CoKer} f$, dove $\bar{n'}$ è l'immagine di n' secondo l'omomorfismo $N' \longrightarrow \operatorname{CoKer} f$.

Per la commutatività dei quadrati, d è ben definita (non dipende cioè da m ed n') e rende inoltre esatta la sequenza. □

Corollario 4.1 *Siano M', M, M'' ed N', N, N'' degli A-moduli; supponiamo che le due sequenze*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0,$$

$$0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0,$$

siano esatte; supponiamo che esistano un omomorfismo $g\colon M \to N$ e due isomorfismi $f\colon M' \to N'$, $h\colon M'' \to N''$; se i quadrati commutano, allora g è un isomorfismo.

Dimostrazione. Consideriamo lo schema

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \operatorname{Ker} f & & \operatorname{Ker} g & & \operatorname{Ker} h & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\
 & & {\scriptstyle f}\downarrow & & {\scriptstyle g}\downarrow & & {\scriptstyle h}\downarrow & & \\
0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \operatorname{CoKer} f & & \operatorname{CoKer} g & & \operatorname{CoKer} h & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

sono banalmente soddisfatte le ipotesi del Lemma del serpente, che assicura che la sequenza

$$0 \longrightarrow \operatorname{Ker} f \longrightarrow \operatorname{Ker} g \longrightarrow \operatorname{Ker} h \longrightarrow \operatorname{CoKer} f \longrightarrow \operatorname{CoKer} g \longrightarrow \operatorname{CoKer} h \longrightarrow 0$$

è esatta; f, h sono isomorfismi e quindi risulta

$$\operatorname{Ker} f = \operatorname{Ker} h = \operatorname{CoKer} f = \operatorname{CoKer} h = 0;$$

l'esattezza della sequenza impone allora che sia $\operatorname{Ker} g = \operatorname{CoKer} g = 0$, e quindi g è un isomorfismo, ossia $M \cong N$. □

Osservazione 4.4 Ad esempio, il precedente Cor. è soddisfatto quando g è un'immersione.

5. Prodotto tensoriale di moduli

Definizione 5.1 Sia A un dominio e siano M, N, P A-moduli; $M \times N$ è ancora un A-modulo; una applicazione $g\colon M \times N \to P$ si dice *bilineare* se è lineare in entrambe le variabili, ossia se soddisfa le seguenti proprietà:

(1) $g(m_1 + m_2, n) = g(m_1, n) + g(m_2, n)$;
(2) $g(am, n) = ag(m, n)$;
(3) $g(m, n_1 + n_2) = g(m, n_1) + g(m, n_2)$;
(4) $g(m, an) = ag(m, n)$.

Fissati due A-moduli M, N, vogliamo ora costruire un A-modulo T ed una mappa bilineare $h\colon M \times N \to T$ tali che, per ogni A-modulo P e per ogni mappa bilineare $g\colon M \times N \to P$ sia possibile determinare un'unico omomorfismo $\varphi\colon T \to P$ tale che $g = \varphi \circ h$. La coppia (T, h) sarà allora *universale*; si vede facilmente che ogni oggetto universale è univocamente determinato, a meno di isomorfismi.

Consideriamo innanzi tutto il modulo libero

$$C = A^{\oplus(M \times N)};$$

i suoi elementi saranno del tipo

$$c = \sum_{i \in I} a_i (x_i, y_i)$$

dove $\{(x_i, y_i)\}_{i \in I}$ è un sottoinsieme finito di $M \times N$, ed $a_i \in A \ \forall\ i \in I$.

In particolare, consideriamo in C gli elementi del tipo

$$\begin{aligned}
&(x + x', y) - (x, y) - (x', y) && \forall\ x, x' \in M, y \in N \\
&(x, y + y) - (x, y) - (x, y') && \forall\ x \in M, y, y' \in N \\
&(ax, y) - a(x, y) && \forall\ a \in A, x \in M, y \in N \\
&(x, ay) - a(x, y) && \forall\ a \in A, x \in M, y \in N;
\end{aligned}$$

sia allora S il sottomodulo di C generato dagli elementi di questo tipo, e sia $T = {}^{C}\!/_{S}$. T prende il nome di *prodotto tensoriale di M, N in A*, e lo si denota con $M \otimes_A N$.

Studiamo ora il modulo T.

Sia $\pi\colon T \to C$ l'omomorfismo canonico; osserviamo che una base di C è formata da $\{(x, y) \mid x \in M, y \in N\}$; denotiamo ora con $x \otimes y$ l'immagine di (x, y) secondo π; ogni elemento di T si scriverà allora nella forma di somme finite del tipo

$$\sum_{i \in I} a_i (x_i \otimes y_i);$$

ne segue allora che $\{x \otimes y \mid x \in M, y \in N\}$ è un insieme di generatori di T; osserviamo che in generale l'insieme suddetto non è una base, poiché coppie distinte di

$M \times N$ possono avere la stessa immagine in T; infatti, per la definizione di S si ha che

$$(4) \quad (x + x') \otimes y = x \otimes y + x' \otimes y \qquad \forall\, x, x' \in M, y \in N$$

$$(5) \quad x \otimes (y + y') = x \otimes y + x \otimes y' \qquad \forall\, x \in M, y, y' \in N$$

$$(6) \quad (ax) \otimes y = a(x \otimes y) \qquad \forall\, a \in A, x \in M, y \in N$$

$$(7) \quad x \otimes (ay) = a(x \otimes y) \qquad \forall\, a \in A, x \in M, y \in N;$$

in particolare, dalle ultime due uguaglianze segue che

$$\sum_{i \in I} a_i(x_i \otimes y_i) = \sum_{i \in I} (a_i x_i) \otimes y_i = \sum_{i \in I} x_i \otimes (a_i y_i)$$

e quindi la decomposizione degli elementi di C come c.l. di generatori non è unica; l'insieme di generatori non forma quindi una base.

Dalle prime due eguaglianze segue inoltre che il *prodotto tensoriale* $\otimes$ è un'applicazione bilineare definita in $M \times N$ ed a valori in T; essa è proprio l'applicazione h che cercavamo; proviamo più in generale che (T, h) è l'oggetto universale che volevamo costruire.

Fissiamo dunque un A-modulo P e sia $g\colon M \times N \to P$ un'applicazione bilineare; proviamo che è possibile definire un'unico omomorfismo $f\colon T \to P$ tale che $g = f \circ h$.

Definiamo $f\colon T \to P$ considerando le immagini dei generatori; precisamente, poniamo

$$f(x \otimes y) = g(x, y)$$

per ogni $x \otimes y$ generatore di T; proviamo innanzi tutto che la definizione è corretta. Occorre provare che su ognuna delle relazioni (4)–(7) la f è coerente; proviamo la coerenza sulla relazione (4): si ha

$$\begin{aligned} f\big((x + x') \otimes y\big) &= g(x + x', y) = g(x, y) + g(x', y) = \\ &= f(x \otimes y) + f(x' \otimes y) = f(x \otimes y + x' \otimes y) \end{aligned}$$

e quindi, per transitività, la coerenza di f rispetto alla relazione (4). Analogamente si prova la coerenza con le restanti relazioni.

f è quindi ben definita; si ha poi banalmente $f \circ h(x, y) = f(x \otimes y) = g(x, y)$, e quindi f è proprio l'omomorfismo cercato (l'unicità segue dalla universalità dell'oggetto).

Osserviamo che in pratica ciò che è stato fatto è stato spostare la bilinearità dall'applicazione g al modulo T.

Vediamo ora alcune proprietà del prodotto tensoriale.

PROPOSIZIONE 5.1 *Siano M, N, Q A-moduli; valgono le seguenti proprietà:*

(1) $M \otimes_A N \cong N \otimes_A M$;
(2) $(M \otimes_A N) \otimes_A Q \cong M \otimes_A (N \otimes_A Q)$;
(3) $(M \oplus N) \otimes_A Q \cong (M \otimes_A Q) \oplus (N \otimes_A Q)$;
(4) $A \otimes_A M \cong M$.

Dimostrazione. Le dimostrazioni sono immediate; ci limitiamo a suggerire che l'isomorfismo del primo caso è $x \otimes y \mapsto y \otimes x$ e, nell'ultimo caso, l'isomorfismo è dato da $a \otimes m = 1 \otimes am \mapsto am$. □

Osservazione 5.1 Sfruttando le precedenti proprietà, è possibile vedere come cambia il prodotto tensoriale al cambiare del dominio A.

Consideriamo ad esempio il caso di $\mathbb{C}$, che può essere visto come spazio vettoriale sia su $\mathbb{C}$ (con dimensione 1) sia su $\mathbb{R}$ (con dimensione 2); vediamo che $\mathbb{C}\otimes_{\mathbb{C}}\mathbb{C}$ e $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}$ sono distinti. Infatti, per l'ultima proprietà, $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C} \cong \mathbb{C}$, mentre $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C}^2$, come prova il seguente ragionamento: essendo $\mathbb{C} \cong \mathbb{R} \oplus \mathbb{R}$, per la **(3)** si ha

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong (\mathbb{R} \oplus \mathbb{R}) \otimes_{\mathbb{R}} \mathbb{C} \cong (\mathbb{R} \otimes_{\mathbb{R}} \mathbb{C}) \oplus (\mathbb{R} \otimes_{\mathbb{R}} \mathbb{C}) \cong \mathbb{C} \oplus \mathbb{C} \cong \mathbb{C}^2.$$

Un altro modo di vedere il precedente fatto è il seguente; in $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$ si ha $\mathfrak{i} \otimes \mathfrak{i} = 1 \otimes -1 \mapsto -1$ (l'unità immaginaria, essendo in questo caso uno scalare, può "spostarsi" da un lato al'altro del prodotto scalare); nel caso in cui il prodotto tensoriale sia considerato rispetto ad $\mathbb{R}$ si ha invece $\mathfrak{i} \otimes \mathfrak{i} \mapsto (\mathfrak{i}, \mathfrak{i})$.

Osservazione 5.2 Se M, N sono moduli liberi, isomorfi rispettivamente ad A^m ed A^n, si ha $M \otimes_A N \cong A^{n \cdot m}$.

Proposizione 5.2 *Se M, N, P sono A-moduli, si ha*

$$\mathrm{Hom}_A(M \otimes_A N, P) \cong \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P))$$

Dimostrazione. Per la definizione di prodotto tensoriale si ha

$$\mathrm{Hom}_A(M \otimes_A N, P) \cong \mathrm{Bil}(M \times N, P),$$

dove il secondo insieme è il modulo degli operatori bilineari; la tesi è allora provata se proviamo che

$$\mathrm{Bil}(M \times N, P) \cong \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P)) \tag{8}$$

Fissiamo una mappa bilineare $g\colon M \times N \to P$; fissato allora $m \in M$, la mappa $g_m\colon N \to P$ definita da $g_m(n) = g(m, n)\ \forall\ n \in N$ è un omomorfismo; per ogni $g \in \mathrm{Bil}(M \times N, P)$ è quindi possibile definire la mappa $m \mapsto g_m$, che associa ad un elemento di M un elemento di $\mathrm{Hom}_A(N, P)$; la bilinearità degli operatori di $\mathrm{Bil}(M \times N, P)$ assicura che $m \mapsto g_m$ è un elemento di $\mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P))$; inoltre, si vede subito che la corrispondenza è una biiezione, e che quindi si ha la (8) che assicura la tesi. □

5.1. Prodotto tensoriale e sequenza esatte. Vediamo ora come si comporta il prodotto tensoriale rispetto all'esattezza a sinistra e a destra delle sequenze di moduli.

Proposizione 5.3 *Il prodotto tensoriale conserva l'esattezza a destra.*

Dimostrazione. Sia

$$E\colon 0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$$

una sequenza esatta; sia $E \otimes_A N$ la sequenza ottenuta componendo la sequenza precedente nel seguente modo:

$$E \otimes_A N\colon 0 \longrightarrow M' \otimes_A N \xrightarrow{u\otimes i} M \otimes_A N \xrightarrow{v\otimes i} M'' \otimes_A N \longrightarrow 0,$$

dove gli omomorfismi sono definiti da:

$$(u \otimes i)(m' \otimes n) = \big(u(m')\big) \otimes n \quad \forall\, m' \in M', n \in N,$$
$$(v \otimes i)(m \otimes n) = \big(v(m)\big) \otimes n \quad \forall\, m \in M, n \in N.$$

Proviamo che $E \otimes_A N$ è esatta a destra.

Ricordiamo che, componendo una sequenza esatta con l'operatore $\mathrm{Hom}(E, \cdot)$, si ottiene una sequenza esatta a sinistra; fissato allora un A-modulo P e considerando l'A-modulo $\mathrm{Hom}_A(N, P)$ si ha che la sequenza $\mathrm{Hom}_A(E, \mathrm{Hom}_A(N, P))$ è esatta a sinistra; ciò equivale alla esattezza a sinistra della sequenza $\mathrm{Hom}_A(E \otimes_A N, P)$ per ogni A-modulo P, e ciò implica che $E \otimes_A N$ è esatta a destra. □

Osservazione 5.3 Il prodotto tensoriale non conserva l'esattezza a sinistra, come dimostra il seguente esempio.

Esempio 5.1 Consideriamo la sequenza esatta

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \longrightarrow \mathbb{Z}_2 \longrightarrow 0.$$

Componendo mediante il prodotto tensoriale con $\mathbb{Z}_2$, si ottiene una sequenza

$$0 \longrightarrow \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2 \xrightarrow{\cdot 2} \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_2 \longrightarrow 0;$$

considerando le proprietà del prodotto tensoriale, si ha che la precedente sequenza è equivalente a

$$0 \longrightarrow \mathbb{Z}_2 \xrightarrow{\cdot 2} \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_2 \longrightarrow 0,$$

che non è una sequenza esatta, in quanto l'omomorfismo $\mathbb{Z}_2 \xrightarrow{\cdot 2} \mathbb{Z}_2$ non è iniettivo.

Definizione 5.2 Un A-modulo N si dice *piatto* se per ogni sequenza esatta E si ha che $E \otimes_A N$ è una sequenza esatta.

Osservazione 5.4 Come visto nel precedente esempio, ciò che in generale fa cadere l'esattezza a sinistra è il fatto che il prodotto tensoriale non conserva l'iniettività delle mappe; ne segue allora immediatamente la seguente caratterizzazione dei moduli piatti.

Teorema 5.1 *Le seguenti condizioni sono equivalenti:*

(1) *N è un modulo piatto;*
(2) *per ogni sequenza esatta corta E si ha che $E \otimes_A N$ è ancora esatta corta;*
(3) *per ogni omomorfismo $u\colon M' \to M$ iniettivo si ha che l'omomorfismo $u \otimes i\colon M' \otimes_A N \to M \otimes_A N$ è iniettivo.*

Dimostrazione. **(1)** implica **(2)** banalmente; **(3)** implica **(2)** poiché l'esattezza a destra è sempre verificata, e l'esattezza a sinistra è assicurata dal mantenimento dell'iniettività.

Proviamo ora che **(2)** implica **(3)**. Sia assegnato un omomorfismo $u\colon M' \to M$, iniettivo; possiamo allora costruire la sequenza

$$0 \longrightarrow M' \xrightarrow{u} M \longrightarrow {}^{M}\!/_{\mathrm{Im}\, u} \longrightarrow 0,$$

che è esatta corta; poiché vale la **(2)**, la sequenza

$$0 \longrightarrow M' \otimes_A N \xrightarrow{u \otimes i} M \otimes_A N \longrightarrow {}^{M}\!/_{\mathrm{Im}\, u} \otimes_A N \longrightarrow 0$$

è esatta, e quindi $u \otimes i$ è iniettiva, come volevasi.

Proviamo infine che **(2)** implica **(1)**. Consideriamo una sequenza esatta E e sia $M' \xrightarrow{u} M \xrightarrow{v} M''$ una sua sottosequenza; essa sarà ancora esatta. Detta v' la funzione avente la medesima legge di v, lo stesso dominio, e per codominio $\operatorname{Im} v$, si ha che la sequenza

$$M' \xrightarrow{u} M \xrightarrow{v'} \operatorname{Im} v \longrightarrow 0$$

è esatta, e quindi, tensorizzando, la sequenza

$$M' \otimes_A N \xrightarrow{u\otimes i} M \otimes_A N \xrightarrow{v'\otimes i} \operatorname{Im} v \otimes_A N \longrightarrow 0$$

è esatta.

Si ha $\operatorname{Im} v \subseteq M''$; sia $j\colon \operatorname{Im} v \to M''$ l'inclusione; essa è iniettiva; ma poiché **(2)** implica **(3)**, la tensorizzazione mantiene l'iniettività, e quindi $j \otimes i\colon \operatorname{Im} v \otimes_A N \to M'' \otimes_A N$ è ancora iniettiva; osserviamo inoltre che $(j \otimes i) \circ (v' \otimes i)\colon M \otimes_A N \to M''\otimes N$ restituisce proprio $v\otimes i$; l'iniettività di $j\otimes i$ assicura inoltre che $\operatorname{Ker}(v \otimes i) = \operatorname{Ker}(v' \otimes i)$; dall'esattezza di

$$M' \otimes_A N \longrightarrow M \otimes_A N \longrightarrow \operatorname{Im} v \otimes_A N \longrightarrow 0$$

segue allora l'esattezza di

$$M' \otimes_A N \longrightarrow M \otimes_A N \longrightarrow M'' \otimes_A N \longrightarrow 0,$$

ed in particolare l'esattezza di

$$M' \otimes_A N \longrightarrow M \otimes_A N \longrightarrow M'' \otimes_A N;$$

poiché il ragionamento può essere ripetuto per ogni sottosequenza di E e per ogni sequenza E, si ha in definitiva che il prodotto tensoriale conserva l'esattezza, e quindi N è un modulo piatto. □

PROPOSIZIONE 5.4 *Si provano immediatamente le seguenti proprietà:*

(1) *A è piatto su A;*
(2) *la somma diretta di moduli piatti è piatta;*
(3) *i moduli liberi sono piatti.*

CAPITOLO III

Anelli di frazioni

1. Definizioni

Al primo anno è stato visto come, dato un dominio d'integrità D, sia possibile costruire un campo $\mathbb{K}$, detto *campo delle frazioni* di D, in cui D si può immergere ed i cui elementi possono essere rappresentati nella forma $\frac{a}{b}$, con la condizione che $\frac{a}{b} = \frac{c}{d}$ se e solo se $ad - bc = 0$.

Vediamo ora come questo procedimento si possa generalizzare; precisamente, a partire da un arbitrario anello A, ed assegnato $S \subseteq A$, vediamo quando è possibile definire una estensione di A in cui gli elementi di S siano invertibili.

DEFINIZIONE 1.1 Sia A un anello commutativo con unità e sia $S \subseteq A$; diremo che S è un insieme *moltiplicativo* se $1 \in S$ e se da $a, b \in S$ segue $a \cdot b \in S$.

Consideriamo ora un anello A ed un suo insieme moltiplicativo S; definiamo, in $A \times S$, la relazione di equivalenza

$$(a, s) \sim (b, t) \iff \exists\ u \in S \mid u(at - bs) = 0.$$

Denotiamo poi con A_S l'insieme quoziente di $A \times S$ con $\sim$; i suoi elementi verranno indicati con simboli del tipo $\frac{a}{s}$, con $a \in A,\ s \in S$, e con la convenzione che

$$\frac{a}{s} = \frac{b}{t} \iff \exists\ u \in S \mid u(at - bs) = 0.$$

Osserviamo che è possibile definire una mappa $\varphi\colon A \to A_S$ con $\varphi(a) = \frac{a}{1}$; φ, in generale, non è iniettiva; infatti, $\varphi(a) = 0 \iff \exists\ u \in S \mid au = 0$.

L'insieme A_S si suole denotare anche con $S^{-1}A$, ed è detto l'*anello delle frazioni di S in A*. L'omomorfismo φ prende il nome di *omomorfismo canonico*.

PROPOSIZIONE 1.1 *L'anello delle frazioni di S in A e l'omomorfismo φ godono delle due seguenti proprietà:*

- *per ogni $s \in S$, esiste $(\varphi(s))^{-1}$;*
- *ogni elemento di S si può scrivere nella forma $\varphi(a)(\varphi(s))^{-1}$, con $a \in A$ ed $s \in S$.*

ESEMPIO 1.1 Vediamo ora un importante esempio di anello di frazioni.

Sia $\mathfrak{p}$ un ideale primo di un anello commutativo con unità A; si vede immediatamente che $S = A \setminus \mathfrak{p}$ è un insieme moltiplicativo di A; ha allora senso considerare l'anello delle frazioni $S^{-1}A$, che si suole anche indicare, in questo caso, con $A_{\mathfrak{p}}$.

Vediamo ora alcune proprietà di $A_{\mathfrak{p}}$. I suoi elementi sono nella forma $\frac{a}{s}$, con $a \in A$ ed $s \notin \mathfrak{p}$; si vede immediatamente che

- se $a \notin \mathfrak{p}$, $\dfrac{a}{s}$ è invertibile ed il suo inverso è $\dfrac{s}{a}$;
- se $a \in \mathfrak{p}$, $\dfrac{a}{s}$ non è invertibile;

ne segue allora, in particolare, che $\mathfrak{m} = \left\{ \dfrac{a}{s} \mid a \in \mathfrak{p}, s \notin \mathfrak{p} \right\}$ è un ideale massimale di $A_\mathfrak{p}$, ed è costituito da tutti e soli gli elementi non invertibili; $\mathfrak{m}$ è allora l'unico ideale massimale di $A_\mathfrak{p}$, che risulta quindi essere un anello locale; $\mathfrak{m}$ è detto *esteso*, e lo si denota anche con $\mathfrak{p}A_\mathfrak{p}$.

Osservazione 1.1 Il precedente esempio mostra anche perché gli anelli con un solo massimale vengano detti *locali*; se un anello locale nasce come anello delle frazioni $A_\mathfrak{p}$, in $A_\mathfrak{p}$ spariscono tutti gli ideali che non sono contenuti in $\mathfrak{p}$, permettendo di studiare, appunto *localmente* l'ideale $\mathfrak{p}$ (senza influenze dall'*esterno*).

Esempio 1.2 Consideriamo ora il caso $A = \mathbb{Z}$; sappiamo che gli ideali primi di $\mathbb{Z}$ sono generati da numeri primi p; per quanto visto nell'esempio precedente possiamo allora dire che $\mathbb{Z}_{(p)}$ è un anello locale, il cui ideale massimale è l'insieme delle frazioni il cui numeratore è multiplo di p.

Osservazione 1.2 Osserviamo che a priori non è escluso che $0 \in S$; in tal caso si ha però $S^{-1}A = \{0\}$, poichè, per ogni $a \in A$ si ha $\dfrac{a}{1} = \dfrac{0}{1}$ (basta prendere $u = 0 \in S$).

Esempio 1.3 Fissiamo $a \in A$, e consideriamo $S = \{a^n \mid n \in \mathbb{N}\}$; $S^{-1}A$ si suole in questi casi indicare con A_a; se a è nilpotente, si ha $0 \in S$, e quindi $A_a = \{0\}$; se invece a non è nilpotente, A_a sarà l'insieme delle frazioni aventi per denominatore una potenza di a. Ad esempio, se $A = \mathbb{Z}$ e $a = 10$, si ha

$$A_{10} = \left\{ \frac{m}{10^t} \mid m \in Z,\ t \in \mathbb{N} \right\},$$

ossia l'insieme dei numeri decimali finiti.

2. Proprietà degli anelli di frazioni

Osservazione 2.1 Supponiamo di avere un A-modulo M ed un insieme moltiplicativo S di A; possiamo allora definire

$$S^{-1}M = \left\{ \frac{m}{s} \mid m \in M, s \in S \right\}$$

con la solita condizione $\dfrac{m}{s} = \dfrac{n}{t} \iff \exists\ u \in S \mid u(mt - ns) = 0$.

Si vede immediatamente che $S^{-1}M$ è sia un A-modulo, sia un $S^{-1}A$-modulo; per quanto riguarda quest'ultimo fatto, basta osservare che

$$\frac{a}{s} \cdot \frac{m}{t} = \frac{am}{st}$$

è perfettamente definita (non dipende, cioè, dai rappresentanti scelti per le frazioni).

Osservazione 2.2 Supponiamo di avere una sequenza

$$M' \xrightarrow{f} M \xrightarrow{g} M'';$$

possiamo allora considerare la sequenza

$$S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M'',$$

dove i moduli possono essere visti sia come A-moduli, sia come $S^{-1}A$ moduli, e gli omomorfismi sono definiti da

$$\big(S^{-1}f\big)\left(\frac{m'}{s}\right) = \frac{f(m')}{s} \quad \forall\ m' \in M', s \in S$$

$$\big(S^{-1}g\big)\left(\frac{m}{s}\right) = \frac{g(m)}{s} \quad \forall\ m \in M, s \in S;$$

proviamo ora che, se la sequenza originaria è esatta, anche la sequenza degli anelli di frazioni è esatta.

Dimostrazione. Supponiamo che la sequenza originaria sia esatta; dalla iniettività di f e suriettività di g seguono immediatamente l'iniettività di $S^{-1}f$ e la suriettività di $S^{-1}g$. Proviamo ora che $\operatorname{Im}\big(S^{-1}f\big) = \operatorname{Ker}\big(S^{-1}g\big)$.

Si ha innanzi tutto $\Big(\big(S^{-1}g\big) \circ \big(S^{-1}f\big)\Big)\left(\dfrac{m'}{s}\right) = \dfrac{(g \circ f)(m')}{s} = 0$ per la esattezza della sequenza originaria, e quindi $\operatorname{Im}\big(S^{-1}f\big) \subseteq \operatorname{Ker}\big(S^{-1}g\big)$.

Viceversa, se $\dfrac{m}{s} \in S^{-1}M$ e $\big(S^{-1}g\big)\left(\dfrac{m}{s}\right) = 0$, esiste $u \in S$ per cui $ug(m) = 0$; ne segue $g(um) = 0$, e quindi $um \in \operatorname{Ker} g = \operatorname{Im} f$; esiste allora $m' \in M'$ per cui $f(m') = um$; quindi $\dfrac{m}{s} = \big(S^{-1}f\big)\left(\dfrac{m'}{s}\right)$, ossia $\dfrac{m}{s} \in \operatorname{Im}\big(S^{-1}f\big)$; si ha allora $\operatorname{Ker}\big(S^{-1}g\big) \subseteq \operatorname{Im}\big(S^{-1}f\big)$; dalle due inclusioni segue $\operatorname{Im}\big(S^{-1}f\big) = \operatorname{Ker}\big(S^{-1}g\big)$, ed in definitiva l'esattezza della sequenza. □

Osservazione 2.3 Si ha $S^{-1}M \cong S^{-1}A \otimes_A M$.

Dimostrazione. Gli elementi di $S^{-1}A \otimes_A M$ sono del tipo

$$\sum_{i \in I} \frac{a_i}{s_i} \otimes m_i,$$

dove la somma è estesa ad un insieme finito; fissato un tale elemento, sia $s = \prod_{i \in I} s_i$; l'elemento si potrà allora scrivere nella forma

$$\sum_{i \in I} \frac{t_i a_i}{s} \otimes m_i = \frac{\sum_{i \in I} (t_i a_i) \otimes m_i}{s} = \frac{1}{s} \otimes \sum_{i \in I} t_i a_i \otimes m_i;$$

ogni elemento di $S^{-1}A \otimes_A M$ si può allora scrivere nella forma $\dfrac{1}{s} \otimes m$ con $s \in S$ ed $m \in M$; viene allora naturale definire un omomorfismo con la legge $\dfrac{1}{s} \otimes m \mapsto \dfrac{m}{s}$; la mappa è banalmente suriettiva; è iniettiva poiché da $\dfrac{m}{s} = 0$ segue che esiste $u \in S$ per cui $um = 0$ e quindi

$$\frac{1}{s} \otimes m = \frac{u}{us} \otimes m = \frac{1}{us} \otimes (um) = 0;$$

la mappa è allora un isomorfismo e la tesi è così provata. □

Osservazione 2.4 La proprietà che gli anelli di frazioni conservano l'esattezza può allora essere enunciata dicendo che, se

$$M' \longrightarrow M \longrightarrow M''$$

è esatta, anche

$$S^{-1}A \otimes_A M' \longrightarrow S^{-1}A \otimes_A M \longrightarrow S^{-1}A \otimes_A M''$$

è esatta; in altre parole, $S^{-1}A$ è un A-modulo piatto su A.

OSSERVAZIONE 2.5 Se M, N sono A-moduli, si vede facilmente che

$$S^{-1}M \otimes_{S^{-1}A} S^{-1}N \cong S^{-1}(M \otimes_A N),$$

ossia la creazione di frazioni commuta con il prodotto tensoriale.

3. Localizzazione

Abbiamo visto che, fissato un ideale primo $\mathfrak{p}$ di un anello A commutativo con unità, nasce spontaneamente $A_\mathfrak{p}$, anello delle frazioni di $S = A \setminus \mathfrak{p}$ su A; il processo consistente nel dedurre proprietà di A a partire da proprietà da $A_\mathfrak{p}$ prende il nome di *localizzazione*; in particolare, una proprietà viene detta *locale* se viene conservata da questo processo.

Vediamo ora alcune importanti proprietà locali.

PROPOSIZIONE 3.1 *Sia M un A-modulo; le seguenti condizioni sono equivalenti:*

(1) *M è nullo;*
(2) *$M_\mathfrak{p}$ è nullo per ogni ideale primo $\mathfrak{p}$ di A;*
(3) *$M_\mathfrak{m}$ è nullo per ogni ideale massimale $\mathfrak{m}$ di A.*

Dimostrazione. **(1)** implica banalmente **(2)**, che implica banalmente **(3)**; basta allora provare che **(3)** implica **(1)**.

Supponiamo che valga le **(3)**, e supponiamo per assurdo che $M \neq 0$; esiste allora $m \in M$, con $m \neq 0$; consideriamo allora l'annullatore di m; essendo $m \neq 0$, si ha $\operatorname{ann}(m) \neq A$, ed esiste allora un massimale $\mathfrak{m}$ contenente $\operatorname{ann}(m)$; per l'ipotesi **(3)**, $M_\mathfrak{m} = 0$, e quindi $\dfrac{m}{1} \in M_\mathfrak{m}$ deve essere nullo; esiste allora $u \notin \mathfrak{m}$ per cui $um = 0$, e quindi $u \in \operatorname{ann}(m) \subseteq \mathfrak{m}$, assurdo. □

PROPOSIZIONE 3.2 *Siano M, N due A-moduli e sia $f\colon M \to N$ un omomorfismo; le seguenti condizioni sono equivalenti:*

(1) *f è iniettivo;*
(2) *$f_\mathfrak{p}\colon M_\mathfrak{p} \to N_\mathfrak{p}$ è iniettivo per ogni ideale primo $\mathfrak{p}$ di A;*
(3) *$f_\mathfrak{m}\colon M_\mathfrak{m} \to N_\mathfrak{m}$ è iniettivo per ogni ideale massimale $\mathfrak{m}$ di A.*

Dimostrazione. **(1)** implica **(2)**, poiché la localizzazione, come visto in generale per il passaggio agli anelli di frazioni, conserva l'esattezza delle sequenze e quindi, in particolare, l'iniettività degli omomorfismi; **(2)** implica **(3)** banalmente; per completare la dimostrazione rimane allora da provare che **(3)** implica **(1)**.

Poniamo $K = \operatorname{Ker} f$ e proviamo che $K = \{0\}$. La sequenza $K \xrightarrow{\mathrm{id}} M \xrightarrow{f} N$ è esatta, essendo $\operatorname{Im}\mathrm{id} = K = \operatorname{Ker} f$; allora anche le sequenze $K_\mathfrak{m} \xrightarrow{\mathrm{id}} M_\mathfrak{m} \xrightarrow{f_\mathfrak{m}} N_\mathfrak{m}$ sono esatte, per ogni massimale $\mathfrak{m}$; quindi, essendo $f_\mathfrak{m}\colon M_\mathfrak{m} \to N_\mathfrak{m}$ iniettivo per l'ipotesi **(3)**, dev'essere $K_\mathfrak{m} = 0$ per ogni massimale $\mathfrak{m}$; per la PROP. 3.1 si ha allora che $K = 0$, ossia l'iniettività di f. □

PROPOSIZIONE 3.3 *Siano M, N due A-moduli e sia $f\colon M \to N$ un omomorfismo; le seguenti condizioni sono equivalenti:*

(1) *f è suriettivo;*
(2) *$f_\mathfrak{p}\colon M_\mathfrak{p} \to N_\mathfrak{p}$ è suriettivo per ogni ideale primo $\mathfrak{p}$ di A;*
(3) *$f_\mathfrak{m}\colon M_\mathfrak{m} \to N_\mathfrak{m}$ è suriettivo per ogni ideale massimale $\mathfrak{m}$ di A.*

Dimostrazione. La dimostrazione è analoga alla dimostrazione della PROP. 3.2, ragionando però sulla sequenza $M \longrightarrow N \longrightarrow \mathrm{CoKer}\, f$. □

PROPOSIZIONE 3.4 *Sia M un A-modulo; le seguenti condizioni sono equivalenti:*

(1) *M è piatto come A-modulo;*
(2) *$M_{\mathfrak{p}}$ è piatto come $A_{\mathfrak{p}}$-modulo, per ogni ideale primo $\mathfrak{p}$ di A;*
(3) *$M_{\mathfrak{m}}$ è piatto come $A_{\mathfrak{m}}$-modulo, per ogni ideale massimale $\mathfrak{m}$ di A.*

Dimostrazione. Proviamo che **(1)** implica **(2)**; occorre provare che se la sequenza di $A_{\mathfrak{p}}$-moduli

$$N' \longrightarrow N \longrightarrow N'' \tag{9}$$

è esatta allora lo è anche la sequenza

$$N' \otimes_{A_{\mathfrak{p}}} M_{\mathfrak{p}} \longrightarrow N \otimes_{A_{\mathfrak{p}}} M_{\mathfrak{p}} \longrightarrow N'' \otimes_{A_{\mathfrak{p}}} M_{\mathfrak{p}}. \tag{10}$$

Per le proprietà del prodotto tensoriale si ha

$$N \otimes_{A_{\mathfrak{p}}} M_{\mathfrak{p}} \cong N \otimes_{A_{\mathfrak{p}}} (A_{\mathfrak{p}} \otimes_A M) \cong \big(N \otimes_{A_{\mathfrak{p}}} A_{\mathfrak{p}}\big) \otimes_A M \cong N \otimes_A M,$$

ed analogamente per N' ed N''; allora, la sequenza (10) si può scrivere

$$N' \otimes_A M \longrightarrow N \otimes_A M \longrightarrow N'' \otimes_A M,$$

che è esatta poiché M è per ipotesi piatto e la sequenza (9) è per ipotesi esatta.

(2) implica banalmente **(3)**; rimane allora da provare che **(3)** implica **(1)**. Basta provare che dall'iniettività di $N' \longrightarrow N$ segue l'iniettività di $N' \otimes_A M \longrightarrow N \otimes_A M$; supponiamo quindi che $N' \longrightarrow N$ sia iniettiva; poiché $A_{\mathfrak{m}}$ è un modulo piatto, anche $N' \otimes_A A_{\mathfrak{m}} \longrightarrow N \otimes_A A_{\mathfrak{m}}$ sarà iniettiva; per la **(3)** si ha allora la iniettività di

$$N' \otimes_A A_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}} \longrightarrow N \otimes_A A_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}},$$

ovvero di

$$N'_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}} \longrightarrow N_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}},$$

o ancora di

$$(N' \otimes_A M)_{\mathfrak{m}} \longrightarrow (N \otimes_A M)_{\mathfrak{m}};$$

per la PROP. 3.2 ne segue infine l'inettività di $N' \otimes_A M \longrightarrow N \otimes_A M$, che è quanto volevamo provare. □

4. Anelli di frazioni ed ideali estesi e contratti

OSSERVAZIONE 4.1 Sia A un anello commutativo con unità, S un suo insieme moltiplicativo, $\varphi\colon A \to S^{-1}A$ l'omomorfismo canonico.

Ad ogni ideale $\mathfrak{a}$ di A possiamo far corrispondere il suo esteso:

$$\mathfrak{a}^e = S^{-1}\mathfrak{a} = \left\{ \frac{a}{s} \mid a \in \mathfrak{a}, s \in S \right\}.$$

Viceversa, ad ogni ideale $\mathfrak{b}$ $S^{-1}A$ si può far corrispondere la propria contrazione:

$$\mathfrak{b}^c = \varphi^{-1}(\mathfrak{b}) = \{a \in A \mid \varphi(a) \in \mathfrak{b}\}.$$

Vediamo ora le principali proprietà delle corrispondenze $\mathfrak{a} \mapsto \mathfrak{a}^e \ \forall\ \mathfrak{a} \subseteq A$, $\mathfrak{b} \mapsto \mathfrak{b}^c \ \forall\ \mathfrak{b} \subseteq S^{-1}A$.

PROPRIETÀ degli ideali estesi e contratti in anelli di frazioni

(1) *ogni ideale di $S^{-1}A$ è un ideale esteso;*
(2) *l'esteso di un ideale $\mathfrak{a}$ di A coincide con $S^{-1}A$ se e solo se $\mathfrak{a} \cap S \neq \varnothing$;*
(3) *$\mathfrak{a}$ è un ideale contratto di A se e solo se nessun elemento di S è divisore dello zero in $A/\mathfrak{a}$;*
(4) *se $\mathfrak{p}$ è un primo di A che non interseca S, allora $S^{-1}\mathfrak{p}$ è un primo di $S^{-1}A$;*
(5) *se $\mathfrak{q}$ è un primo di $S^{-1}A$, allora $\mathfrak{q}^c$ è un primo di A che non interseca S;*
(6) *la legge $\mathfrak{a} \mapsto S^{-1}\mathfrak{a}$ conserva le somme finite, i prodotti finiti, le intersezioni finite ed i radicali; in altre parole, per ogni $\mathfrak{a}, \mathfrak{a}' \in A$ si ha:*
   (a) $S^{-1}(\mathfrak{a} + \mathfrak{a}') = S^{-1}\mathfrak{a} + S^{-1}\mathfrak{a}'$;
   (b) $S^{-1}(\mathfrak{a} \cdot \mathfrak{a}') = S^{-1}\mathfrak{a} \cdot S^{-1}\mathfrak{a}'$;
   (c) $S^{-1}(\mathfrak{a} \cap \mathfrak{a}') = S^{-1}\mathfrak{a} \cap S^{-1}\mathfrak{a}'$;
   (d) $S^{-1}(\mathfrak{r}(\mathfrak{a})) = \mathfrak{r}\big(S^{-1}\mathfrak{a}\big)$.

Dimostrazione. Proviamo la **(1)**.

Fissiamo un ideale $\mathfrak{b}$ di $S^{-1}A$; allora $\mathfrak{b}^c$ è un ideale di A; proviamo che $\mathfrak{b} = \mathfrak{b}^{ce}$; si ha sempre $\mathfrak{b}^{ce} \subseteq \mathfrak{b}$; proviamo il viceversa; sia $\dfrac{x}{s} \in \mathfrak{b}$; allora $\dfrac{x}{1} \in \mathfrak{b}$; ma $\dfrac{x}{1} = \varphi(x)$, e quindi $x \in \mathfrak{b}^c$, ossia $\dfrac{x}{1} \in \mathfrak{b}^{ce}$, e quindi $\dfrac{x}{s} \in \mathfrak{b}^{ce}$, come volevasi.

Proviamo la **(2)**.

Supponiamo in un primo tempo che $\mathfrak{a} \cap S \neq \varnothing$; sia $s \in \mathfrak{a} \cap S$; $\dfrac{s}{1} \in \mathfrak{a}^e$, ed è invertibile; quindi $\mathfrak{a}^e = S^{-1}A$.

Viceversa, supponiamo che $\mathfrak{a}^e = S^{-1}A$; allora $\dfrac{1}{1} \in \mathfrak{a}^e$, e quindi $\dfrac{1}{1} = \dfrac{a}{s}$ con $a \in \mathfrak{a}$ ed $s \in S$; esiste allora $u \in S$ per cui $u(s - a) = 0$, ossia $ua = us$; ma il primo membro sta in $\mathfrak{a}$ ed il secondo in S; allora $ua = us \in \mathfrak{a} \cap S$ e quindi $\mathfrak{a} \cap S \neq \varnothing$.

Proviamo la **(3)**.

Supponiamo in un primo tempo che $\mathfrak{a}$ sia contratto; fissiamo $s \in S$ e proviamo che s non è divisore dello zero in $A/\mathfrak{a}$, provando che da $\bar{s}\bar{x} = 0$ segue $\bar{x} = 0$; $\bar{s}\bar{x} = 0$ equivale a $sx \in \mathfrak{a}$; allora $\dfrac{x}{1} = \dfrac{sx}{s} \in \mathfrak{a}^e$, ossia $x \in \mathfrak{a}^{ec} = \mathfrak{a}$, ovvero $\bar{x} = 0$, come volevamo provare.

Viceversa, supponiamo che nessun elemento di S sia divisore dello zero in $A/\mathfrak{a}$; allora, da $sx \in \mathfrak{a}$, $s \in S$, segue $x \in \mathfrak{a}$; fissiamo ora $x \in \mathfrak{a}^{ec}$, e proviamo che $x \in \mathfrak{a}$; $x \in \mathfrak{a}^{ec}$ implica $\dfrac{x}{1} \in \mathfrak{a}^e$; esistono allora $y \in \mathfrak{a}$ ed $s \in S$ per cui $\dfrac{x}{1} = \dfrac{y}{s}$, e quindi esiste $u \in S$ per cui $u(sx - y) = 0$, ossia $usx = uy$; uy è un elemento di $\mathfrak{a}$, e quindi anche $usx \in \mathfrak{a}$; ma $us \in S$, e quindi, per quanto osservato, $x \in a$; è così provato che $\mathfrak{a}^{ec} \subseteq \mathfrak{a}$; poiché l'altra inclusione è sempre vera, si ha l'uguaglianza, e quindi $\mathfrak{a}$ è il contratto del proprio esteso, ovvero $\mathfrak{a}$ è un ideale contratto, come volevasi.

Proviamo la **(4)**.

Fissiamo due elementi $\dfrac{x}{s}, \dfrac{y}{t}$ di $S^{-1}A$ tali che $\dfrac{x}{s} \cdot \dfrac{y}{t} \in S^{-1}\mathfrak{p}$; allora $\dfrac{xy}{st} \in S^{-1}\mathfrak{p}$, ed esistono quindi $z \in \mathfrak{p}$, $u \in S$ tali che $\dfrac{xy}{st} = \dfrac{z}{u}$; esiste allora $v \in S$ per cui $v(uxy - stz) = 0$, ossia $vstz = uvxy$; il primo membro sta in $\mathfrak{p}$ (in quanto $z \in \mathfrak{p}$), e quindi anche $uvxy \in \mathfrak{p}$; poiché $\mathfrak{p} \cap S = \varnothing$, u, v ed uv non stanno in $\mathfrak{p}$, e deve quindi necessariamente $xy \in \mathfrak{p}$; ne segue allora che $x \in \mathfrak{p}$ oppure $y \in \mathfrak{p}$, ovvero $\dfrac{x}{s} \in S^{-1}\mathfrak{p}$

oppure $\frac{y}{t} \in S^{-1}\mathfrak{p}$, e quindi $S^{-1}\mathfrak{p}$ è primo.

Osserviamo che la condizione $\mathfrak{p} \cap S = \varnothing$ è essenziale, poiché altrimenti si avrebbe, per la **(2)**, $S^{-1}\mathfrak{p} = S^{-1}A$, che non è un ideale primo.

Proviamo ora la **(5)**.

Poniamo $\mathfrak{p} = \mathfrak{q}^c$; per **(1)**, tutti gli ideali di $S^{-1}A$ sono estesi, e quindi $\mathfrak{q} = \mathfrak{p}^e$; inoltre, essendo $\mathfrak{q} \neq S^{-1}A$, per **(2)** si ha $\mathfrak{p} \cap S = \varnothing$. Proviamo che $\mathfrak{p}$ è primo; fissiamo $x, y \in A$ tali che $x \cdot y \in \mathfrak{p}$; allora $\frac{x}{1} \cdot \frac{y}{1} \in \mathfrak{q}$; $\mathfrak{q}$ è primo, e quindi $\frac{x}{1} \in \mathfrak{q}$ o $\frac{y}{1} \in \mathfrak{q}$, ossia $x \in \mathfrak{p}$ o $y \in \mathfrak{p}$; quindi $\mathfrak{p}$ è primo.

Proviamo infine la **(6)**.

(6a) e **(6b)** sono sempre vere nel passaggio da un ideale all'ideale esteso; la **(6d)** è banale; proviamo allora **(6c)**. L'inclusione $S^{-1}(\mathfrak{a} \cap \mathfrak{a}') \subseteq S^{-1}\mathfrak{a} \cap S^{-1}\mathfrak{a}'$ è sempre vera; proviamo l'altra; fissiamo $z \in S^{-1}\mathfrak{a} \cap S^{-1}\mathfrak{a}'$; allora $z = \frac{x}{s} = \frac{y}{t}$ con $x \in \mathfrak{a}, y \in \mathfrak{a}'$, $s, t \in S$; esiste allora $u \in S$ per cui $u(tx - sy) = 0$, ossia $utx = usy$; il primo membro sta in $\mathfrak{a}$ ed il secondo in $\mathfrak{a}'$, e quindi entrambi stanno in $\mathfrak{a} \cap \mathfrak{a}'$; da $\frac{x}{s} = \frac{y}{t}$ segue anche che $\frac{utx}{uts} = \frac{usy}{uts}$; i denominatori appartengono ad $\mathfrak{a} \cap \mathfrak{a}'$, e quindi le frazioni stanno in $S^{-1}(\mathfrak{a} \cap \mathfrak{a}')$; ma le frazioni sono entrambe uguali a z, e quindi $z \in S^{-1}(\mathfrak{a} \cap \mathfrak{a}')$, come volevasi. □

COROLLARIO 4.1 *Sia $\mathcal{N}$ il nilradicale di A; allora $S^{-1}\mathcal{N}$ è il nilradicale di $S^{-1}A$*

OSSERVAZIONE 4.2 Le proprietà **(4)** e **(5)** suggeriscono che ci sia una corrispondenza biunivoca tra i primi di A che non intersecano S ed i primi di $S^{-1}A$; ciò è vero; per verificare ciò, basta provare che $\mathfrak{p} \mapsto \mathfrak{p}^e$ e $\mathfrak{q} \mapsto \mathfrak{q}^c$ sono l'una l'inversa dell'altra.

Si ha $\mathfrak{q} \mapsto \mathfrak{q}^c \mapsto \mathfrak{q}^{ce} = \mathfrak{q}$ per la **(1)**; rimane da provare che $\mathfrak{p} \mapsto \mathfrak{p}^e \mapsto \mathfrak{p}^{ec} = \mathfrak{p}$; per la **(3)**, basta verificare che gli elementi di S non dividono lo zero in $A/\mathfrak{p}$; ciò segue immediatamente dal fatto che $A/\mathfrak{p}$ è un dominio (essendo $\mathfrak{p}$ primo) e dal fatto che $\mathfrak{p} \cap S = \varnothing$; quindi gli elementi di S sono non nulli in $A/\mathfrak{p}$, e non dividono lo zero in quanto $A/\mathfrak{p}$ non ha divisori dello zero.

COROLLARIO 4.2 *Se $\mathfrak{p}$ è un primo di A, c'è una biiezione tra i primi di A contenenti $\mathfrak{p}$ e i primi di $A_\mathfrak{p}$.*

CAPITOLO IV

Anelli e moduli noetheriani ed artiniani

1. Prime definizioni e proprietà

DEFINIZIONE 1.1 Sia M un A-modulo.

Diremo che M soddisfa la *condizione delle catene ascendenti finite* (*c.c.a.f.*) se ogni catena ascendente di sottomoduli di M è finita.

Diremo che M soddisfa la *condizione delle catene discendenti finite* (*c.c.d.f.*) se ogni catena discendente di sottomoduli di M è finita.

DEFINIZIONE 1.2 Un modulo che soddisfa la c.c.a.f. si dice *noetheriano*; un modulo che soddisfa al c.c.d.f. si dice *artiniano*.

PROPOSIZIONE 1.1 *Sia M un A-modulo; le seguenti condizioni sono equivalenti:*

(1) *c.c.a.f.;*
(2) *ogni famiglia di sottomoduli ammette un massimale;*
(3) *ogni sottomodulo è finitamente generato.*

Dimostrazione. Proviamo che **(1)** implica **(2)**.

Sia $\mathcal{F}$ una famiglia di sottomoduli di M; fissiamo $M_0 \in \mathcal{F}$; se M_0 è massimale, la tesi è vera; altrimenti è possibile sceglie $M_1 \in \mathcal{F}$ con $M_0 \subset M_1$; ragionando analogamente su M_1, si ottiene o la massimalità di M_1 (e quindi la tesi), oppure l'esistenza di $M_2 \in \mathcal{F}$ con $M_1 \subset M_2$; così procedendo, nasce una catena $M_0 \subset M_1 \subset M_2 \subset \dots$; per la c.c.a.f., questa catena dovrà necessariamente avere termine, ossia esiste un massimale (che sarà l'ultimo elemento della catena).

Proviamo ora che **(2)** implica **(3)**.

Sia N un sottomodulo di M; proviamo che N è finitamente generato; consideriamo la famiglia $\mathcal{F}$ dei sottomoduli di N finitamente generati; per la **(2)**, $\mathcal{F}$ ha un massimale $\bar{N}$; la tesi è provata se proviamo che $\bar{N} = N$; supponiamo per assurdo che $\bar{N} \neq N$; esiste allora $n \in N \setminus \bar{N}$; detti $n_1, n_2, \dots, n_t$ i generatori di $\bar{N}$, si ha allora che $\langle n_1, n_2, \dots, n_t, n\rangle$ è un sottomodulo di N finitamente generato e contenente propriamente $\bar{N}$; ciò è assurdo per la massimalità di $\bar{N}$, e quindi $N = \bar{N}$ è finitamente generato.

Proviamo infine che **(3)** implica **(1)**.

Sia $M_0 \subseteq M_1 \subseteq \dots \subseteq M_n \subseteq \dots$ una catena ascendente di sottomoduli di M e sia $N = \bigcup_{n\in\mathbb{N}} M_n$; N è un sottomodulo di M, e quindi N è finitamente generato; siano $n_1, n_2, \dots, n_t$ i suoi generatori; per ogni $i = 1, 2, \dots, t$ è possibile trovare M_{j_i} per cui $n_i \in M_{j_i}$; detto allora $h = \max\{j_1, j_2, \dots, j_t\}$, per la crescenza della catena si ha $n_i \in M_h \ \forall\ i = 1, 2, \dots, n$, e quindi $N \subseteq M_h$; risulta allora

$$N \subseteq M_h \subseteq M_{h+1} \subseteq \dots \subseteq N,$$

ossia tutti i moduli sono uguali ad N, a partire dal modulo M_h; la catena $M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n \subseteq \ldots$ è allora finita, poiché distinti sono solo i primi h moduli. □

Osservazione 1.1 Ogni anello A è un A-modulo, ed i suoi sottomoduli sono gli ideali. La condizione **(3)** si legge allora dicendo che un anello A è noetheriano se e solo se i suoi ideali sono finitamente generati.

Per i moduli artiniani vale la seguente

Proposizione 1.2 *Sia M un A-modulo; le seguenti condizioni sono equivalenti:*

(1) *c.c.d.f.;*
(2) *ogni famiglia di sottomoduli ammette un minimale.*

Osservazione 1.2 Supponiamo che $A = \mathbb{Z}$; sappiamo che i $\mathbb{Z}$-moduli sono i gruppi abeliani.

Banalmente, ogni gruppo abeliano G finito è sia artiniano che noetheriano; se invece G è ciclico infinito (e quindi isomorfo a $\mathbb{Z}$), G è noetheriano, ma non artiniano. Consideriamo infatti ad esempio $\mathbb{Z}$ come $\mathbb{Z}$-modulo; poiché tutti gli ideali di $\mathbb{Z}$ sono finitamente generati (addirittura principali), $\mathbb{Z}$ è noetheriano; non è artiniano, poiché ad esempio la catena

$$(2) \supseteq (4) \supseteq (8) \supseteq \cdots \supseteq (2^n) \supseteq \ldots$$

è discendente non finita.

Portiamo ora un esempio di modulo artiniano non noetheriano. Fissiamo un numero primo p e consideriamo, in $\mathbb{C}$, per ogni $n \in \mathbb{N}$, l'insieme $G(p^n)$ delle radici p^n-esime dell'unità; esse formano un gruppo rispetto al prodotto; posto allora $G(p^\infty) = \bigcup_{n\in\mathbb{N}} G(p^n)$, si ha che $G(p^\infty)$ è un gruppo abeliano; si può provare che gli unici suoi sottogruppi sono proprio i gruppi $G(p^n)$. Allora, ogni catena discendente è finita, poiché sarà una sottocatena di

$$\langle 1\rangle \subseteq G(p) \subseteq G\big(p^2\big) \subseteq \cdots \subseteq G(p^n) \subseteq \ldots$$

e deve quindi terminare, al più con $\langle 1\rangle$; Questa stessa catena è ascendente non finita; $G(p^\infty)$ è allora artiniano, non noetheriano.

Proposizione 1.3 *Sia $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ una sequenza esatta; allora M è noetheriano (*risp. *artiniano) se e solo se M' ed M'' sono noetheriani (*risp. *artiniani).*

Dimostrazione. Proviamo il teorema nel caso di noetherianità dei moduli (per l'artinianità si ragionerà in maniera analoga).

Supponiamo che M sia noetheriano; allora M' è noetheriano, in quanto suo sottomodulo (per l'esattezza della sequenza); M'' è anche noetheriano; infatti, essendo la mappa $M \longrightarrow M''$, la controimmagine di una catena di sottomoduli di M'' è una catena di sottomoduli di M e moduli distinti hanno controimmagini distinte; in M la catena è finita, e quindi deve essere finita anche in M''.

Viceversa, supponiamo che M' ed M'' siano noetheriani; proviamo che M è noetheriano. Fissiamo una catena ascendente

$$M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n \subseteq \ldots$$

di sottomoduli di M; essendo $M'' \cong {}^{M}\!/_{M'}$, le immagini in M'' degli elementi della catena saranno insiemi del tipo ${}^{M_i + M'}\!/_{M'}$, e formeranno una catena ascendente di M''; per la noetherianità di M'', esiste un $\bar{n} \in \mathbb{N}$ tale che

$$M_n + M'/M' = M_{\bar{n}} + M'/M' \qquad \forall\, n \geq \bar{n};$$

per il Teor. dell'isomorfismo si ha poi

$$M_i + M'/M' \cong M_i/M_i \cap M' \qquad \forall\, i \in \mathbb{N},$$

e quindi

$$M_n/M_n \cap M' = M_{\bar{n}}/M_{\bar{n}} \cap M' \qquad \forall\, n \geq \bar{n};$$

ma gli insiemi $M_i \cap M'$ formano una catena di M', che è noetheriano, ed esiste allora $\bar{m} \in \mathbb{N}$ tale che

$$M_m \cap M' = M_{\bar{m}} \cap M' \qquad \forall\, m \geq \bar{m}.$$

Possiamo inoltre sceglie $\bar{m} \geq \bar{n}$[1]

Fissato $m \geq \bar{m}$, consideriamo le due sequenze

$$0 \longrightarrow M_{\bar{m}} \cap M' \longrightarrow M_{\bar{m}} \longrightarrow {}^{M_{\bar{m}}}\!/_{M_{\bar{m}} \cap M'} \longrightarrow 0,$$

$$0 \longrightarrow M_m \cap M' \longrightarrow M_m \longrightarrow {}^{M_m}\!/_{M_m \cap M'} \longrightarrow 0;$$

per la scelta di m si ha $M_m \cap M' = M_{\bar{m}} \cap M'$ e ${}^{M_{\bar{m}}}\!/_{M_{\bar{m}} \cap M'} = {}^{M_m}\!/_{M_m \cap M'}$; il Cor. 4.1, Cap. II del Lemma del serpente assicura allora che $M_{\bar{m}} = M_m$; questo vale per ogni $m \geq \bar{m}$, e quindi la catena dei moduli M_i è finita (termina al più con $M_{\bar{n}}$), che è quanto serviva per dimostrare la noetherianità di M. □

Esempio 1.1 Possiamo ora portare facilmente un esempio di gruppo non noetheriano e non artiniano; consideriamo infatti il gruppo

$$G = \left\{ \frac{m}{p^t} \mid m \in \mathbb{Z}, t \geq 0 \right\};$$

la sequenza

$$0 \longrightarrow \mathbb{Z} \longrightarrow G \longrightarrow G(p^\infty) \longrightarrow 0$$

è esatta; $\mathbb{Z}$ non è artiniano, $G(p^\infty)$ non è noetheriano, e quindi G non è né artiniano né noetheriano.

Osservazione 1.3 Una sequenza esatta spezzata

$$0 \longrightarrow M' \longrightarrow M' \oplus M'' \longrightarrow M'' \longrightarrow 0$$

gode della precedente proprietà; allora, un modulo M che è somma diretta di una famiglia $\{M_i\}_{i \in I}$ è noetheriano (*risp.* artiniano) se e solo se M_i è noetheriano (*risp.* artiniano) per ogni $i \in I$.

Corollario 1.1 *Sia A un anello noetheriano (*risp. *artiniano); se M è un modulo su A finitamente generato, allora M è noetheriano (*risp. *artiniano).*

[1] Nel caso $\bar{m} < \bar{n}$, basta prendere $\bar{m} = \bar{n}$.

Dimostrazione. Infatti, detti $m_1, m_2, \ldots, m_t$ i generatori di M, esiste un omomorfismo suriettivo $\varphi\colon A^t \to M$, con la legge $\varphi(a_1, a_2, \ldots, a_t) = \sum_{i=1}^{t} a_i m_i$; M è allora quoziente del modulo libero A^t, che è noetheriano (*risp.* artiniano), e quindi M è noetheriano (*risp.* artiniano). □

2. Serie di composizione

DEFINIZIONE 2.1 Sia M un modulo; una catena finita

$$(0) = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_t = M$$

si dice una *serie di composizione* se non è raffinabile, ovvero se non esistono sottomoduli di M compresi fra M_{i-1} ed M_i, per ogni $i = 1, 2, \ldots, t$, o, equivalentemente, se tutti i quozienti M_i/M_{i-1} sono semplici, ovvero privi di sottomoduli propri non banali.

NOTAZIONI Per ogni modulo M che possegga una serie di composizione, denotiamo con $l(M)$ la minima lunghezza di una serie di composizione di M.

PROPOSIZIONE 2.1 *Sia M un modulo; supponiamo che M possieda una serie di composizione; allora:*

(1) *per ogni sottomodulo N di M si ha $l(N) \leq l(M)$, ed $l(N) = l(M)$ se e solo se $N = M$;*
(2) *ogni catena di sottomoduli di M ha lunghezza non maggiore di $l(M)$;*
(3) *ogni serie di composizione ha lunghezza $l(M)$;*
(4) *ogni catena di sottomoduli di M si può raffinare ad una serie di composizione;*
(5) *una catena è una serie di composizione se e solo se ha lunghezza $l(M)$.*

Dimostrazione. Sia $t = l(M)$ la minima lunghezza di una serie di composizione di M.

Proviamo innanzi tutto che, per ogni sottomodulo N di M, si ha $l(N) \leq l(M)$. Fissiamo un sottomodulo N di M; sia

$$(0) = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_t = M$$

una serie di composizione di M di lunghezza minima; allora, la catena

$$(0) = M_0 \cap N \subseteq M_1 \cap N \subseteq \cdots \subseteq M_t \cap N = N \tag{11}$$

è una serie di composizione di N, ed ha lunghezza non maggiore di t (poiché non può avere più moduli della serie di composizione originaria); allora la minima lunghezza di una serie di composizione di N sarà non maggiore della lunghezza di (11), che a sua volta è non maggiore di $t = l(M)$; in definitiva, $l(N) \leq l(M)$ (potendo anche essere $l(N) < l(M)$, se esiste un i per cui $M_i \cap N = M_{i+1} \cap N$).

Proviamo ora che, se $l(N) = l(M)$, allora $N = M$. Per quanto appena osservato, $l(N) = l(M)$ implica che $M_i \cap N \neq M_{i+1} \cap N \ \forall\ i = 0, 1, \ldots, t-1$; si ha quindi $M_{i+1} \cap N/M_i \cap N = M_{i+1}/M_i \ \forall\ i = 0, 1, \ldots, t-1$; proviamo per induzione che da questo segue $M_i \cap N = M_i \ \forall\ i = 0, 1, \ldots, t$, ragionando per induzione.

Se $i = 0$, si ha $M_0 = M_0 \cap N = (0)$; allora $M_1 \cap N/(0) = M_1/(0)$, ossia $M_1 \cap N = M_1$; l'uguaglianza è allora vera nei casi $i = 0$ $i = 1$.

Supponiamo ora che sia $i > 1$ e che $M_{i-1} = M_{i-1} \cap N$; proviamo che $M_i = M_i \cap N$; confrontiamo le sequenze

$$0 \longrightarrow M_{i-1} \longrightarrow M_i \longrightarrow {}^{M_i}\!/_{M_{i-1}} \longrightarrow 0,$$
$$0 \longrightarrow M_{i-1} \cap N \longrightarrow M_i \cap N \longrightarrow {}^{M_i \cap N}\!/_{M_{i-1} \cap N} \longrightarrow 0;$$

gli estremi sono uguali (il primo per ipotesi induttiva, il secondo per quanto visto sopra), e i moduli di mezzo soddisfano l'inclusione $M_i \cap N \subseteq M_i$; ne segue allora (Cor. 4.1, Cap. II del Lemma del serpente) $M_i \cap N = M_i$.

È quindi verificato per induzione che $M_i = M_i \cap N$ per ogni $i = 1, 2, \ldots, t$; in particolare, per $i = t$ si ha $N = M_t \cap N = M_t = M$, ossia $N = M$.

Questo prova la **(1)**. Proviamo ora le **(2)** e **(3)**.

Fissiamo una catena finita

$$(0) = M_0 \subset M_1 \subset \cdots \subset M_k = M;$$

di sottomoduli di M; per quanto visto sopra, risulta

$$l(M) > l(M_{k-1}) > \cdots > l(M_1) > l(M_0) = 0;$$

poichè ogni lunghezza è un numero intero, le maggiorazioni strette assicurano che $t = l(M) \geq k$ (ogni diseguaglianza stretta fra interi aggiunge almeno un'unità, e vi sono k diseguaglianze strette); quindi $k \leq l(M)$, ovvero la catena ha lunghezza non maggiore di $l(M)$; ciò prova la **(2)**; ne segue anche che non possono esistere catene infinite di sottomoduli di M (poiché da una catena infinita se ne potrebbe estrarre una finita di lunghezza maggiore di $l(M)$, contro il fatto che ogni catena finita ha lunghezza non maggiore di $l(M)$); inoltre, se la catena fissata è una serie di composizione, essa deve avere almeno lunghezza $t = l(M)$ (che era la lunghezza minima di una serie di composizione); quindi $k \geq t$ per le serie di composizione; ma $k \leq t$ sempre, e quindi $t = k$ per le serie di composizione, ovvero ogni serie di composizione ha lunghezza $t = l(M)$; ciò prova la **(3)**.

Proviamo infine le **(4)** e **(5)**.

Fissiamo una catena

$$(0) = M_0 \subset M_1 \subset \cdots \subset M_k = M;$$

di sottomoduli di M (che abbiamo appena vista essere necessariamente finita) e proviamo che la si può raffinare ad una serie di composizione; se la catena è una serie di composizione, abbiamo finito; supponiamo allora che la catena non sia una serie di composizione; ciò vuol dire che almeno un quoziente ${}^{M_{i+1}}\!/_{M_i}$ non è semplice; equivalentemente, ciò vuol dire che si possono intercalare moduli tra M_i ed M_{i+1} per qualche $i = 1, 2, \ldots, k$; l'operazione di intercalare moduli allunga la catena: la sua lunghezza passerà da k a $k + 1$; il procedimento termina qui se la nuova catena è una serie di composizione; se non si è ancora ottenuta una serie di composizione, allora il ragionamento può essere ripetuto, e la catena si allungherà ancora, passando da $k+1$ a $k+2$ moduli; il procedimento continua finché la catena ottenuta aggiungendo moduli non sia una serie di composizione; osserviamo che il procedimento ha termine, poiché ogni catena ha lunghezza non maggiore di t, e

quindi il procedimento termina dopo al più $t-k$ passi: abbiamo quindi provato che ogni catena si può raffinare, aggiungendo al più $t-k$ moduli, ad una serie di composizione (punto **(4)**); dal procedimento seguito per raffinare la catena segue anche che la catena non è raffinabile se e solo se ha lunghezza t, ossia la catena è una serie di composizione se e solo se ha lunghezza t (punto **(5)**).

La tesi è allora completamente provata. □

DEFINIZIONE 2.2 Se M ammette una serie di composizione, M si dice *di lunghezza finita*, e la lunghezza di una sua qualunque serie di composizione si dirà *lunghezza* di M, e verrà indicata con il simbolo $l(M)$.

PROPOSIZIONE 2.2 *Un modulo M ha lunghezza finita se e solo se è noetheriano e artiniano.*

Dimostrazione. Se M ha lunghezza finita, ogni catena di M è finita; allora M soddisfa sia la c.c.d.f. che la c.c.a.f., ed è quindi sia noetheriano, sia artiniano.

Viceversa, supponiamo che M sia noetheriano ed artiniano; per la noetherianità, esiste M_1 sottomodulo massimale di M; anche M_1 è noetheriano, ed esiste quindi M_2 sottomodulo massimale di M_1; così procedendo, si crea una catena discendente di sottomoduli di M, non raffinabile; per l'artinianità di M, la catena è finita, ed è quindi una serie di composizione; M ha allora lunghezza finita. □

OSSERVAZIONE 2.1 Se $A=\mathbb{K}$ è un campo, ogni suo modulo V è un $\mathbb{K}$-spazio vettoriale; in tal caso, le condizioni c.c.a.f., c.c.d.f., V di lunghezza finita, sono equivalenti, e corrispondo alla condizione che V sia di dimensione finita.

COROLLARIO 2.1 *Sia A un anello; se (0) è prodotto di un numero finito di massimali $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_t$, allora A è noetheriano se e solo se è artiniano.*

Dimostrazione. Consideriamo la catena

$$A \supset \mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \cdots \supset \mathfrak{m}_1 \ldots \mathfrak{m}_t = (0);$$

il quoziente $A/\mathfrak{m}_1$ è un campo, ed è quindi semplice; $\mathfrak{m}_1/\mathfrak{m}_1\mathfrak{m}_2$ è un $A/\mathfrak{m}_2$-spazio vettoriale; $\mathfrak{m}_1\mathfrak{m}_2/\mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3$ è un $A/\mathfrak{m}_3$-spazio vettoriale, e così via; negli spazi vettoriali c.c.d.f. e c.c.a.f. coincidono, ovvero gli spazi vettoriali sono noetheriani se e solo se sono artiniani.

A è noetheriano se e solo se ogni quoziente $\mathfrak{m}_1 \cdots \mathfrak{m}_i/\mathfrak{m}_1 \cdots \mathfrak{m}_i\mathfrak{m}_{i+1}$ è noetheriano; i quozienti, in quanto spazi vettoriali, sono noetheriani se e solo se sono artiniani; ma i quozienti sono artiniani se e solo se A è artiniano; quindi A è noetheriano se e solo se è artiniano. □

3. Proprietà degli anelli noetheriani

OSSERVAZIONE 3.1 Abbiamo già osservato che, se A è un anello noetheriano, allora i suoi quozienti $A/\mathfrak{a}$ sono noetheriano; si prova anche facilmente che gli anelli di frazioni $S^{-1}A$ (con S insieme moltiplicativo di A) sono noetheriano.

TEOREMA 3.1 (della base di Hilbert) *Se A è noetheriano, allora $A[x]$ è noetheriano.*

Dimostrazione. Per ogni polinomio $f \in A[x]$, chiameremo *coefficiente direttivo* di f il coefficiente del monomio di grado massimo.

Fissiamo un ideale $\mathfrak{a}$ di $A[x]$; proviamo che è finitamente generato; consideriamo l'insieme I dei coefficienti direttivi degli elementi di $\mathfrak{a}$; I è un ideale di A, che è noetheriano; quindi I è finitamente generato; sia $\{a_1, a_2, \ldots, a_t\}$ un insieme di generatori di I; per la definizione di I, esistono $f_1, f_2, \ldots, f_t \in \mathfrak{a}$ tali che a_i è il coefficiente direttivo di f_i.

Per ogni $i = 1, 2, \ldots, t$, poniamo $n_i = \deg f_i$, e sia $n = \max\{n_1, n_2, \ldots, n_t\}$; consideriamo in $A[x]$ i polinomi $1, x, \ldots, x^{n-1}$, e sia M l'insieme delle loro combinazioni lineari (ossia dei polinomi di grado minore di n); M è un A-modulo, finitamente generato. Sia poi $\mathfrak{a}'$ l'ideale generato dagli f_i; per provare che $\mathfrak{a}$ è finitamente generato, basta provare che $\mathfrak{a} = \mathfrak{a}' + (\mathfrak{a} \cap M)$; infatti, in tal caso $\mathfrak{a}$ sarà somma di ideali finitamente generati, e sarà quindi finitamente generato: un suo insieme di generatori sarà costituito dall'unione di un insieme di generatori di $\mathfrak{a}'$ e di un insieme di generatori di $\mathfrak{a} \cap M$. Proviamo dunque che $\mathfrak{a} = \mathfrak{a}' + (\mathfrak{a} \cap M)$; poiché l'inclusione $\mathfrak{a}' + (\mathfrak{a} \cap M) \subseteq \mathfrak{a}$ è banalmente verificata, basta provare che $\mathfrak{a} \subseteq \mathfrak{a}' + (\mathfrak{a} \cap M)$.

Sia $f \in \mathfrak{a}$; proviamo che $f \in \mathfrak{a}' + (\mathfrak{a} \cap M)$, ragionando per induzione su $\deg f$.

Se $\deg f \leq n - 1$, si ha $f \in M$; ma $f \in \mathfrak{a}$, e quindi $f \in \mathfrak{a} \cap M \subseteq \mathfrak{a}' + (\mathfrak{a} \cap M)$ (base dell'induzione).

Supponiamo ora che $d = \deg f \geq n$, e che ogni polinomio di $\mathfrak{a}$ di grado minore di d stia in $\mathfrak{a}' + (\mathfrak{a} \cap M)$; proviamo che $f \in \mathfrak{a}' + (\mathfrak{a} \cap M)$. Sia a il coefficiente direttivo di f; per definizione di I, si ha $a \in I$, e quindi esistono $b_1, b_2, \ldots, b_t \in A$ tali che

$$a = \sum_{i=1}^{t} b_i a_i;$$

allora, il polinomio $g = f - \sum_{i=1}^{t} b_i f_i$ ha grado minore di d; essendo poi $\mathfrak{a}$ un ideale e $f_1, f_2, \ldots, f_t, f \in \mathfrak{a}$, si ha $g \in \mathfrak{a}$; per ipotesi induttiva si ha allora $g \in \mathfrak{a}' + (\mathfrak{a} \cap M)$, e quindi $f = g + \sum_{i=1}^{t} b_i f_i \in \mathfrak{a}' + (\mathfrak{a} \cap M) + \mathfrak{a}' \subseteq \mathfrak{a}' + (\mathfrak{a} \cap M)$, che è quanto volevamo provare.

Si ha allora $\mathfrak{a} \subseteq \mathfrak{a}' + (\mathfrak{a} \cap M)$; l'altra inclusione è banale, e vale allora l'uguaglianza che, come già osservato, prova che $\mathfrak{a}$ è finitamente generato; per l'arbitrarietà di $\mathfrak{a}$ si ha allora che $A[x]$ è noetheriano, ossia la tesi. □

PROPOSIZIONE 3.1 *Ogni ideale $\mathfrak{a}$ un anello noetheriano A contiene una potenza del proprio radicale.*

Dimostrazione. Il radicale di $\mathfrak{a}$ è ancora un ideale di A, ed è allora finitamente generato; sia $\{x_1, x_2, \ldots, x_k\}$ un insieme di generatori di $\mathfrak{r}(\mathfrak{a})$; per definizione di radicale, in corrispondenza ad ogni x_i è possibile determinare $n_i \in \mathbb{N}$ tale che ${x_i}^{n_i} \in \mathfrak{a}$; poniamo ora $m = \sum_{i=1}^{k} (n_i - 1) + 1$ e consideriamo l'insieme

$$(\mathfrak{r}(\mathfrak{a}))^m = \left\{ {x_1}^{r_1} {x_2}^{r_2} \ldots {x_k}^{r_k} \mid \sum_{i=1}^{k} r_i = m \right\};$$

preso un suo elemento ${x_1}^{r_1} {x_2}^{r_2} \ldots {x_k}^{r_k}$, esiste $r_{\bar{\imath}} \geq n_{\bar{\imath}}$ (da $r_i < n_i \ \forall\, i = 1, 2, \ldots, k$ seguirebbe $\sum_{i=1}^{k} r_i < m$); allora ${x_{\bar{\imath}}}^{r_{\bar{\imath}}} \in \mathfrak{a}$, e quindi ${x_1}^{r_1} {x_2}^{r_2} \ldots {x_k}^{r_k} \in \mathfrak{a}$; il ragionamento vale per ogni elemento di $(\mathfrak{r}(\mathfrak{a}))^m$, e quindi $(\mathfrak{r}(\mathfrak{a}))^m \subseteq \mathfrak{a}$ (si vede anzi facilmente che m è la minima potenza per cui ciò accade). □

COROLLARIO 3.1 *In ogni anello noetheriano il nilradicale è nilpotente.*

Dimostrazione. Per definizione il nilradicale $\mathcal{N}$ è il radicale di (0); per la precedente PROP., esiste una potenza m di $\mathcal{N}$ che è contenuta in (0); d'altra parte (0) è contenuto in ogni ideale, e quindi $\mathcal{N}^m = (0)$, cioè il nilradicale è nilpotente. □

TEOREMA 3.2 (dell'intersezione di Krull) *Sia A un anello noetheriano e sia $\mathfrak{a}$ un ideale di A; posto $\mathfrak{b} = \bigcap_{n\in\mathbb{N}} \mathfrak{a}^n$, si ha $\mathfrak{ab} = \mathfrak{b}$; inoltre, se $\mathfrak{a} \subseteq \mathcal{R}$, allora $\mathfrak{b} = (0)$.*

Dimostrazione. Essendo A noetheriano, $\mathfrak{a}$ sarà finitamente generato. Fissiamo un insieme $\{a_1, a_2, \ldots, a_k\}$ di suoi generatori; sappiamo allora che gli elementi di $\mathfrak{a}$ sono del tipo $\sum_{i=1}^k \lambda_i a_i$, gli elementi di $\mathfrak{a}^2$ sono del tipo $\sum_{i,j=1}^k \lambda_{i\,j} a_i a_j$, e così via; in generale, gli elementi di $\mathfrak{a}^n$ sono le valutazioni su $(a_1, a_2, \ldots, a_k)$ di opportuni polinomi omogenei di grado n in k variabili.

Per ogni $n \in \mathbb{N}$, sia S_n l'insieme dei polinomi f omogenei di grado n in k variabili per cui $f(a_1, a_2, \ldots, a_k) \in \mathfrak{b}$. Sia poi S l'ideale di $A[x_1, x_2, \ldots, x_k]$ generato da $\bigcup_{n\in\mathbb{N}} S_n$; per il TEOR. della base di Hilbert (TEOR. 3.1, pag. 46), $A[x_1, x_2, \ldots, x_k]$ è noetheriano, e quindi S è generato da un numero finito di elementi $g_1, g_2, \ldots, g_t$; ogni g_i è combinazione lineare di elementi di $\bigcup_{n\in\mathbb{N}} S_n$: g_1 sarà quindi c.l. di certi $f_1, f_2, \ldots, f_{s_1}$, g_2 sarà c.l. di certi $f_{s_1+1}, f_{s_1+2}, \ldots, f_{s_2}$, e così via, fino a g_t che sarà c.l. di certi $f_{s_{t-1}+1}, f_{s_{t-1}+2}, \ldots, f_r$; S è allora generato dai polinomi $f_1, f_2, \ldots, f_r$, che sono elementi di $\bigcup_{n\in\mathbb{N}} S_n$; chiamiamo d_i il grado di f_i, e sia d il massimo grado dei polinomi f_i.

Per provare la tesi, occorre provare che ogni elemento di $\mathfrak{b}$ sta in $\mathfrak{ab}$ (poiché l'inclusione inversa è banalmente vera); fissiamo allora $b \in \mathfrak{b}$; per la definizione di $\mathfrak{b}$, b starà in particolare in $\mathfrak{a}^{d+1}$, e quindi esisterà $f \in S_{d+1}$ tale che $f(a_1, a_2, \ldots, a_k) = b$; ma $S_{d+1} \subseteq S$, e quindi f è combinazione di $f_1, f_2, \ldots, f_r$: esistono cioè r polinomi h_i tali che $f = \sum_{i=1}^r h_i f_i$; essendo d'altronde f omogeneo di grado $d+1$ e gli f_i omogenei di grado d_i, i polinomi h_i saranno omogenei di grado $d+1-d_i$; si ha poi

$$b = f(a_1, a_2, \ldots, a_k) = \sum_{i=1}^r \underbrace{h_i(a_1, a_2, \ldots, a_k)}_{\in \mathfrak{a}^{d+1-d_i} \subseteq \mathfrak{a}} \underbrace{f_i(a_1, a_2, \ldots, a_k)}_{\in \mathfrak{b}} \in \mathfrak{ab},$$

e quindi $b \in \mathfrak{ab}$, come volevasi.

La prima parte del TEOR. è così provata; la seconda parte segue immediatamente dal LEMMA di Nakayama, poiché $\mathfrak{b}$ è un A-modulo finitamente generato e, per la parte già provata, $\mathfrak{ab} = \mathfrak{b}$. □

4. Proprietà dei anelli artiniani

PROPOSIZIONE 4.1 *Ogni dominio artiniano D è un campo.*

Dimostrazione. Sia x un elemento non nullo di D; consideriamo la catena discendente

$$(x) \supseteq \left(x^2\right) \supseteq \cdots \supseteq (x^n) \supseteq \cdots ;$$

poiché D è artiniano, la catena è finita, e quindi esiste n tale che, in particolare, $(x^n) = \left(x^{n+1}\right)$, e quindi $x^n = \lambda x^{n+1}$, con λ opportuno; poiché nei domini vale la legge di cancellazione, dalla precedente uguaglianza segue $1 = \lambda x$, e quindi λ è il reciproco di x; per l'arbitrarietà della scelta di x non nullo, si ha che ogni elemento non nullo è invertibile, e quindi D è un campo. □

PROPOSIZIONE 4.2 *Se A è un anello artiniano, allora:*

(1) *ogni ideale primo è massimale;*
(2) *il nilradicale coincide con il radicale di Jacobson;*
(3) *esiste solo un numero finito di primi (ovvero di massimali);*
(4) *il nilradicale è nilpotente.*

Dimostrazione. Proviamo la **(1)**; fissiamo quindi un ideale primo $\mathfrak{p}$ di A, e proviamo che $A/\mathfrak{p}$ è un campo; ciò segue immediatamente dalla precedente PROP., poiché $A/\mathfrak{p}$ è un dominio (essendo $\mathfrak{p}$ primo) ed è artiniano (in quanto quoziente di un anello artiniano).

La **(2)** segue immediatamente dalla **(1)** e dalle definizioni.

Proviamo la **(3)**, provando che la famiglia dei massimali è finita. Sia $\mathcal{M}$ la famiglia dei massimali di A, e sia $\mathcal{I}$ la famiglia delle intersezioni finite di massimali di A; essendo A artiniano, $\mathcal{I}$ ammette un elemento minimale $\mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_t$. Proviamo ora che $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_t$ sono gli unici massimali; sia $\mathfrak{m}$ un massimale; allora $\mathfrak{m} \cap \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_t$ è un elemento di $\mathcal{I}$, e deve quindi contenere $\mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_t$; ma l'altra inclusione è sempre vera, e quindi $\mathfrak{m} \cap \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_t = \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_t$; in particolare, $\bigcap_{i=1}^{t} \mathfrak{m}_i \subseteq \mathfrak{m}$ e quindi, per la PROP. 1 di pag. 10, deve esistere i tale che $\mathfrak{m}_i \subseteq \mathfrak{m}$; ma $\mathfrak{m}_i$ è massimale, e quindi $\mathfrak{m}_i = \mathfrak{m}$, come volevasi.

Proviamo infine la **(4)**. Consideriamo la catena discendente

$$\mathcal{N} \supseteq \mathcal{N}^2 \supseteq \cdots \supseteq \mathcal{N}^n \supseteq \cdots ;$$

essendo A artiniano, la catena è finita, e quindi esiste $n \in \mathcal{N}$ tale che $\mathcal{N}^n = \mathcal{N}^{n+p}\ \forall\ p \in \mathcal{N}$. Poniamo, per semplicità, $\mathfrak{n} = \mathcal{N}^n$; proviamo che $\mathfrak{n} = (0)$.

Supponiamo per assurdo che $\mathfrak{n} \neq (0)$, e sia $\mathcal{C}$ la famiglia degli ideali $\mathfrak{c}$ di A per cui $\mathfrak{c}\mathfrak{n} \neq (0)$; $\mathcal{C}$ è non vuota, in quanto $\mathfrak{n} \in \mathcal{C}$ (infatti, $\mathfrak{n}^2 = \mathcal{N}^{n+n} = \mathcal{N}^n = \mathfrak{n} \neq (0)$); essendo A artiniano, esiste allora $\mathfrak{d}$ minimale per $\mathcal{C}$; essendo in particolare $\mathfrak{d} \in \mathcal{C}$, si ha $\mathfrak{d}\mathfrak{n} \neq (0)$, ed esiste quindi $d \in \mathfrak{d}$ tale che $d\mathfrak{n} \neq (0)$; si ha allora $(d) \in \mathcal{C}$, e quindi $(d) \supseteq \mathfrak{d}$; ma $d \in \mathfrak{d}$, e quindi $(d) \subseteq \mathfrak{d}$; in definitiva $\mathfrak{d} = (d)$.

Osserviamo anche che $(d\mathfrak{n})\mathfrak{n} = d\mathfrak{n}^2 = d\mathfrak{n} \neq (0)$, e quindi $d\mathfrak{n} \supseteq \mathfrak{d} = (d)$; ma $(d) \subseteq d\mathfrak{n}$, e quindi $d\mathfrak{n} = (d)$; allora $d = \lambda d$, con $\lambda \in \mathfrak{n}$, e si ha allora l'uguaglianza

$$d = d\lambda = d\lambda^2 = \cdots = d\lambda^n = \cdots ;$$

essendo poi $\lambda \in \mathfrak{n} \subseteq \mathcal{N}$, λ è nilpotente, e quindi una sua potenza si annulla; allora $d = 0$, contro il fatto che $d\mathfrak{n} \neq (0)$. L'assurdo assicura allora che $\mathfrak{n} = (0)$, ossia che $\mathcal{N}$ è nilpotente. □

CAPITOLO V

Decomposizioni primarie

1. Introduzione

DEFINIZIONE 1.1 Un ideale $\mathfrak{a}$ si dice irriducibile se da $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ segue $\mathfrak{a} = \mathfrak{b}$ oppure $\mathfrak{a} = \mathfrak{c}$.

PROPOSIZIONE 1.1 *Sia A un anello noetheriano; ogni suo ideale è intersezione di un numero finito di ideali irriducibili.*

Dimostrazione. Supponiamo per assurdo che la tesi non sia vera, e sia $\mathcal{M}$ la famiglia degli ideali di A che non verificano la tesi; essendo $\mathcal{M}$ non vuota ed A noetheriano, esiste un elemento massimale di $\mathcal{M}$; sia esso $\mathfrak{a}$; $\mathfrak{a}$ non è irriducibile (poiché altrimenti $\mathfrak{a}$ sarebbe intersezione di un ideale irriducibile: se stesso), e quindi esistono $\mathfrak{b}, \mathfrak{c}$ ideali di A tali che $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$, ma $\mathfrak{a} \neq \mathfrak{b}$ e $\mathfrak{a} \neq \mathfrak{c}$; d'altra parte $\mathfrak{a} \subseteq \mathfrak{b}$ e $\mathfrak{a} \subseteq \mathfrak{c}$, e quindi, per la massimalità di $\mathfrak{a}$, $\mathfrak{b}$ e $\mathfrak{c}$ non sono elementi di $\mathcal{M}$, e possono quindi essere scritti come intersezioni finite di ideali irriducibili; siano $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ gli ideali irriducibili di $\mathfrak{b}$ e $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_t$ gli ideali irriducibili di $\mathfrak{c}$; allora

$$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c} = \left(\bigcap_{i=1}^{n} \mathfrak{p}_i \right) \cap \left(\bigcap_{j=1}^{t} \mathfrak{q}_i \right),$$

e quindi $\mathfrak{a}$ è intersezione finita di ideali irriducibili, contro il fatto che $\mathfrak{a} \in \mathcal{M}$. □

OSSERVAZIONE 1.1 La scomposizione di ideali in intersezione di ideali irriducibili ha lo svantaggio di non presentare alcun tipo di unicità.

NOTA Nel seguito, qualora non diversamente specificato, supporremo sempre che A sia un anello noetheriano.

2. Ideali primari

DEFINIZIONE 2.1 Un ideale $\mathfrak{q}$ si dice *primario* se è proprio e da $xy \in \mathfrak{q}$ segue $x \in \mathfrak{q}$ oppure $y^n \in \mathfrak{q}$ per n opportuno (cioè $xy \in \mathfrak{q} \implies x \in \mathfrak{q} \vee y \in \mathfrak{r}(\mathfrak{q})$).

OSSERVAZIONE 2.1 Un ideale $\mathfrak{q}$ è primario se e solo se in $A/\mathfrak{q}$ ogni divisore dello zero è nilpotente. In particolare, quindi, ogni ideale primo è primario.

PROPOSIZIONE 2.1 *Se $\mathfrak{q}$ è un ideale primario, $\mathfrak{r}(\mathfrak{q})$ è primo.*

Dimostrazione. Essendo $\mathfrak{q} \neq A$, si ha $\mathfrak{r}(\mathfrak{q}) \neq A$; supponiamo ora che $xy \in \mathfrak{r}(\mathfrak{q})$; allora esiste $n \in \mathbb{N}$ per cui $(xy)^n \in \mathfrak{q}$, ossia $x^n y^n \in \mathfrak{q}$; essendo $\mathfrak{q}$ primario, si ha allora $x^n \in \mathfrak{q}$, oppure $y^{nm} \in \mathfrak{q}$, per m opportuno; allora $x \in \mathfrak{r}(\mathfrak{q})$, oppure $y \in \mathfrak{r}(\mathfrak{q})$, e quindi $\mathfrak{r}(\mathfrak{q})$ è primo. □

DEFINIZIONE 2.2 Un ideale primario $\mathfrak{q}$ si dice essere $\mathfrak{p}$-primario se $\mathfrak{p} = \mathfrak{r}(\mathfrak{q})$.

OSSERVAZIONE 2.2 Dalla PROP. 2.1 segue che, se $\mathfrak{q}$ è un ideale $\mathfrak{p}$-primario, allora esiste una potenza di $\mathfrak{p}$ contenuta in $\mathfrak{q}$. Infatti, $\mathfrak{p}$ è finitamente generato, essendo A noetheriano; sia $\{p_1, p_2, \ldots, p_t\}$ un'insieme di generatori di $\mathfrak{p}$; poiché $\mathfrak{p} = \mathfrak{r}(\mathfrak{q})$, per ogni $i = 1, 2, \ldots, t$ esiste $n_i \in \mathbb{N}$ tale che ${p_i}^{n_i} \in \mathfrak{q}$; posto $n = \max\{n_1, n_2, \ldots, n_t\}$, si ha che $\mathfrak{p}^n$ è generato da $\{{p_1}^n, {p_2}^n, \ldots, {p_t}^n\}$, che sono elementi di $\mathfrak{q}$, e quindi $\mathfrak{p}^n \subseteq \mathfrak{q}$.

PROPOSIZIONE 2.2 *Ogni ideale irriducibile è primario.*

Dimostrazione. Osserviamo che basta provare la proprietà nel caso in cui l'ideale sia quello nullo; infatti, se invece consideriamo $\mathfrak{a} \neq (0)$, possiamo sempre ricondurci all'anello $A/\mathfrak{a}$, in cui $\mathfrak{a}$ coincide con l'ideale nullo (l'irriducibilità e la primarietà sono invarianti per immersioni).

Supponiamo quindi che (0) sia irriducibile e proviamo che è primario.

Siano $x, y \in A$ tali che $xy = 0$; occorre provare che, se $x \neq 0$, allora y è nilpotente.

Consideriamo la catena ascendente degli annullatori delle potenze di y:

$$\operatorname{ann}(y) \subseteq \operatorname{ann}\left(y^2\right) \subseteq \cdots \subseteq \operatorname{ann}\left(y^n\right) \subseteq \cdots ;$$

essendo A noetheriano, la catena sarà finita, e quindi esiste n tale che $\operatorname{ann}(y^n) = \operatorname{ann}(y^{n+p})\ \forall\ p \in \mathbb{N}$.

Proviamo ora che $(0) = (x) \cap (y^n)$; prendiamo un elemento dell'intersezione: esso sarà del tipo $bx = cy^n$; moltiplicando per y si ottiene $bxy = cy^{n+1}$; ma $xy = 0$, e quindi $cy^{n+1} = 0$; allora $c \in \operatorname{ann}\left(y^{n+1}\right) = \operatorname{ann}(y^n)$, e quindi $cy^n = 0$, ovvero $bx = cy^n \in (0)$; è così provata l'inclusione $(x) \cap (y^n) \subseteq (0)$; l'altra inclusione è banalmente verificata, e quindi vale l'uguaglianza $(0) = (x) \cap (y^n)$; essendo poi $x \neq 0$ e (0) irriducibile, deve essere $(0) = (y^n)$, e quindi $y^n = 0$, che è quanto volevamo provare. □

COROLLARIO 2.1 *Ogni ideale è intersezione di un numero finito di ideali primari.*

DEFINIZIONE 2.3 Una decomposizione come nell'enunciato del precedente COR. si dice una *decomposizione primaria*.

LEMMA 2.1 (Akizuki) *Un anello è artiniano se e solo se è noetheriano ed ogni primo è massimale.*

Dimostrazione. Supponiamo in primo tempo che A sia un anello artiniano; proviamo che A è noetheriano; l'artinitanità di A assicura che ogni primo è massimale, che A ha un numero finito di massimali $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_t$, e che il nilradicale $\mathcal{N} = \bigcap_{i=1}^{t} \mathfrak{m}_i$ è nilpotente; si ha $\prod_{i=1}^{t} \mathfrak{m}_i \subseteq \bigcap_{i=1}^{t} \mathfrak{m}_i = \mathcal{N}$, e quindi $\prod_{i=1}^{t} \mathfrak{m}_i$ è nilpotente; detta n la sua nilpotenza, si ha che

$$(0) = \left(\prod_{i=1}^{t} \mathfrak{m}_i\right)^n = \underbrace{\mathfrak{m}_1\mathfrak{m}_1\mathfrak{m}_1\cdots\mathfrak{m}_1}_{n} \cdot \underbrace{\mathfrak{m}_2\mathfrak{m}_2\mathfrak{m}_2\cdots\mathfrak{m}_2}_{n} \cdots \underbrace{\mathfrak{m}_t\mathfrak{m}_t\mathfrak{m}_t\cdots\mathfrak{m}_t}_{n}$$

è prodotto di un numero finito di massimali, e quindi l'artinianità di A ne implica la noetherianità (COR. 2.1, CAP. IV, pag. 46).

Viceversa, supponiamo che A sia noetheriano, e che ogni suo primo sia massimale. Sia

$$(0) = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_t,$$

una decomposizione primaria dell'ideale nullo, dove $\mathfrak{q}_i$ è $\mathfrak{p}_i$-primario; si ha allora $\mathcal{N} = \mathsf{r}(0) = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \cdots \cap \mathfrak{p}_t$, e quindi $\prod_{i=1}^t \mathfrak{p}_i \subseteq \bigcap_{i=1}^t \mathfrak{p}_i = \mathcal{N}$; come nella parte precedente, la nilpotenza di $\mathcal{N}$ (per la noetherianità di A) assicura che (0) è prodotto di un numero finito di primi, cioè di massimali; è nuovamente soddisfatto il Cor. 2.1, Cap. IV, e quindi la notetherianità di A ne implica l'artinianità. □

3. Unicità della decomposizione

Osservazione 3.1 Sia $\mathfrak{a}$ un ideale di A, e sia $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ una sua decomposizione primaria, con $\mathfrak{q}_i$ ideale $\mathfrak{p}_i$-primario.

Se $\mathfrak{p}_i = \mathfrak{p}\ \forall\ i = 1, 2, \ldots, n$, allora $\mathfrak{a}$ è un ideale $\mathfrak{p}$-primario; infatti, se $xy \in \mathfrak{a}$ ed $y \notin \mathfrak{p}$, si ha $xy \in \mathfrak{q}_i, y \notin \mathfrak{p}_i\ \forall\ i = 1, 2, \ldots, n$, e quindi $x \in \mathfrak{q}_i\ \forall\ i = 1, 2, \ldots, n$, ossia $x \in \mathfrak{a}$; quindi $\mathfrak{a}$ è primario; d'altra parte, $\mathsf{r}(\mathfrak{a}) = \bigcap_{i=1}^n \mathsf{r}(\mathfrak{q}_i) = \bigcap_{i=1}^n \mathfrak{p}_i = \mathfrak{p}$, e quindi $\mathfrak{a}$ è $\mathfrak{p}$-primario.

Supponiamo ora che alcuni primi $\mathfrak{p}_i$ siano distinti; possiamo allora prendere, nella decomposizione, solo i $\mathfrak{q}_i$ associati ai primi distinti; possiamo anche eliminare i $\mathfrak{q}_i$ contenenti le intersezioni dei rimanenti, arrivando infine ad una decomposizione

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$$

con

$$\mathsf{r}(\mathfrak{q}_i) \neq \mathsf{r}(\mathfrak{q}_j) \text{ se } i \neq j,$$

$$\mathfrak{q}_i \not\supset \bigcap_{j \neq i} \mathfrak{q}_j.$$

Definizione 3.1 Una tale decomposizione si definisce *irridondante*; gli ideali primari $\mathfrak{q}_i$ si dicono le *componenti primarie* di $\mathfrak{a}$, e gli ideali $\mathfrak{p}_i$ sono detti *primi associati* ad $\mathfrak{a}$. A loro volta, i primi associati si dividono in *primi minimali* o *isolati* (quando non contengono altri primi della decomposizione), e primi *immersi*, se contengono altri primi; le corrispondenti componenti prendo ancora il nome di *componenti isolate* (quelle il cui primo corrispondente è isolato), e *componenti immerse* (quelle il cui primo corrispondente è immerso).

Sia ora $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ una sua decomposizione primaria qualsiasi; allora $\mathsf{r}(\mathfrak{a}) = \bigcap_{i=1}^n \mathfrak{p}_i$, dove $\mathfrak{p}_i$ è il radicale di $\mathfrak{q}_i$; siano $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$ i primi minimali di detta decomposizione; proviamo che ogni primo di A contenente $\mathfrak{a}$ contiene un $\mathfrak{p}_i$.

Se $\mathfrak{p}$ è un primo di A contenente $\mathfrak{a}$, allora (passando ai radicali) $\mathsf{r}(\mathfrak{a}) \subseteq \mathsf{r}(\mathfrak{p})$, ossia $\bigcap_{i=1}^n \mathfrak{p}_i \subseteq \mathfrak{p}$; per le proprietà già viste sulle intersezioni dei primi, deve allora esistere un i tale che $\mathfrak{p}_i \subseteq \mathfrak{p}$, come volevamo provare.

Possiamo allora dire che i primi minimali di una decomposizione sono anche i primi minimali nell'insieme dei primi contenenti $\mathfrak{a}$; da ciò segue in particolare che i primi minimali di $\mathfrak{a}$ sono in numero finito; infatti, quelli provenienti dalla fissata decomposizione sono in numero finito; vediamo che non possono essercene altri;

sia infatti $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i'$, un'altro decomposizione primaria di $\mathfrak{a}$; i primi associati ad $\mathfrak{a}$ in questa nuova decomposizione contengono $\mathfrak{a}$, e devono quindi contenere i primi minimali della precedente decomposizione; in particolare, i primi minimali della nuova decomposizione coincidono con quelli della vecchia decomposizione (in quanto li contengono e vi sono contenuti); ne segue allora che i primi minimali sono gli stessi in ogni decomposizione, e sono quindi in particolare in numero finito.

Se la decomposizione fissata in origine era irridondante, si ottiene in particolare che ogni primo $\mathfrak{p}$ contenente $\mathfrak{a}$ deve contenere un primo isolato associato ad $\mathfrak{a}$; ossia, i primi isolati sono i minimali della famiglia dei primi contenenti $\mathfrak{a}$.

OSSERVAZIONE 3.2 Il motivo per cui i primi immersi si chiamano in questo modo è l'interpretazione geometrica che si può dare degli ideali; ad esempio, nell'anello $k[x, y]$, dove k è un campo, ogni ideale corrisponde ad una figura geometrica; ad esempio, l'ideale (x) corrisponde all'asse delle y (di equazione $x = 0$); l'ideale (x, y) corrisponde all'origine (di equazioni $x = 0, y = 0$); in particolare, se un primo $\mathfrak{p}'$ è contenuto in un primo $\mathfrak{p}''$, allora la figura generata da $\mathfrak{p}''$ è contenuta nella figura generata da $\mathfrak{p}'$; quindi, i primi immersi rappresentano figure immerse nelle figure rappresentate dai primi isolati.

ESEMPIO 3.1 Consideriamo, nell'anello $A = k[x, y]$, l'anello $\mathfrak{a} = \big(x^2, xy\big)$; una sua decomposizione primaria irridondante è data da

$$\mathfrak{a} = (x) \cap \big(x^2, y\big),$$

dove $\mathfrak{q}_1 = (x)$ e $\mathfrak{q}_2 = \big(x^2, y\big)$ sono primari con primi associati $\mathfrak{p}_1 = (x)$ e $\mathfrak{p}_2 = (x, y)$; poiché si ha $\mathfrak{p}_1 \subsetneq \mathfrak{p}_2$, possiamo dire che $\mathfrak{p}_1$ è un primo isolato, mentre $\mathfrak{p}_2$ è un primo immerso. Per quanto riguarda l'interpretazione geometrica, si ha che l'origine ($\mathfrak{p}_2$) appartiene all'asse delle y ($\mathfrak{p}_1$).

Vediamo ora di dare qualche teorema di unicità sulle decomposizioni irridondanti.

LEMMA 3.1 *Sia $\mathfrak{q}$ un ideale $\mathfrak{p}$-primario e sia $x \in A$; allora*

(1) *se $x \in \mathfrak{q}$, si ha $\mathfrak{q} : x = A$;*
(2) *se $x \notin \mathfrak{q}$, si ha $\mathfrak{q} \subseteq \mathfrak{q} : x \subseteq \mathfrak{p}$, e $\mathfrak{q} : x$ è $\mathfrak{p}$-primario.*

Dimostrazione. Il primo caso è banale; supponiamo allora che $x \notin \mathfrak{q}$.

L'inclusione $\mathfrak{q} \subseteq \mathfrak{q} : x$ è sempre verificata; l'inclusione $\mathfrak{q} : x \subseteq \mathfrak{p}$ seguirà dal fatto che $\mathfrak{q} : x$ è $\mathfrak{p}$-primario; proviamo allora che, se $y, z \in A$ con $yz \in \mathfrak{q} : x$, e se $y \notin \mathfrak{p}$, allora $z \in \mathfrak{q} : x$; da $yz \in \mathfrak{q} : x$ segue che $yzx \in \mathfrak{q}$, e quindi da $y \notin \mathfrak{p}$ segue $zx \in \mathfrak{q}$, ossia $z \in \mathfrak{q} : x$, come volevasi. □

TEOREMA 3.1 *I primi associati ad un ideale $\mathfrak{a}$ sono tutti e soli gli ideali primi del tipo $\mathfrak{r}(\mathfrak{a} : x)$.*

Dimostrazione. Sia $\mathfrak{a}$ un ideale di A, e sia $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ una sua decomposizione primaria irridondante, con $\mathfrak{q}_i$ $\mathfrak{p}_i$-primario per ogni $i = 1, 2, \ldots, n$; l'irridondanza della decomposizione assicura che $\mathfrak{p}_i \neq \mathfrak{p}_j$ se $i \neq j$, e che $\mathfrak{q}_i \not\supseteq \bigcap_{j \neq i} \mathfrak{q}_j$.

Fissiamo ora $x \in A$ tale che $\mathsf{r}(\mathfrak{a} : x)$ sia primo, e proviamo che $\mathsf{r}(\mathfrak{a} : x)$ è uno dei $\mathfrak{p}_i$; osserviamo che si ha

$$\mathfrak{a} : x = \left(\bigcap_{i=1}^{n} \mathfrak{q}_i \right) : x = \bigcap_{i=1}^{n} (\mathfrak{q}_i : x)$$

e quindi

$$\mathsf{r}(\mathfrak{a} : x) = \bigcap_{i=1}^{n} \mathsf{r}(\mathfrak{q}_i : x) = \bigcap_{\substack{i \text{ t.c.} \\ x \notin \mathfrak{q}_i}} \mathfrak{p}_i,$$

dove l'ultima uguaglianza segue dal punto **(2)** del precedente LEMMA, e l'ultima intersezione è non vuota (se fosse $x \in \mathfrak{q}_i \ \forall\, i = 1, 2, \ldots, n$, si avrebbe $x \in \mathfrak{a}$, e quindi $\mathfrak{a} : x = A$; allora $\mathsf{r}(\mathfrak{a} : x) = A$ non sarebbe primo, contro la scelta di x); abbiamo allora in definitiva che $\mathsf{r}(\mathfrak{a} : x)$ è un primo uguale ad una intersezione di primi, e pertanto (PROP. 2 di pag. 10) $\mathsf{r}(\mathfrak{a} : x)$ sarà uguale ad un primo dell'intersezione, e sarà quindi un primo minimale di $\mathfrak{a}$.

Viceversa, proviamo che ogni $\mathfrak{p}_i$ primo isolato di $\mathfrak{a}$ è nella forma $\mathsf{r}(\mathfrak{a} : x)$. L'irridondanza della decomposizione assicura che esiste $x \in \bigcap_{j \neq i} \mathfrak{q}_j \setminus \mathfrak{q}_i$; allora $\mathsf{r}(\mathfrak{a} : x) = \bigcap_{\substack{h \text{ t.c.} \\ x \notin \mathfrak{q}_h}} \mathfrak{p}_h = \mathfrak{p}_i$. □

COROLLARIO 3.1 *I primi associati di un ideale sono univocamente determinati.*

OSSERVAZIONE 3.3 Sia $\mathfrak{a} = (0)$; sappiamo già che l'intersezione dei primi associati ad $\mathfrak{a}$ è uguale all'intersezione dei primi minimali di $\mathfrak{a}$; ma i primi minimali di $\mathfrak{a} = (0)$ sono i primi minimali nell'insieme di tutti i primi di A, e quindi l'intersezione dei primi associati ad $\mathfrak{a}$ è uguale all'intersezione di tutti i primi di $\mathfrak{a}$, ossia al nilradicale:

$$\bigcap_{\substack{\mathfrak{p} \text{ primi} \\ \text{associati} \\ \text{a } (0)}} \mathfrak{p} = \mathcal{N};$$

proviamo ora che l'unione dei primi associati ad (0) è l'insieme $\mathcal{D}$ dei divisori dello zero, ossia

$$\bigcup_{\substack{\mathfrak{p} \text{ primi} \\ \text{associati} \\ \text{a } (0)}} \mathfrak{p} = \mathcal{D}; \tag{12}$$

Dimostrazione. Come già osservato in precedenza (OSS. 2.2, CAP. I), si ha

$$\mathcal{D} = \bigcup_{x \neq 0} \operatorname{ann}(x) = \bigcup_{x \neq 0} (0 : x);$$

Consideriamo ora il radicale di $\mathcal{D}$ (abbiamo già osservato che il radicale può essere definito per un qualsiasi insieme, non solo per gli ideali); proviamo innanzi tutto che si ha $\mathcal{D} = \mathsf{r}(\mathcal{D})$.

L'inclusione $\mathcal{D} \subseteq \mathsf{r}(\mathcal{D})$ è vera per qualsiasi insieme; proviamo l'inclusione inversa; supponiamo che $x \in \mathsf{r}(\mathcal{D})$ e proviamo che $x \in \mathcal{D}$; per ipotesi una potenza x^n di x dividerà lo zero; esisterà allora $b \neq 0$ tale che $bx^n = 0$, ossia $\left(bx^{n-1}\right)x = 0$; se $bx^{n-1} \neq 0$, ne segue allora che x è un divisore dello zero, e quindi $x \in \mathcal{D}$ come volevasi; se invece $bx^{n-1} = 0$, possiamo scrivere $\left(bx^{n-2}\right)x = 0$, e quindi ancora

o x dividerà lo zero (se $bx^{n-2} \neq 0$), oppure $bx^{n-2} = 0$, e si potrà proseguire nel procedimento; il procedimento, d'altra parte, dovrà necessariamente avere termine, poiché al più, dopo n passaggi, si otterrà $bx = 0$, ed essendo $b \neq 0$ ne seguirà che x è un divisore dello zero; è quindi provato che $\mathsf{r}(\mathcal{D}) \subseteq \mathcal{D}$; dalle due inclusioni segue $\mathcal{D} = \mathsf{r}(\mathcal{D})$.

Proviamo ora la nostra tesi (12), provando le due inclusioni.

Da un lato si ha

$$\mathcal{D} = \mathsf{r}(\mathcal{D}) = \mathsf{r}\left(\bigcup_{x\neq 0} (0:x)\right) = \bigcup_{x\neq 0} \mathsf{r}(0:x) = \bigcup_{x\neq 0}\left(\bigcap_{x\notin \mathfrak{p}_i} \mathfrak{p}_i\right),$$

dove l'ultima eguaglianza è dovuta al Teor. 3.1 ed al Lemma 3.1 e dove i $\mathfrak{p}_i$ dell'ultima intersezione sono i primi associati a (0) e per cui $x \notin \mathfrak{p}_i$; osserviamo ora che, se $x \neq 0$, l'intersezione dei primi associati ad (0) che non contengono x è non vuota, poiché altrimenti si avrebbe $\mathsf{r}(0:x) = (0)$, ovvero $x = 0$, contro la scelta di x; d'altra parte, l'intersezione degli ideali è contenuta nell'unione, e quindi

$$\mathcal{D} \subseteq \bigcup_{x\neq 0}\left(\bigcap_{x\notin \mathfrak{p}_i} \mathfrak{p}_i\right) \subseteq \bigcup_{x\neq 0}\left(\bigcup_{x\notin \mathfrak{p}_i} \mathfrak{p}_i\right) \subseteq \bigcup \mathfrak{p}_i$$

e quindi, per transitività

$$\mathcal{D} \subseteq \bigcup \mathfrak{p}_i;$$

d'altra parte, ogni primo associato ad (0) è nella forma $\mathsf{r}(0:x)$ con $x \neq 0$, e quindi

$$\bigcup_{\substack{\mathfrak{p} \text{ primi} \\ \text{associati} \\ \text{a } (0)}} \mathfrak{p} \subseteq \bigcup_{x\neq 0} \mathsf{r}(0:x) = \mathsf{r}(\mathcal{D}) = \mathcal{D};$$

dalle due inclusioni segue allora l'eguaglianza (12) della tesi. □

Esempio 3.2 Consideriamo, nell'anello $A = k[x,y]$, l'ideale $\mathfrak{a} = \left(x^2, xy\right)$, ed una sua decomposizione primaria $(x) \cap \left(x^2, y\right)$ ($(x) = \mathfrak{q}_1$, $\left(x^2, y\right) = \mathfrak{q}_2$), con primi associati $\mathfrak{p}_1 = (x)$, $\mathfrak{p}_2 = (x,y)$.

In $k[x,y]/\left(x^2, xy\right)$, $\bar{\mathfrak{p}_1}$, $\bar{\mathfrak{p}_2}$ sono i primi associati dello zero, e si ha $\bar{\mathfrak{p}_1} \cap \bar{\mathfrak{p}_2} = \bar{\mathfrak{p}_1} = \mathcal{N}$ e $\bar{\mathfrak{p}_1} \cup \bar{\mathfrak{p}_2} = \bar{\mathfrak{p}_2} = \mathcal{D}$; infatti, $\bar{x}$ è nilpotente ($\bar{x}^2 = 0$), e quindi $\bar{\mathfrak{p}_1} = \mathcal{N}$, e $\bar{y}$ è divisore dello zero ($\bar{y}\bar{x} = 0$), ma non nilpotente, quindi $\bar{\mathfrak{p}_2} = \mathcal{D}$

Teorema 3.2 *Le componenti isolate di una decomposizione primaria sono univocamente determinate.*

Dimostrazione. Sia $\mathfrak{a}$ un ideale di A, e sia $\mathfrak{q}_i$ una componente isolata di una decomposizione primaria irridondante di $\mathfrak{a}$; per provare che è univocamente determinata, basta provare che $\mathfrak{q}_i = \mathfrak{q}_i'$, dove

$$\mathfrak{q}_i' = \{x \in A \mid (\mathfrak{a}:x) \nsubseteq \mathfrak{p}_i\};$$

infatti, $\mathfrak{q}_i'$ è univocamente determinato (essendo univocamente determinato $\mathfrak{p}_i$).

Proviamo dunque che $\mathfrak{q}_i = \mathfrak{q}_i'$.

Se $x \in \mathfrak{q}_i'$, si ha $(\mathfrak{a}:x) \nsubseteq \mathfrak{p}_i$, e quindi esiste $y \in (\mathfrak{a}:x) \setminus \mathfrak{p}_i$; allora $xy^n \in \mathfrak{a} \subseteq \mathfrak{q}_i$; ma $y \notin \mathfrak{p}_i$, e quindi $x \in \mathfrak{q}_i$; è così provato che $\mathfrak{q}_i' \subseteq \mathfrak{q}_i$.

Proviamo ora l'inclusione inversa; essendo $\mathfrak{q}_i$ una componente isolata, si ha $\mathfrak{p}_i \not\supseteq \bigcap_{j\neq i} \mathfrak{p}_j$, e quindi $\mathfrak{p}_j \not\subseteq \mathfrak{p}_i$ se $j \neq i$; esiste allora, per ogni $j \neq i$, un $b_j \in \mathfrak{p}_j \setminus \mathfrak{p}_i$; d'altra parte, essendo $\mathfrak{q}_j$ $\mathfrak{p}_j$-primario, per ogni $j \neq i$ esiste n_j tale che ${\mathfrak{p}_j}^{n_j} \subseteq \mathfrak{q}_j \subseteq \mathfrak{p}_j$; si ha allora ${b_j}^{n_j} \in \mathfrak{q}_j \ \forall\ j \neq i$, e quindi $b = \prod_{j\neq i} {b_j}^{n_j} \in \bigcap_{j\neq i} \mathfrak{q}_i$, e $b \notin \mathfrak{p}_i$. Siamo ora in grado di provare che, se $x \in \mathfrak{q}_i$, allora $x \in \mathfrak{q}_i'$; infatti, da $x \in \mathfrak{q}_i$ segue $xb \in \bigcap_{j=1}^{n} \mathfrak{q}_j$, e quindi $b \in \mathfrak{a} : x$; ma $b \notin \mathfrak{p}_i$, e quindi $(\mathfrak{a} : x) \not\subseteq \mathfrak{p}_i$, ossia $x \in \mathfrak{q}_i'$. □

OSSERVAZIONE 3.4 Il precedente teorema non vale per le componenti immerse, come prova il seguente

ESEMPIO 3.3 Consideriamo, in $A = k[x, y]$, l'ideale $\mathfrak{a} = \big(x^2, xy\big)$; esso si può decomporre nei due modi seguenti, aventi la stessa componente isolata (in accordo con il precedente TEOR.), ma componenti immerse distinte:

$$\mathfrak{a} = (x) \cap \big(x^2, y\big) = (x) \cap \big(x^2, x + y\big).$$

4. Ulteriori proprietà degli ideali primari

PROPOSIZIONE 4.1 *Siano A, B due anelli commutativi con unità, e sia $f : A \to B$ un omomorfismo; se $\mathfrak{q}$ è un ideale primario di B, allora la sua contrazione $f^{-1}(\mathfrak{q})$ è un ideale primario di A.*

OSSERVAZIONE 4.1 Se $\mathfrak{q}$ è un ideale $\mathfrak{p}$-primario, abbiamo visto che esiste una potenza n di $\mathfrak{p}$ tale che $\mathfrak{p}^n \subseteq \mathfrak{q} \subseteq \mathfrak{p}$; in generale, però, non si ha $\mathfrak{p}^n = \mathfrak{q}$, come mostra il seguente esempio.

ESEMPIO 4.1 Sia k un campo e sia $A = k[x, y]$; consideriamo l'ideale primario $\mathfrak{q} = \big(x^2, y\big)$; il suo radicale è $\mathfrak{p} = (x, y)$, e $\mathfrak{p}^2 = \big(x^2, y^2\big)$ è la più piccola potenza di $\mathfrak{p}$ che contiene $\mathfrak{q}$; quindi $\mathfrak{p}^2 \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$.

Inoltre, non è detto che un ideale che abbia per radicale un numero primo $\mathfrak{p}$ sia $\mathfrak{p}$-primario, neanche nel caso delle potenze $\mathfrak{p}^n$, come mostra il seguente esempio.

ESEMPIO 4.2 Sia k un campo, e sia $A = {k[x, y, z]}/{\big(xy - z^2\big)}$; consideriamo l'ideale primo $\mathfrak{p} = (\bar{x}, \bar{z})$ (che sia primo si vede osservando che ${A}/{\mathfrak{p}} \cong k[y]$ è un dominio). L'ideale $\mathfrak{p}^2 = \big(\bar{x}^2, \bar{z}^2, \bar{x}\bar{z}\big)$ ha per radicale $\mathfrak{p}$, ma non è $\mathfrak{p}$-primario; infatti, $\bar{z}^2 = \bar{x}\bar{y} \in \mathfrak{p}^2$ ma $\bar{x} \notin \mathfrak{p}^2$ e $\bar{y} \notin \mathfrak{r}\big(\mathfrak{p}^2\big) = \mathfrak{p}$.

PROPOSIZIONE 4.2 *Se $\mathfrak{q}$ è un ideale di A e $\mathfrak{r}(\mathfrak{q}) = \mathfrak{m}$ è un ideale massimale, allora $\mathfrak{q}$ è $\mathfrak{m}$-primario.*

Dimostrazione. L'anello ${A}/{\mathfrak{q}}$ è locale, in quanto i suoi ideali primi sono le immagini dei primi di A contenenti $\mathfrak{q}$; ma se un primo $\mathfrak{p}$ contiene $\mathfrak{q}$, allora deve contenere il radicale di $\mathfrak{q}$, che è il massimale $\mathfrak{m}$, e quindi $\mathfrak{p} = \mathfrak{m}$; in definitiva ${A}/{\mathfrak{q}}$ ha un unico primo (e quindi massimale): $\bar{\mathfrak{m}}$; in particolare $\bar{\mathfrak{m}}$, essendo l'unico massimale, coinciderà con il nilradicale di ${A}/{\mathfrak{q}}$; la noetherianità di A assicura inoltre la noetherianità di ${A}/{\mathfrak{q}}$, e quindi la nilpotenza del nilradicale $\bar{\mathfrak{m}}$; gli elementi di ${A}/{\mathfrak{q}}$ sono allora o nilpotenti (se stanno in $\bar{\mathfrak{m}}$), oppure invertibili (se non stanno in $\bar{\mathfrak{m}}$); in particolare, i divisori dello zero in ${A}/{\mathfrak{q}}$ sono nilpotenti, e quindi $\mathfrak{q}$ è primario. □

COROLLARIO 4.1 *Le potenze degli ideali massimali $\mathfrak{m}$ sono $\mathfrak{m}$-primari.*

OSSERVAZIONE 4.2 Sia A un anello noetheriano e sia $\mathfrak{q}$ un suo ideale $\mathfrak{p}$-primario; sia S un insieme moltiplicativo di A.

Se $S \cap \mathfrak{p} \neq \varnothing$, allora l'esteso di $\mathfrak{q}$ in $S^{-1}A$ è tutto $S^{-1}A$; infatti, preso $s \in S \cap \mathfrak{p}$ si ha $s \in \mathfrak{p}$, e quindi esiste $n \in \mathbb{N}$ tale che $s^n \in \mathfrak{q}$; ma $s^n \in S$, e quindi $\mathfrak{q} \cap S \neq \varnothing$, da cui segue che $\mathfrak{q}^e = S^{-1}A$.

Se invece $S \cap \mathfrak{p} = \varnothing$, allora $\mathfrak{q}^e$ è $\mathfrak{p}^e$-primario in $S^{-1}A$.

Possiamo anzi dire qualcosa di più: se $\mathfrak{q}$ è un ideale primo o primario di A che non interseca S, allora $\mathfrak{q}^e$ è un ideale primo o primario di $S^{-1}A$, e la sua contrazione $\mathfrak{q}^{ec}$ è ancora un ideale primo o primario di A (per i primi ciò è stato visto nelle PROP. 4 e 5, CAP. III di pag. 38; per i primari si prova con la stessa tecnica); proviamo ora che in questo caso si ha addirittura $\mathfrak{q}^{ec} = \mathfrak{q}$.

Dimostrazione. Poiché si ha sempre $\mathfrak{q} \subseteq \mathfrak{q}^{ec}$ (l'inclusione vale per ogni insieme), occorre provare la diseguaglianza inversa.

Fissiamo dunque $x \in \mathfrak{q}^{ec}$, e proviamo che $x \in \mathfrak{q}$; essendo $x \in \mathfrak{q}^{ec}$ è possibile determinare $y \in \mathfrak{q}$ ed $s \in S$ tali che $\dfrac{x}{1} = \dfrac{y}{s}$, e quindi esiste $u \in S$ tale che $u(sx - y) = 0$; quindi $usx = uy$; il secondo membro sta in $\mathfrak{q}$, e quindi anche il $usx \in \mathfrak{q}$;

- se $\mathfrak{q}$ è primo (ed è quindi l'ideale su cui si fa la localizzazione), da $us \in S$ segue $us \notin \mathfrak{q}$; essendo poi $usx \in \mathfrak{q}$, deve essere $x \in \mathfrak{q}$, come volevasi;
- se $\mathfrak{q}$ è primario, detto $\mathfrak{p}$ il suo radicale (e quindi l'ideale su cui si fa la localizzazione), da $us \in S$ segue $us \notin \mathfrak{p}$; allora $usx \in \mathfrak{q}$ implica $x \in \mathfrak{q}$, come volevasi;

è allora provato che $x \in \mathfrak{q}\ \forall\ x \in \mathfrak{q}^{ec}$, ossia $\mathfrak{q}^{ec} \subseteq \mathfrak{q}$; dall'altra inclusione, sempre vera, segue allora l'uguaglianza della tesi. □

OSSERVAZIONE 4.3 Abbiamo già visto che, se $\mathfrak{p}$ è un primo di un anello noetheriano, allora $\mathfrak{p}^n$ ha $\mathfrak{p}$ come radicale, ma non è in generale detto che $\mathfrak{p}^n$ sia $\mathfrak{p}$-primario; si vede però facilmente che $\mathfrak{p}$ è l'unico primo minimale di $\mathfrak{p}^n$; una qualsiasi decomposizione primaria irridondante $\mathfrak{p}^n = \mathfrak{q} \cap \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$ di $\mathfrak{p}^n$ avrà allora una componente isolata $\mathfrak{q}$ $\mathfrak{p}$-primaria e t componenti immerse $\mathfrak{q}_i$, con $\mathfrak{q}_i$ $\mathfrak{p}_i$-primaria; per il TEOR. di unicità delle componenti isolate, $\mathfrak{q}$ è univocamente determinata; la si suole indicare con
(DEF) $\mathfrak{p}^{(n)}$, e la si chiama *potenza n-esima simbolica* di $\mathfrak{p}$.

Vediamo ora un altro modo per ottenere la potenza n-esima simbolica di $\mathfrak{p}$.

Consideriamo l'omomorfismo canonico $A \longrightarrow A_{\mathfrak{p}}$; l'esteso $\mathfrak{p}^n A_{\mathfrak{p}}$ di $\mathfrak{p}^n$ ha come radicale $\mathfrak{p}A_{\mathfrak{p}}$, esteso di $\mathfrak{p}$, che è l'unico massimale di $A_{\mathfrak{p}}$; allora, $\mathfrak{p}^n A_{\mathfrak{p}}$ è $\mathfrak{p}A_{\mathfrak{p}}$-primario; contraendo, si ha allora che $(\mathfrak{p}^n A_{\mathfrak{p}})^c$ è $(\mathfrak{p}A_{\mathfrak{p}})^c$-primario, ossia $\mathfrak{p}$-primario; d'altra parte $\mathfrak{p}^n \subseteq (\mathfrak{p}^n A_{\mathfrak{p}})^c$. Proviamo ora che $(\mathfrak{p}^n A_{\mathfrak{p}})^c = \mathfrak{p}^{(n)}$.

Si ha infatti

$$\mathfrak{p}^n = \mathfrak{p}^{(n)} \cap \left(\bigcap_{i=1}^{t} \mathfrak{q}_i \right);$$

allora, estendendo in $A_{\mathfrak{p}}$ e tenendo conto che $\mathfrak{q}_i \supseteq \mathfrak{p}_i \supset \mathfrak{p}$,

$$\mathfrak{p}^n A_{\mathfrak{p}} = \mathfrak{p}^{(n)} A_{\mathfrak{p}} \cap A_{\mathfrak{p}} = \mathfrak{p}^{(n)} A_{\mathfrak{p}}; \tag{13}$$

per l'Oss. 4.2, si ha $\left(\mathfrak{p}^{(n)}A_{\mathfrak{p}}\right)^c = \mathfrak{p}^{(n)}$; contraendo allora nella (13) si ottiene $(\mathfrak{p}^n A_{\mathfrak{p}})^c = \mathfrak{p}^{(n)}$.

ESEMPIO 4.3 Consideriamo l'anello $A = {}^{k[x,y,z]}\!/_{\left(xy-z^2\right)}$, e l'ideale $\mathfrak{p} = (\bar{x}, \bar{z})$; l'ideale $\mathfrak{p}^2$ non è primario; infatti si ha $\mathfrak{p}^2 = \left(\bar{x}^2, \bar{x}\bar{z}, \bar{z}^2\right)$; ma $\bar{z}^2 = \bar{x}\bar{y} \in \mathfrak{p}^2$, e $\bar{y} \notin \mathfrak{p}$, $\bar{x} \notin \mathfrak{p}^2$; quindi $\mathfrak{p}^2$ non è primario; vediamo allora chi è $\mathfrak{p}^{(2)}$.

Per quanto visto nell'osservazione, si ha $\mathfrak{q} = \mathfrak{p}^{(2)}$; per quanto visto sopra, sappiamo che $\mathfrak{q} = \left(\mathfrak{p}^{(2)}\right)^{ec}$; poniamoci quindi nel localizzato $A_{\mathfrak{p}} = k(y)[z]$; in questo anello y è invertibile (poiché $y \notin \mathfrak{p}$), e quindi da $xy = z^2$ segue $x = \dfrac{z^2}{y}$; l'immagine di $\mathfrak{p}^2$ è allora $\left(z^2\right)$; osserviamo che, posto $\mathfrak{q}_1 = \left(x, z^2\right)$ si ha che $\mathfrak{q}_1$ è $\mathfrak{p}$-primario, ed inoltre ${\mathfrak{q}_1}^e = {\mathfrak{p}^2}^e$; contraendo: $\mathfrak{q}_1 = {\mathfrak{q}_1}^{ec} = {\mathfrak{p}^2}^{ec} = \mathfrak{q}$, e quindi $\mathfrak{q}_1 = \mathfrak{q}$, ossia $\mathfrak{p}^{(2)} = \mathfrak{q} = \left(x, z^2\right)$.

CAPITOLO VI

Teoria della dimensione

DEFINIZIONE 1.1 Sia $\mathfrak{p}$ un primo di un anello noetheriano A; diremo *altezza* di $\mathfrak{p}$, e la indicheremo con il simbolo $\mathrm{ht}(\mathfrak{p})$, l'estremo superiore delle lunghezze delle catene di primi del tipo

$$\mathfrak{p} = \mathfrak{p}_h \supsetneq \mathfrak{p}_{h-1} \supsetneq \cdots \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{p}_0.$$

ESEMPIO 1.1 Il $\mathbb{Z}$, l'ideale $2\mathbb{Z}$ ha altezza due, in quanto la massima catena di primi è $(0) \subsetneq 2\mathbb{Z}$ (in effetti, ogni ideale primo non nullo di $\mathbb{Z}$ ha altezza due).

In $k[x, y]$, l'ideale $\mathfrak{p} = (x, y)$ ha altezza tre; una catena di lunghezza massima è $(0) \subsetneq (x) \subseteq (x, y)$.

DEFINIZIONE 1.2 Chiameremo *dimensione* di un anelo noetheriano A, e la indicheremo con il simbolo $\dim A$, l'estremo superiore delle altezze dei primi di A.

OSSERVAZIONE 1.1 $\mathbb{Z}$ ha dimensione due. $k[x, y]$ ha dimensione tre.

DEFINIZIONE 1.3 Sia $\mathfrak{a}$ un ideale di un anello noetheriano A; si chiama *altezza* di $\mathfrak{a}$, e la si indica con il simbolo $\mathrm{ht}(\mathfrak{a})$, la minima altezza dei primi contenenti $\mathfrak{a}$.

OSSERVAZIONE 1.2 L'altezza di un ideale $\mathfrak{a}$ è la minima altezza dei primi isolati di $\mathfrak{a}$.

LEMMA 1.1 (*Krull) Sia A un dominio noetheriano e sia a un elemento non nullo e non invertibile di A; ogni primo minimale $\mathfrak{p}$ di (a) ha altezza* 1.

Dimostrazione. Sia $\mathfrak{p}$ un primo minimale di (a); per provare che $\mathfrak{p}$ ha altezza uno, occorre provare che l'unico primo contenuto propriamente in $\mathfrak{p}$ è l'ideale nullo.

Osserviamo inoltre che possiamo sempre supporre che A sia un anello locale, e che $\mathfrak{p}$ sia il suo unico massimale; infatti, se così non fosse, basterebbe ragionare sul localizzato $A_{\mathfrak{p}}$, per ottenere lo stesso risultato.

Supponiamo quindi che A sia locale e che $\mathfrak{p}$ sia il suo unico massimale; sia $\mathfrak{q}$ un primo di A contenuto propriamente in $\mathfrak{p}$; proviamo che $\mathfrak{q} = (0)$.

Consideriamo la catena delle potenze simboliche di $\mathfrak{q}$

$$\mathfrak{q} \supseteq \mathfrak{q}^{(2)} \supseteq \mathfrak{q}^{(2)} \supseteq \cdots \supseteq \mathfrak{q}^{(n)} \supseteq \cdots , \tag{14}$$

e la catena

$$\mathfrak{q} + (a) \supseteq \mathfrak{q}^{(2)} + (a) \supseteq \mathfrak{q}^{(2)} + (a) \supseteq \cdots \supseteq \mathfrak{q}^{(n)} + (a) \supseteq \cdots ; \tag{15}$$

l'anello $A/(a)$ è ancora un anello noetheriano, ed il suo ideali primi sono in corrispondenza biunivoca con i primi di A che contengono (a); per la minimalità di $\mathfrak{p}$, e per la sua massimalità, si ha che $\bar{\mathfrak{p}}$ è l'unico ideale primo di $A/(a)$; allora in $A/(a)$ ogni primo è massimale, e quindi la noetherianità implica l'artinianità; considerata allora in $A/(a)$ la catena degli estesi di (14) (i cui elementi sono $\left(\mathfrak{q}^{(n)}\right)^e$), si ha che

la suddetta catena è finita; contraendo, anche la catena formata dagli ideali $\left(\mathfrak{q}^{(n)}\right)^{ec}$ risulta finita; ma questa è proprio la catena (15); esiste allora $n \in \mathbb{N}$ tale che

$$\mathfrak{q}^{(j)} + (a) = \mathfrak{q}^{(n)} + (a) \qquad \forall\ j \geq n;$$

ne segue in particolare che $\mathfrak{q}^{(n)} \subseteq \mathfrak{q}^{(j)} + (a)\ \forall\ j \geq n$.

Fissiamo $j \geq n$; preso $x \in \mathfrak{q}^{(n)}$, si ha allora $x = y + \lambda a$, con $y \in \mathfrak{q}^{(j)}$; quindi $\lambda a = x - y \in \mathfrak{q}^{(n)} + \mathfrak{q}^{(j)}$; ma $j \geq n$ implica $\mathfrak{q}^{(j)} \subseteq \mathfrak{q}^{(n)}$, e quindi $\lambda a \in \mathfrak{q}^{(n)}$; ma $\mathfrak{q}^{(n)}$ è $\mathfrak{q}$-primario, ed $a \notin \mathfrak{q}$ (in quanto $\mathfrak{p}$ è il primo minimale di a, e $\mathfrak{q} \subsetneq \mathfrak{p}$); quindi $\lambda \in \mathfrak{q}^{(n)}$; allora $x = y + \lambda a \in \mathfrak{q}^{(j)} + (a)\mathfrak{q}^{(n)}$; per l'arbitrarietà di $x \in \mathfrak{q}^{(n)}$, si ha allora

$$\mathfrak{q}^{(n)} \subseteq \mathfrak{q}^{(j)} + (a)\mathfrak{q}^{(n)};$$

l'altra inclusione è pure banalmente verificata (essendo $\mathfrak{q}^{(j)} \subseteq \mathfrak{q}^{(n)}$), e quindi

$$\mathfrak{q}^{(n)} = \mathfrak{q}^{(j)} + (a)\mathfrak{q}^{(n)};$$

ma (a) è contenuto nel radicale di Jacobson di A (in quanto, nelle nostre ipotesi, $\mathfrak{p}$ è l'unico massimale, e coincide pertanto con il radicale di Jacobson); per un Cor. del Lemma di Nakayama si ha allora $\mathfrak{q}^{(n)} = \mathfrak{q}^{(j)}$; il ragionamento vale per ogni $j \geq n$, e quindi la catena (14) è finita.

Poiché gli ideali $\mathfrak{q}^{(j)}$ sono primari, si ha $\mathfrak{q}^{(j)} = \left(\mathfrak{q}^{(j)}\right)^{ec} = \left(\mathfrak{q}^j A_{\mathfrak{q}}\right) \cap A$; d'altra parte, per il Teor. dell'intersezione di Krull (Teor. 3.2, Cap. IV), si ha $\bigcap_{j\in\mathbb{N}} \left(\mathfrak{q}^j A_{\mathfrak{q}}\right) = (0)$, e quindi risulta $\bigcap_{j\in\mathbb{N}} \mathfrak{q}^{(j)} = (0)$, ossia, per la finitezza della catena (14), $\mathfrak{q} \cap \mathfrak{q}^{(2)} \cap \cdots \cap \mathfrak{q}^{(n)} = (0)$; la catena è non crescente, e quindi l'ultima uguaglianza si scrive $\mathfrak{q}^{(n)} = (0)$; allora $\mathfrak{q} = \mathfrak{r}\left(\mathfrak{q}^{(n)}\right) = (0)$, ossia $\mathfrak{q} = (0)$, che è quanto volevamo provare. □

Teorema 1.1 (dell'altezza di Krull) *Sia A un anello noetheriano e sia $\mathfrak{a}$ un suo ideale; sia $\{a_1, a_2, \ldots, a_r\}$ una famiglia di generatori di $\mathfrak{a}$; ogni polinomio minimale $\mathfrak{p}$ di $\mathfrak{a}$ ha altezza al più r.*

Dimostrazione. Ragioniamo per induzione su r; se $r = 1$, si ha $\mathfrak{a} = (a)$, e la tesi è conseguenza immediata del Lemma di Krull.

Supponiamo ora che $r > 1$, e supponiamo che la tesi sia vera per gli ideali generati da $r - 1$ elementi. Proviamo che, se $\mathfrak{a}$ è generato dagli r elementi $a_1, a_2, \ldots, a_r$, allora ogni primo minimale $\mathfrak{p}$ di $\mathfrak{a}$ ha altezza il più r.

Sia $\mathfrak{p}$ un primo minimale di $\mathfrak{a}$ e sia

$$\mathfrak{p} \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{p}_2 \supsetneq \cdots \supsetneq \mathfrak{p}_s$$

una catena discendente di primi; per provare che $\mathrm{ht}(\mathfrak{p}) \leq r$ basta provare che $s \leq r$.

Osserviamo che possiamo sempre supporre che non esistano primi intermedi fra $\mathfrak{p}$ e $\mathfrak{p}_1$, poiché, se così non fosse, basterebbe prendere $\mathfrak{p}_1'$ elemento massimale della famiglia dei primi contenuti in $\mathfrak{p}$ e contenenti $\mathfrak{p}_1$ ($\mathfrak{p}_1'$ esiste per la noetherianità di A), e considerare la catena avente $\mathfrak{p}_1'$ intercalato fra $\mathfrak{p}$ e $\mathfrak{p}_1$. Possiamo anche supporre che $\mathfrak{p}$ sia l'unico massimale di A; se così non fosse, basterebbe infatti ragionare su $A_{\mathfrak{p}}$ per ottenere il medesimo risultato.

Per la minimalità di $\mathfrak{p}$, si ha che $\mathfrak{a} \subseteq \mathfrak{p}$ e $\mathfrak{a} \nsubseteq \mathfrak{p}_i\ \forall\ i = 1, 2, \ldots, s$; in particolare $\mathfrak{a} \nsubseteq \mathfrak{p}_1$, e quindi un generatore di $\mathfrak{a}$ non sta in $\mathfrak{p}_1$; supponiamo, per fissare le idee, che sia $a_1 \in \mathfrak{a} \setminus \mathfrak{p}_1$.

Consideriamo ora $\mathfrak{p}_1+(a_1) \subseteq \mathfrak{p}$; poiché abbiamo supposto che non ci sono primi fra $\mathfrak{p}_1$ e $\mathfrak{p}$, $\mathfrak{p}$ è il più piccolo primo contenente $\mathfrak{p}_1 + (a_1)$; allora $\mathfrak{r}(\mathfrak{p}_1 + (a_1)) = \mathfrak{p}$, e quindi $\mathfrak{p}_1 + (a_1)$ è $\mathfrak{p}$-primario (avendo supposto $\mathfrak{p}$ massimale in A). Sia $\mathfrak{p}^t$ la più piccola potenza di $\mathfrak{p}$ contenuta in $\mathfrak{p}_1 + (a_1)$; da $\mathfrak{a} \subseteq \mathfrak{p}$ segue allora $\mathfrak{a}^t \subseteq \mathfrak{p}^t$, e quindi $\mathfrak{a}^t \subseteq \mathfrak{p}_1 + (a_1)$; in particolare, per ogni $i = 2, 3, \ldots, r$ si ha ${a_i}^t \in \mathfrak{p}_1 + (a_1)$ e quindi esistono $b_i \in A$ e $c_i \in \mathfrak{p}_1$ tali che

$$(16) \qquad {\mathfrak{a}_i}^t = c_i + a_1 b_i;$$

consideriamo ora l'ideale $\mathfrak{a}' = (c_2, c_3, \ldots, c_r) \subseteq \mathfrak{p}_1$; se proviamo che $\mathfrak{p}_1$ è primo minimale di $\mathfrak{a}'$, si avrà $\mathrm{ht}(\mathfrak{p}_1) \leq r-1$ e quindi $s \leq r$, da cui la tesi. Per completare la dimostrazione basta allora provare che $\mathfrak{p}_1$ è un primo minimale di $\mathfrak{a}'$; in particolare, basta provare che, se $\mathfrak{p}'$ è un primo minimale di $\mathfrak{a}'$ contenuto in $\mathfrak{p}_1$, allora si ha $\mathfrak{p}_1 = \mathfrak{p}'$.

Osserviamo che $a_i \in \mathfrak{r}(\mathfrak{a}' + (a_1)) \ \forall\ i = 1, 2, \ldots, r$ (per a_1 è banale; per gli altri segue dalla (16)); allora $\mathfrak{a} \subseteq \mathfrak{r}(\mathfrak{a}' + (a_1))$, e quindi $\mathfrak{r}(\mathfrak{a}) \subseteq \mathfrak{r}(\mathfrak{r}(\mathfrak{a}' + (a_1)))$, ossia $\mathfrak{p} \subseteq \mathfrak{r}(\mathfrak{a}' + (a_1))$; per la massimalità di $\mathfrak{p}$ si ha allora $\mathfrak{p} = \mathfrak{r}(\mathfrak{a}' + (a_1))$, e quindi (sempre essendo $\mathfrak{p}$ massimale) $\mathfrak{a}' + (a_1)$ risulta essere $\mathfrak{p}$-primario.

Sia ora $\mathfrak{p}'$ un primo minimale di $\mathfrak{a}'$ contenuto in $\mathfrak{p}_1$; proviamo che $\mathfrak{p}' = \mathfrak{p}_1$; essendo $\mathfrak{p}'$ un ideale primo, ${}^{A}\!/_{\mathfrak{p}'}$ è un dominio, il cui unico massimale è ${}^{\mathfrak{p}}\!/_{\mathfrak{p}'}$, che è primo minimale di ${}^{(a_1)+\mathfrak{p}'}\!/_{\mathfrak{p}'} = (a_1)^e$; per il Lemma di Krull si ha allora $\mathrm{ht}\left({}^{\mathfrak{p}}\!/_{\mathfrak{p}'}\right) = 1$, e quindi fra $\mathfrak{p}'$ e $\mathfrak{p}$ non vi sono altri ideali; da $\mathfrak{p}' \subseteq \mathfrak{p}_1 \subsetneq \mathfrak{p}$ segue allora $\mathfrak{p}_1 = \mathfrak{p}'$ e quindi, come già visto, la tesi. □

Esempio 1.2 Consideriamo l'anello $A = k[x, y, z]$ ed i suoi ideali

$$\mathfrak{a} = \left(x^2, xy\right), \qquad \mathfrak{b} = (xy, xz);$$

una decomposizione di $\mathfrak{a}$ è $\mathfrak{a} = (x) \cap (x, y)$, una decomposizione di $\mathfrak{b}$ è $\mathfrak{b} = (x) \cap (y, z)$; il primo minimale di $\mathfrak{a}$ è allora (x), di altezza 1; i primi minimali di $\mathfrak{b}$ sono (x), di altezza 1, ed (y, z), di altezza 2 (che (y, z) abbia altezza 2 si vede osservando che, per Krull, (y, z) ha altezza non maggiore di 2; d'altra parte, la catena di primi $(0) \subseteq (y) \subseteq (y, z)$ ha lunghezza 2; quindi (y, z) ha esattamente lunghezza 2).

Esempio 1.3 Consideriamo l'anello $A = {}^{k[u,v,w]}\!/_{\left(uv,\, uw,\, w - v^2\right)}$ ed il suo ideale

$$\mathfrak{a} = (\bar{u}, \bar{v}, \bar{w});$$

determiniamo l'altezza di $\mathfrak{a}$; osserviamo che, poiché $A \cong {}^{k[u,v]}\!/_{(uv)}$, $\mathfrak{a} \cong (\bar{u}, \bar{v})$ ha altezza non maggiore di 2; d'altra parte, $\mathfrak{a}$ contiene l'ideale nullo, e quindi contiene i primi minimali di (0), che sono $(\bar{u})$, $(\bar{v})$; in ${}^{A}\!/_{(\bar{u})}$ si ha $\mathrm{ht}\left({}^{(\bar{u},\bar{v})}\!/_{(\bar{u})}\right) = 1$, in quanto l'ideale è principale (generato da $\bar{v}$), e $\mathrm{ht}\left({}^{(\bar{u})}\!/_{(\bar{u})}\right) = \mathrm{ht}(0) = 0$; ne segue allora $\mathrm{ht}((\bar{u}, \bar{v})) = 1$, e quindi $\mathfrak{a}$ ha altezza 1.

Osservazione 1.3 In un anello noetheriano A ogni primo ha altezza finita (poiché ogni ideale è finitamente generato, ed ogni primo è primo minimale di un ideale); non è però detto che A sia di dimensione finità, poiché possono esistere un numero infinito di primi $\mathfrak{p}_n$, con $\mathrm{ht}(\mathfrak{p}_n) = n$; in tal caso, la dimensione di A risulta essere infinita.

ESEMPIO 1.4 Consideriamo l'anello $A = k[x_1, x_2, \ldots, x_n, \ldots]$ dei polinomi in infinite variabili, e consideriamo in esso i primi

$$\mathfrak{p}_1 = (x_1), \quad \mathfrak{p}_2 = (x_2, x_3), \quad \mathfrak{p}_3 = (x_4, x_5, x_6), \quad \mathfrak{p}_4 = (x_7, x_8, x_9, x_{10}), \quad \ldots;$$

sia poi $S = A \setminus \left(\bigcup_{n\in\mathbb{N}} \mathfrak{p}_n\right) = \bigcap_{n\in\mathbb{N}} (A \setminus \mathfrak{p}_n)$, e consideriamo l'anello $A_S = S^{-1}A$; si può provare che questo anello è noetheriano; inoltre, le immagini dei $\mathfrak{p}_n$ in A_S sono ideali massimali, di altezza n; quindi A_S è un anello noetheriano di dimensione infinita.

OSSERVAZIONE 1.4 Se A è un anello locale o semi-locale (ossia, con un numero finito di massimali), A ha necessariamente dimensione finita. In particolare,

- se A è $\mathfrak{m}$-locale, allora $\dim A = \mathrm{ht}(\mathfrak{m})$;
- se A è semi-locate, allora $\dim A = \max\{\mathrm{ht}(\mathfrak{m}_i) \mid \mathfrak{m}_i \text{ massimale di } A\}$.

TEOREMA 1.2 *Se $\mathfrak{p}$ è un primo di A di altezza r, allora esiste un ideale $\mathfrak{a}$ di A, generato da r elementi e di cui $\mathfrak{p}$ è un primo minimale.*

Dimostrazione. Costruiamo per induzione i generatori $a_1, a_2, \ldots, a_r$ di $\mathfrak{a}$, in modo che $(a_1, a_2, \ldots, a_i)$ abbia altezza i. Essendo $\mathfrak{p}$ primo, $\mathfrak{p}$ è non vuoto e quindi esiste $a_1 \in \mathfrak{p}$; (a_1) costituisce la base dell'induzione; supponiamo ora di aver costruito $a_1, a_2, \ldots, a_i$, con $i < r$, e costruiamo a_{i+1}.

Sia $\mathfrak{q}$ un primo minimale di $(a_1, a_2, \ldots, a_i)$; per il TEOR. di Krull dell'altezza, $\mathrm{ht}(\mathfrak{q}) \leq i$; d'altra parte, $(a_1, a_2, \ldots, a_i) \subseteq \mathfrak{q}$ e $\mathrm{ht}(a_1, a_2, \ldots, a_i) = i$, quindi $\mathrm{ht}(\mathfrak{q}) \geq i$; in definitiva, $\mathrm{ht}(\mathfrak{q}) = i$; l'arbitrarietà di $\mathfrak{q}$ assicura che tutti i primi minimali di $(a_1, a_2, \ldots, a_i)$ hanno altezza i.

Essendo $i < r$, $\mathfrak{p}$ non è contenuto in alcun minimale di $(a_1, a_2, \ldots, a_i)$; per la PROP. 1 di pag. 10 ne segue allora che $\mathfrak{p}$ non è contenuto nell'unione dei primi minimali di $(a_1, a_2, \ldots, a_i)$, ed è quindi possibile sceglie $a_{i+1} \in \mathfrak{p}$, a_{i+1} non appartenente ad alcun primo minimale di $(a_1, a_2, \ldots, a_i)$; per provare la tesi basta provare che $(a_1, a_2, \ldots, a_{i+1})$ ha altezza $i + 1$.

Sia $\mathfrak{t}$ un primo minimale di $(a_1, a_2, \ldots, a_{i+1})$; per il TEOR. di Krull dell'altezza si ha $\mathrm{ht}(\mathfrak{t}) \leq i+1$; d'altra parte, detto $\mathfrak{q}$ un primo minimale di $(a_1, a_2, \ldots, a_i)$, si ha $\mathfrak{q} \subsetneq \mathfrak{t}$, e quindi $\mathrm{ht}(\mathfrak{t}) > \mathrm{ht}(\mathfrak{q}) \geq i$, ossia $\mathrm{ht}(\mathfrak{t}) \geq i + 1$; risulta allora $\mathrm{ht}(\mathfrak{t}) = i + 1$, per ogni primo minimale $\mathfrak{t}$ di $(a_1, a_2, \ldots, a_{i+1})$, e quindi $(a_1, a_2, \ldots, a_{i+1})$ ha altezza $i + 1$, come volevasi. □

COROLLARIO 1.1 *In un anello $\mathfrak{m}$-locale A di dimensione d esiste un ideale $\mathfrak{m}$-primario generato da d elementi.*

Dimostrazione. Infatti, d è l'altezza di $\mathfrak{m}$; per il precedente TEOR., esiste allora $\mathfrak{a}$ generato da d elementi, ed $\mathfrak{m}$ è un primo minimale di $\mathfrak{a}$; allora $\mathfrak{a}$ è $\mathfrak{m}$-primario, ed è generato da d elementi. □

COROLLARIO 1.2 *Sia A un anello $\mathfrak{m}$-locale; la dimensione d di A è il minimo numero di elementi necessari per generare un ideale $\mathfrak{m}$-primario.*

Dimostrazione. Dal precedente COR. segue che la dimensione di A è non minore del minimo numero di elementi necessari per generare un ideale $\mathfrak{m}$-primario; d'altra

parte, se vi fosse la maggiorazione stretta, esisterebbe un ideale $\mathfrak{a}$ $\mathfrak{m}$-primario generato da $r < d$ elementi, e quindi si avrebbe $\mathrm{ht}(\mathfrak{m}) \leq r < d = \dim A$, assurdo; vale allora l'uguaglianza. □

DEFINIZIONE 1.4 Sia A un anello $\mathfrak{m}$-locale di dimensione d e sia $\mathfrak{a} = (a_1, a_2, \ldots, a_d)$ un ideale $\mathfrak{m}$-primario di A; gli elementi $a_1, a_2, \ldots, a_d$ si dicono un *sistema di parametri* di A.

OSSERVAZIONE 1.5 Sia A un anello $\mathfrak{m}$-locale e sia $\nu(\mathfrak{m})$ il minimo numero di generatori di $\mathfrak{m}$; le precedenti osservazioni assicurano che $\dim A \leq \nu(\mathfrak{m})$; vedremo ora che gli anelli per cui è verificata l'uguaglianza godono di una proprietà molto importante.

DEFINIZIONE 1.5 Sia A un anello $\mathfrak{m}$-locale; il minimo numero di generatori di $\mathfrak{m}$ si suole chiamare *dimensione d'immersione* di A, e lo si denota con il simbolo e-dim A (e = *embedding*, immersione in inglese).

DEFINIZIONE 1.6 Un anello locale A per cui si abbia $\dim A =$ e-dim A suole dirsi *regolare*.

LEMMA 1.2 *Sia A un anello noetheriano $\mathfrak{m}$-locale; nessun ideale principale può contenere propriamente un primo non nullo.*

Dimostrazione. Supponiamo per assurdo che esistano un ideale principale (x) ed un ideale primo $\mathfrak{p}$ tali che $(0) \subsetneq \mathfrak{p} \subsetneq (x)$; sia $p \neq 0$ un generatore di $\mathfrak{p}$; da $p \in (x)$ segue che $p = \lambda x$; ma $x \notin \mathfrak{p}$, $\lambda x = p \in \mathfrak{p}$ implicano $\lambda \in \mathfrak{p} \subset (x)$, e quindi $\lambda = \lambda_1 x$; ripetendo il ragionamento, si costruisce una successione $\{\lambda_n\}$ tale che $\lambda_n \in \mathfrak{p}\ \forall\ n \in \mathbb{N}$ e

$$p = \lambda x = \lambda_1 x^2 = \cdots = \lambda_n x^{n+1} = \cdots ;$$

allora $p \in (x^n)\ \forall\ n \in \mathbb{N}$; ma $\bigcap_{n \in N} (x^n) = (0)$ (per il TEOR. dell'intersezione di Krull[1]), e quindi $p = 0$, contro il fatto che p fosse non nullo. □

LEMMA 1.3 *Sia A un anello regolare, e sia $x \in \mathfrak{m} \setminus \mathfrak{m}^2$; allora $A/(x)$ è regolare.*

Dimostrazione. Consideriamo il campo residuo di A, $k = A/\mathfrak{m}$; $\mathfrak{m}/\mathfrak{m}^2$ è uno spazio vettoriale su k; dalle definizioni segue inoltre che e-dim $A = \dim_k \mathfrak{m}/\mathfrak{m}^2$; essendo A regolare, si ha allora $r = \dim A =$ e-dim $A = \dim_k \mathfrak{m}/\mathfrak{m}^2$.

Consideriamo ora l'anello $\bar{A} = A/(x)$ e sia $\bar{\mathfrak{m}} = \mathfrak{m}/(x)$ l'immagine di $\mathfrak{m}$ in $\bar{A}$; per provare che A è regolare basta provare che $\dim \bar{A} = \dim_k \bar{\mathfrak{m}}/\bar{\mathfrak{m}}^2$; essendo $x \in \mathfrak{m} \setminus \mathfrak{m}^2$, l'immagine di x in $\mathfrak{m}/\mathfrak{m}^2$ è non nulla e quindi[2] $\dim_k \bar{\mathfrak{m}}/\bar{\mathfrak{m}}^2 = r - 1$; occorre allora provare che $s = \dim \bar{A} = r - 1$; si ha certamente $s \leq r - 1$ (un quoziente diminuisce sempre la dimensione di un anello); proviamo l'uguaglianza. Sappiamo che, essendo $s = \dim \bar{A}$, esiste un ideale $\bar{\mathfrak{m}}$-primario generato da s elementi $\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_s$; allora $(x, a_1, a_2, \ldots, a_s)$ è un ideale $\mathfrak{m}$-primario (immagine inversa di un ideale primario); quindi $s + 1 \geq r$, ossia $s \geq r - 1$; l'altra diseguaglianza è gia stata vista, e si ha quindi $s = r - 1$; allora $\dim \bar{A} = \dim_k \bar{\mathfrak{m}}/\bar{\mathfrak{m}}^2 =$ e-dim $\bar{A}$, e ciò assicura che $\bar{A}$ è regolare. □

---

[1] TEOR. 3.2, CAP. IV, pag. 48; (x) è contenuto nel radicale di Jacobson $\mathcal{R}$ poiché l'anello è $\mathfrak{m}$-locale, e quindi $\mathcal{R} = \mathfrak{m}$ ed ogni ideale di A è contenuto in $\mathfrak{m}$

[2] sia $\mathcal{B}$ di $\mathfrak{m}/\mathfrak{m}^2$ contenente l'immagine $\bar{x}$ di x; $\mathcal{B}$ ha r elementi; l'insieme $\mathcal{B} \setminus \{\bar{x}\}$ è una base di $\bar{\mathfrak{m}}/\bar{\mathfrak{m}}^2$, ed ha $r - 1$ elementi (in quanto $\bar{x} \neq 0$); quindi $\bar{\mathfrak{m}}/\bar{\mathfrak{m}}^2$ ha dimensione $r - 1$.

TEOREMA 1.3 (*Auslander–Buchsbaum*) *Ogni anello regolare è un UFD.*

Dimostrazione. Sia A un anello regolare. Proviamo che A è un dominio (la dimostrazione del fatto che A è a fattorizzazione unica viene omessa).

Ragioniamo per induzione sulla dimensione d di A.

Se $d = 0$, si ha $\mathfrak{m} = (0)$, e quindi A è un campo; in particolare, A è allora un dominio.

Supponiamo ora che $d > 0$, e che ogni anello regolare di dimensione $d-1$ sia un dominio; proviamo che A è un dominio.

Osserviamo che $d > 0$ assicura che $\mathfrak{m} \neq (0)$, e quindi $\mathfrak{m} \neq \mathfrak{m}^2$; esiste allora $x \in \mathfrak{m} \setminus \mathfrak{m}^2$; $A/(x)$ è regolare (per il precedente LEMMA 1.3), ed ha dimensione $d-1$ (visto nella dimostrazione del LEMMA suddetto); quindi $A/(x)$ è un dominio (per induzione); ne segue che (x) è primo.

Supponiamo ora per assurdo che A non sia un dominio; si ha $\operatorname{ht}(x) \leq 1$, ma poiché A non è un dominio, (0) non è primo, e quindi $\operatorname{ht}(x) = 0$ (LEMMA 1.2); in particolare, (x) è un primo minimale dello zero; il ragionamento vale per ogni $x \in \mathfrak{m} \setminus \mathfrak{m}^2$; possiamo allora dire che ogni elemento di $\mathfrak{m} \setminus \mathfrak{m}^2$ sta in un primo minimale dello zero; siano $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$ i primi minimali dello zero; abbiamo allora ottenuto che $\mathfrak{m} \setminus \mathfrak{m}^2 \subseteq \bigcup_{i=1}^t \mathfrak{p}_i$, e quindi $\mathfrak{m} \subseteq \left(\bigcup_{i=1}^t \mathfrak{p}_i\right) \cup \mathfrak{m}^2$; per l'OSS. 1.7, CAP. I, essendo $\mathfrak{m} \not\subseteq \mathfrak{m}^2$, esiste un indice $i = 1, 2, \ldots, t$ per cui $\mathfrak{m} \subseteq \mathfrak{p}_i$; la massimalità di $\mathfrak{m}$ assicura allora che $\mathfrak{m} = \mathfrak{p}_i$; i $\mathfrak{p}_i$ sono minimali dello zero, ed hanno quindi altezza zero; si avrebbe allora $d = \dim A = \operatorname{ht}(\mathfrak{m}) = 0$, assurdo. La tesi è allora verificata. □

OSSERVAZIONE 1.6 Nel LEMMA 1.3, l'ipotesi $x \notin \mathfrak{m}^2$ è essenziale; infatti, se $x \in \mathfrak{m}^2$, si ha $\dim \mathfrak{m}/\mathfrak{m}^2 = \dim \bar{\mathfrak{m}}/\bar{\mathfrak{m}}^2$ (poiché l'immagine di x è nulla, e quindi non sta in nessuna base); ma $\dim A/(x) = (\dim A) - 1$; si ha allora la diseguaglianza

$$\dim A/(x) < \dim A = \dim \mathfrak{m}/\mathfrak{m}^2 = \dim \bar{\mathfrak{m}}/\bar{\mathfrak{m}}^2 = \text{e-dim } A/(x);$$

per transitività, $\dim A/(x) < \text{e-dim } A/(x)$, ossia $A/(x)$ non è regolare.

ESEMPIO 1.5 L'anello $A = k[x,y]_{(x,y)}$ è regolare, in quanto $\dim A = 2$ (una catena di lunghezza massima per il massimale $\mathfrak{m} = (x,y)$ è $(0) \subset (x) \subset (x,y)$), e si ha anche $\text{e-dim } A = \nu(x,y) = 2$.

$A/(xy)$ non è regolare, in quanto non è un dominio.

$A/(x-y^2)$ è regolare, poiché $x - y^2 \in \mathfrak{m} \setminus \mathfrak{m}^2$.

ESEMPIO 1.6 L'anello $A = k[x,y,z]_{(x,y,z)}$ è regolare, in quanto $\dim A = 3$ (una catena di lunghezza massima per il massimale $\mathfrak{m} = (x,y,z)$ è $(0) \subset (x) \subset (x,y) \subset (x,y,z)$), e si ha anche $\text{e-dim } A = \nu(x,y,z) = 3$.

$A/(x-y^2-z^2)$ è regolare, poiché $x - y^2 \in \mathfrak{m} \setminus \mathfrak{m}^2$.

$B = A/(x^2-y^2-z^2)$ non è regolare; osserviamo a tal fine che B è un domino; non è tuttavia UFD ($\bar{x}^2 - \bar{y}^2 - \bar{z}^2 = 0$ implica $\bar{z}^2 = \bar{x}^- \bar{y}^2 = (\bar{x} - \bar{y})(\bar{x} + \bar{y})$: $\bar{z}^2$ non si decompone in maniera unica).

ESEMPIO 1.7 L'anello $A = \mathbb{C}[x,y,z,t]_{(x,y,z,t)}$ è regolare, di dimensione 4; il suo anello quoziente $A/(x^2+y^2+z^2+t^2)$ non è regolare, in quanto non è un domino a fattorizzazione unica (ciò si vede come nell'esempio precedente).

Osservazione 1.7 Sorprendentemente, il ragionamento fatto per gli anelli di frazioni generati a partire dagli anelli di polinomi a tre o quattro variabili non sussiste più per cinque variabili; infatti, l'anello $A = \mathbb{C}[x, y, z, t, u]_{(x,y,z,t,u)}$ è regolare, di dimensione 5; il suo anello quoziente $A\big/\big(x^2 + y^2 + z^2 + t^2 + u^2\big)$ è un dominio a fattorizzazione unica; si può però provare che il suddetto quoziente non è regolare; possiamo quindi affermare che la condizione di regolarità del precedente Teor. è necessaria, ma non sufficiente, in quanto è appena stato portato un esempio di UFD non regolare.

Osservazione 1.8 Diamo infine un'interpretazione geometrica degli anelli regolari; come esempio, guardiamo al caso $A = k[x, y, z]_{(x,y,z)}$ ed ai due anelli quoziente

$$A\big/\big(x^2 - y^2 - z^2\big), \qquad A\big/\big(x - y^2 - z^2\big);$$

abbiamo visto che il primo non è regolare, mentre il secondo lo è; ora, se consideriamo, in $\mathbb{R}^3$ le equazioni

$$x^2 - y^2 - z^2 = 0, \tag{17}$$

$$x \ - y^2 - z^2 = 0, \tag{18}$$

sappiamo che rappresentano rispettivamente un cono (la (17)) ed un paraboloide (la (18)); la differenza sostanziale nelle due figure geometriche è che la prima ha un punto singolare, mentre la seconda no; in generale, si può dimostrare che un anello quoziente regolare corrisponde ad una figura geometrica con tutti punti regolari, mentre un anello quoziente non regolare corrisponde ad una figura geometrica con almeno un punto singolare.